

Gerd Fischer

Lernbuch Lineare Algebra und Analytische Geometrie

Das Wichtigste ausführlich
für das Lehramts- und Bachelorstudium

2. Auflage

STUDIUM

A geometric diagram is overlaid on the lower half of the cover. It features several intersecting lines in shades of green and blue. Several angles are marked with small arcs and labeled with mathematical symbols: α_0 , β_0 , γ_0 , and δ_0 . The diagram appears to be a complex geometric construction, possibly related to projective geometry or linear algebra.

 Springer Spektrum

Lernbuch Lineare Algebra und Analytische Geometrie

Gerd Fischer

Lernbuch Lineare Algebra und Analytische Geometrie

Das Wichtigste ausführlich
für das Lehramts- und Bachelorstudium

2., überarbeitete und erweiterte Auflage

Unter Mitarbeit von Florian Quiring

STUDIUM



Springer Spektrum

Prof. Dr. Gerd Fischer
Zentrum Mathematik
Technische Universität München
Garching
Deutschland

ISBN 978-3-8348-2378-6
DOI 10.1007/978-3-8348-2379-3

ISBN 978-3-8348-2379-3 (eBook)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Springer Spektrum

© Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden 2011, 2012

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Planung und Lektorat: Ulrike Schmickler-Hirzebruch | Barbara Gerlach

Satz: Jutta Niebauer und Florian Quiring

Bilder: Fabian Biebl

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Spektrum ist eine Marke von Springer DE.

Springer DE ist Teil der Fachverlagsgruppe Springer Science+Business Media.

www.springer-spektrum.de

Vorwort zur zweiten Auflage

Neben zahlreichen kleinen Verbesserungen und zusätzlichen Beispielen wurden einige umfangreichere Ergänzungen eingefügt. Sie behandeln Bezüge zur *numerischen Mathematik*, etwa die LR-Zerlegung und die QR-Zerlegung von Matrizen, sowie die Methode der kleinsten Quadrate zur Berechnung approximativer Lösungen von überbestimmten linearen Gleichungssystemen, zur *Geometrie*, wie Kegelschnitte durch vorgegebene Punkte, oder EULERSche Winkel, und schließlich zur *Physik*, wie gedämpfte Schwingungen, sowie Trägheitstensoren. Das sind Themen, für die in den meisten Vorlesungen kaum Zeit bleibt, die aber gut geeignet sind für ein Proseminar zur Ergänzung.

Besonderer Dank für die Hilfen bei der Vorbereitung der Neuauflage gilt meinem bewährten Team. Voran Florian Quiring für die vielen guten Ideen die er beigetragen hat, Jutta Niebauer für die stilvolle Gestaltung der Druckvorlage, sowie Fabian Biebl für die perfekten Abbildungen.

Wie immer möchte ich meine Leserinnen und Leser bitten, mir Hinweise auf verbliebene Fehler und mögliche Verbesserungen mitzuteilen.

München, im Februar 2012

Gerd Fischer

Vorwort

Die Lineare Algebra ist im 19. Jahrhundert entstanden, zunächst als Teil der Geometrie; sie wurde aber im Laufe des 20. Jahrhunderts zu einem unentbehrlichen Hilfsmittel in allen Teilen der Mathematik. Darüber hinaus benutzen viele andere Wissenschaften – wie beispielsweise Physik, Informatik, Technik und Ökonomie – Methoden der Linearen Algebra. Dem entsprechend ist die Lineare Algebra zusammen mit Aspekten der analytischen Geometrie fest verankert im Curriculum der Studienanfänger.

Die zentralen Themen dieses Buches sind Vektorräume, lineare und bilineare Abbildungen, Determinanten und Eigenwerte, mit ihren Anwendungen auf die Geometrie. Es wird versucht, die elementaren Grundlagen sehr ausführlich darzustellen, illustriert durch zahlreiche im Detail erklärte und durchgerechnete Beispiele, sowie viele Bilder, die helfen sollen, den geometrischen Hintergrund für abstrakte Konzepte aufzuhellen. Daher der Name „Lernbuch“: Es soll Studierenden helfen, als Begleittext zu einer Vorlesung auch zusätzliche Hintergründe und Ergänzungen bereit zu stellen, und so das Verständnis zu vertiefen. Weitergehende interaktive Visualisierungen mit „dynamischer Geometrie“ findet man unter

www.mathe-vital.de

Beim Studium der Mathematik ist es besonders wichtig, die abstrakten Begriffe und technischen Methoden zunächst anschaulich zu motivieren, um ihre Entstehung zu erklären und ihre enorme Wirksamkeit deutlich zu machen. Die Mathematik hat über Jahrtausende eine stetige Entwicklung durchlaufen; was EUKLID um 300 v. Chr. bewiesen hat, ist auch heute noch gültig. Um Studierenden einen besseren Einblick in die Geschichte zu ermöglichen, sind neben historischen Anmerkungen auch zahlreiche grundlegende mathematische Veröffentlichungen der Vergangenheit im Literaturverzeichnis zitiert. Ein Gang in die Bibliothek und ein Blick in die alten Bücher kann ein äußerst spannendes Erlebnis sein!

Kapitel 0 soll den Übergang von der Schule zur Hochschule herstellen und den Einstieg in das Studium der Mathematik erleichtern. Zukünftige Lehrer kann es auch auf den Weg zurück in die Schule vorbereiten, und später dort begleiten. Es wird dabei versucht, dem Leitmotiv von FELIX KLEIN – einer *Elementarmathematik vom höheren Standpunkt* – zu folgen; einem Standpunkt etwas höher als die Mathematik in der Schule, aber nicht über den Wolken. Ziel dieses einführenden Kapitels ist die auf GAUSS zurückgehende systematische Methode der Elimination zur Lösung linearer Gleichungssysteme. Das ist und bleibt das wichtigste Ergebnis der elementaren Linearen Algebra.

In Kapitel 1 wird der in der zweiten Hälfte des 19. Jahrhunderts begonnene systematische und axiomatische Aufbau der Mathematik skizziert. Das gehört heute zu den Grundlagen aller Teile der Mathematik, muss aber nicht gleich zu Beginn in dieser Ausführlichkeit studiert werden. Als zentrales Projekt wurde der von DEDEKIND begonnene systematische Aufbau des Systems der Zahlen, von den natürlichen bis zu den komplexen Zahlen, aufgenommen. Einschließlich eines technisch anspruchsvollen Abschnitts über eine Konstruktion des Körpers der reellen Zahlen und die Zusammenhänge mit Dezimalbrüchen.

Kapitel 2 enthält die grundlegenden Dinge der Linearen Algebra, soweit sie ohne Benutzung von Determinanten behandelt werden können. Als Anwendung werden auch lineare Gleichungssysteme noch einmal in allgemeinerem Rahmen beschrieben. Kapitel 3 dient der Beschreibung von Determinanten; dabei wird auch etwas ausführlicher auf die in vielen anderen Zusammenhängen wichtigen Permutationen eingegangen. Damit sind die Vorbereitungen getroffen für den etwas fortgeschritteneren Teil der Linearen Algebra, die Theorie der Eigenwerte in Kapitel 4. Sie führt bis hin zur JORDANSchen Normalform, zu deren Verständnis etwas Übung mit all den grundlegenden Techniken der Linearen Algebra nötig ist.

In Kapitel 5 werden schließlich bilineare Abbildungen, sowie im reellen und komplexen Fall metrische Eigenschaften behandelt. Die geometrische Seite davon ist die klassische Theorie der Kegelschnitte und Quadriken, die viele Anwendungen auch in der Physik hat. Leider sind diese spannenden Themen, hoffentlich nur vorübergehend, aus den Lehrplänen der Gymnasien so gut wie verschwunden.

Als Hilfestellung für die Lektüre sind Teile, die man eventuell zunächst überspringen kann, mit einem * markiert. Die Hinweise in eckigen Klammern, etwa [EU], beziehen sich auf das Literaturverzeichnis. Um das Lernen zu erleichtern, sind Inhaltsverzeichnis und Index sehr umfangreich gestaltet.

Dieses „Lernbuch“ enthält inhaltlich, aber wesentlich ausführlicher in der Darstellung, die wichtigsten Themen aus den beiden „klassischen“ Büchern [FI₁] und [FI₂]; dort werden darüber hinaus auch weiterführende Dinge wie Dualität, Tensorprodukte und projektive Geometrie behandelt. Viele spannende Anwendungen der Linearen Algebra findet man in [STR].

Trotz aller Sorgfalt bei den Korrekturen des Textes ist es erfahrungsgemäß kaum zu vermeiden, dass noch Druckfehler und Ungenauigkeiten verblieben sind. Daher möchte ich alle Leserinnen und Leser, die fündig geworden sind bitten, mir die kritischen Stellen mitzuteilen, an

gfisher@ma.tum.de

Auf meiner Homepage

<http://www-m10.ma.tum.de/bin/view/Lehrstuhl/GerdFischer>

wird dann eine Seite mit Verbesserungen eingerichtet, außerdem findet sich dort eine Sammlung von Übungsaufgaben.

Mein Dank gilt all den Helferinnen und Helfern, die beim Entstehen dieses Buches mitgewirkt haben. In erster Linie meinem langjährigen Mitarbeiter Florian Quiring, dem Meister der Bilder Fabian Biebl, Bernhard Hanke für nützliche Hinweise, sowie Eva Dörfler, Vanessa Krummeck, Matthias Lehner, Jutta Niebauer, Michael Vogt und auch den Studierenden der TU München, die mich mit kritischen Bemerkungen immer wieder zu Verbesserungen und Ergänzungen angeregt haben. Die TUM-School of Education hat die Veröffentlichung mit Mitteln der Deutschen Telekom Stiftung unterstützt. Schließlich danke ich Ulrike Schmickler-Hirzebruch sehr herzlich für ihre stetige Ermutigung, dieses Projekt in Angriff zu nehmen und zügig zu Ende zu bringen.

Inhalt

0	Lineare Geometrie im n-dimensionalen reellen Raum	1
0.1	Der n -dimensionale reelle Raum	1
0.1.1	Zahlen	1
0.1.2	Der Vektorraum \mathbb{R}^n	7
0.1.3	Multiplikation von Vektoren	11
0.2	Geraden	12
0.2.1	Ausblick	12
0.2.2	Geraden im \mathbb{R}^n	12
0.2.3	Geraden in der Ebene	16
0.3	Abstände und Winkel	20
0.3.1	Das Skalarprodukt im \mathbb{R}^n	20
0.3.2	Anwendungen in der Elementargeometrie	22
0.3.3	Winkel im \mathbb{R}^n	26
0.3.4	Senkrechte Vektoren und Abstände	33
0.3.5	Die HESSEsche Normalform einer Geradengleichung	35
0.3.6	Lineare Unabhängigkeit	38
0.3.7	Das Vektorprodukt im \mathbb{R}^3	41
0.3.8	Abstand von Geraden	46
0.4	Ebenen	51
0.4.1	Ebenen im \mathbb{R}^n	51
0.4.2	Ebenen im \mathbb{R}^3	55
0.4.3	Abstand eines Punktes von einer Ebene	59
0.4.4	Das Spatprodukt	61
0.5	Lineare Gleichungssysteme	64
0.5.1	Zwei Geraden in der Ebene	64
0.5.2	Beschreibung durch Matrizen	66
0.5.3	Koeffizientenmatrix in Zeilenstufenform	67
0.5.4	Das GAUSSsche Eliminationsverfahren	73
0.5.5	Wahl der Pivots und Rundungsfehler	77

1	Grundlagen	81
1.1	Mengen, Relationen, Abbildungen	81
1.1.1	Mengen und Teilmengen	81
1.1.2	Operationen mit Mengen	83
1.1.3	Abbildungen	85
1.1.4	Abzählbare Mengen*	89
1.1.5	Äquivalenzrelationen*	93
1.2	Halbgruppen und Gruppen	98
1.2.1	Die natürlichen Zahlen*	98
1.2.2	Verknüpfungen und Halbgruppen	103
1.2.3	Gruppen	105
1.2.4	Die ganzen Zahlen als additive Gruppe*	108
1.2.5	Untergruppen und Homomorphismen	112
1.3	Ringe und Körper	114
1.3.1	Die ganzen Zahlen als Ring*	114
1.3.2	Der Körper der rationalen Zahlen	119
1.3.3	Dezimalbruchentwicklung rationaler Zahlen*	126
1.3.4	Konstruktion der reellen Zahlen*	130
1.3.5	Reelle Zahlen als Dezimalbrüche*	138
1.3.6	Komplexe Zahlen	143
1.3.7	Endliche Körper*	149
1.3.8	Rückblick und Ausblick	155
1.4	Polynome*	157
1.4.1	Polynome und Polynomfunktionen	157
1.4.2	Der Ring der Polynome	158
1.4.3	Division mit Rest	160
1.4.4	Nullstellen von Polynomen	161
1.4.5	Eine Vorzeichenregel für reelle Polynome	165
1.4.6	Der Fundamentalsatz der Algebra	167
2	Vektorräume und lineare Abbildungen	173
2.1	Grundlagen	174
2.1.1	Vektorräume	174
2.1.2	Untervektorräume	177
2.1.3	Operationen mit Untervektorräumen	178
2.1.4	Lineare Unabhängigkeit	181
2.2	Basis und Dimension	188
2.2.1	Erzeugendensysteme und Basen	188
2.2.2	Dimension eines Vektorraums	191
2.2.3	Charakterisierungen einer Basis	196
2.2.4	Praktische Verfahren zur Bestimmung einer Basis	199
2.2.5	Summen und direkte Summen	203
2.2.6	Der Rang einer Matrix	210

2.3	Lineare Abbildungen	216
2.3.1	Definitionen und Beispiele	216
2.3.2	Elementare Eigenschaften linearer Abbildungen	220
2.3.3	Spezielle lineare Abbildungen	223
2.3.4	Eine Dimensionsformel für lineare Abbildungen	227
2.3.5	Lineare Gleichungssysteme	229
2.3.6	Quotientenvektorräume*	234
2.4	Lineare Abbildungen und Matrizen	240
2.4.1	Erzeugung linearer Abbildungen	240
2.4.2	Die darstellende Matrix einer linearen Abbildung	242
2.4.3	Multiplikation von Matrizen	247
2.4.4	Rechenregeln für Matrizen	251
2.4.5	Die allgemeine lineare Gruppe	255
2.4.6	Elementarmatrizen	257
2.4.7	Lineare Gleichungssysteme und Elementarmatrizen*	264
2.4.8	Die LR-Zerlegung*	265
2.4.9	Dualität*	268
2.5	Transformationen	271
2.5.1	Basistransformationen und Koordinatentransformationen	271
2.5.2	Transformationsformel für lineare Abbildungen	274
2.5.3	Eine Normalform für darstellende Matrizen	276
3	Determinanten	281
3.1	Motivation	281
3.1.1	Lineare Gleichungssysteme	281
3.1.2	Flächeninhalt und Orientierung	282
3.2	Berechnung von Determinanten	287
3.2.1	Axiome für Determinanten	287
3.2.2	Weitere Eigenschaften der Determinante	290
3.2.3	Permutationen	298
3.2.4	Die alternierende Gruppe	304
3.2.5	Existenz und Eindeutigkeit	305
3.3	Minoren	311
3.3.1	Die komplementäre Matrix	311
3.3.2	LAPLACE-Entwicklung	313
3.3.3	Die CRAMERSche Regel	314
4	Eigenwerte	315
4.1	Grundbegriffe	315
4.1.1	Eigenwerte und Eigenvektoren	315
4.1.2	Endomorphismen des \mathbb{R}^2	318
4.1.3	Differentialgleichungen*	320
4.1.4	Das charakteristische Polynom	325

4.2	Diagonalisierung und Trigonalisierung	329
4.2.1	Diagonalisierbarkeit	329
4.2.2	Geometrische und algebraische Vielfachheit	331
4.2.3	Rechenverfahren zur Diagonalisierung	335
4.2.4	Trigonalisierung*	337
4.2.5	Zerlegung in Haupträume*	343
4.2.6	Nilpotente Endomorphismen*	349
4.2.7	Die JORDANSche Normalform*	356
4.2.8	Gedämpfte Schwingungen*	358
5	Bilineare Algebra und Geometrie	363
5.1	Kegelschnitte*	363
5.1.1	Die Gleichungen der ebenen Schnitte eines Kreiskegels	363
5.1.2	Geometrische Eigenschaften der Kegelschnitte*	366
5.1.3	Kegelschnitte durch vorgegebene Punkte*	370
5.1.4	Pol und Polare*	377
5.2	Bilinearformen	380
5.2.1	Definitionen und beschreibende Matrix	380
5.2.2	Transformationsformel für darstellende Matrizen	383
5.2.3	Entartung und Rang einer Bilinearform	384
5.2.4	Diagonalisierung einer symmetrischen Bilinearform	385
5.2.5	Das Trägheitsgesetz von SYLVESTER*	390
5.2.6	Exkurs über affine Geometrie*	393
5.2.7	Quadriken*	396
5.3	Euklidische und unitäre Vektorräume	409
5.3.1	Hermiteische Formen	409
5.3.2	Definitheit	410
5.3.3	Orthogonalität	418
5.3.4	QR-Zerlegung und Methode der kleinsten Quadrate*	424
5.3.5	Orthogonale und unitäre Endomorphismen	429
5.3.6	Die Gruppe $SO(3)$ *	435
5.3.7	Selbstadjungierte Endomorphismen	442
5.3.8	Hauptachsentransformation von Quadriken*	447
5.3.9	Der Trägheitstensor*	458
5.3.10	Ausblick	466
	Literaturverzeichnis	469
	Index	471
	Symbolverzeichnis	473

Kapitel 0

Lineare Geometrie im n -dimensionalen reellen Raum

Dieses einführende Kapitel soll als elementare Grundlage für das Studium der linearen Algebra dienen. Es werden Fragen behandelt, die auch in den Lehrplänen von Gymnasien enthalten sind. Studierende des Lehramts können dadurch diese Themen von einem etwas höheren Standpunkt betrachten und sich überzeugen, dass für exakte Begründungen ein angemessener theoretischer Rahmen nützlich ist. Aber auch alle anderen Leser können sich dadurch für das weitere Studium der linearen Algebra zusätzlich motivieren.

An einigen Stellen dieser Einführung werden schon elementare Eigenschaften und Notationen zu Mengen und Abbildungen verwendet. Wer damit noch nicht vertraut ist, kann das im Kapitel 1 nachlesen. Dort beginnt der systematische Aufbau der Theorie.

0.1 Der n -dimensionale reelle Raum

0.1.1 Zahlen

Die einfachsten geometrischen Gebilde neben Punkten sind die Geraden. EUKLID erklärt diese Begriffe um 300 v. Chr. zu Beginn seines I. Buches so [EU]:

1. Ein **Punkt** ist, was keine Teile hat.
2. Eine **Linie** ist eine breitenlose Länge.

Diese Erklärung von EUKLID ist recht scharfsinnig, aber natürlich keine präzise Definition. D. HILBERT hat die axiomatische Begründung über 2000 Jahre später sehr konsequent wieder aufgegriffen, das Ergebnis sind seine 1899 veröffentlichten „Grundlagen der Geometrie“ [HI₂].

Ein anderer Ansatz geht auf R. DESCARTES zurück. In seinem 1637 verfassten „Discours de la méthode“ führt er **Koordinaten** ein (heute „kartesisch“ genannt); dadurch wird es möglich, geometrische Objekte mit Hilfe von Zahlen zu beschreiben, und Aussagen durch Rechnungen zu prüfen und zu beweisen. Durch diese so genannte „analytische“ Geometrie ist ein höchst präzises und lebendiges Wechselspiel zwischen der Geometrie auf der einen und Algebra sowie Analysis auf der anderen Seite entstanden.

Grundlage für Rechnungen sind die Zahlen, der Prototyp einer Geraden ist die reelle Zahlengerade. Eine präzise Beschreibung dieses Kontinuums von Zahlen ist aber erst gegen Ende des 19. Jahrhunderts gelungen, vor allem durch die Arbeiten von R. DEDEKIND [DED₁, DED₂]. Bevor wir mit der elementaren analytischen Geometrie starten, ist es daher angebracht, den Aufbau des Systems der Zahlen wenigstens kurz – und zunächst recht informell – zu skizzieren. Etwas präziser wird das anschließend in Kapitel 1 ausgeführt.

Die verschiedenen Zahlbereiche werden schrittweise aufeinander aufgebaut. Leitmotiv dabei ist das Problem der Lösbarkeit von zunehmend schwierigen Gleichungen. Man startet mit der Menge

$$\mathbb{N} := \{0, 1, 2, \dots\}$$

der **natürlichen Zahlen**. Sie sind entstanden aus dem Vorgang des Zählens; die Null als Zahl ist schon etwas abstrakter. Dass \mathbb{N} die Null enthalten soll, ist eine manchmal nützliche Konvention. Will man sie ausschließen, so schreibt man:

$$\mathbb{N}^* := \{1, 2, \dots\} = \mathbb{N} \setminus \{0\}.$$

Für zwei beliebige natürliche Zahlen $m, n \in \mathbb{N}$ ist die Summe $m + n$ wieder in \mathbb{N} enthalten. Die Gleichung

$$m + x = n$$

hat jedoch nur dann eine Lösung $x \in \mathbb{N}$, wenn $m \leq n$ gilt. Will man solche Gleichungen für beliebige $m, n \in \mathbb{N}$ lösbar machen, so muss man negative Zahlen einführen. Das führt zur Menge

$$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$$

der **ganzen Zahlen**. Dabei ist die charakteristische Eigenschaft der neuen abstrakteren Zahl $-m$ für $m \in \mathbb{N}$, dass

$$m + (-m) = 0.$$

Für beliebige $m, n \in \mathbb{Z}$ hat damit die Gleichung

$$m + x = n$$

die eindeutige Lösung $x = n - m \in \mathbb{Z}$.

Mit Hilfe der Addition kann man auch eine Multiplikation natürlicher Zahlen erklären: Für $m, n \in \mathbb{N}$ ist

$$m \cdot n := \underbrace{n + \dots + n}_{m\text{-mal}}$$

wobei $0 \cdot n := 0$. Benützt man die Vorzeichenregeln

$$+ \cdot + = - \cdot - = + \quad \text{und} \quad + \cdot - = - \cdot + = -,$$

so kann diese Multiplikation von \mathbb{N} auf \mathbb{Z} fortgesetzt werden. Zu $m, n \in \mathbb{Z}$ hat man also ein Produkt $m \cdot n \in \mathbb{Z}$.

Beim Studium von Größenverhältnissen stößt man für $m, n \in \mathbb{Z}$ auf eine Gleichung der Form

$$n \cdot x = m.$$

Dafür hat man schon in der Antike mit rationalen (von lat. *ratio* = Verhältnis) Lösungen

$$x = \frac{m}{n},$$

falls $n \neq 0$, gerechnet. Dieses x ist nur dann ganzzahlig, wenn n ein Teiler von m ist. Um die Gleichung allgemein lösbar zu machen, geht man über zur Menge

$$\mathbb{Q} := \left\{ \frac{m}{n} : m, n \in \mathbb{Z}, n > 0 \right\}$$

der **rationalen Zahlen**. Da der Nenner n positiv sein soll, kann man das Vorzeichen am Zähler m ablesen. Zu bedenken ist, dass die Darstellung einer rationalen Zahl nicht eindeutig ist. Offensichtlich gilt:

$$\frac{m}{n} = \frac{m'}{n'} \Leftrightarrow m \cdot n' = n \cdot m'.$$

Dabei ist zu bemerken, dass die durch Multiplikation über Kreuz erhaltene Bedingung auf der rechten Seite innerhalb von \mathbb{Z} überprüft werden kann.

Addition und Multiplikation in \mathbb{Q} werden erklärt durch die Definitionen

$$\frac{m}{n} + \frac{m'}{n'} := \frac{mn' + nm'}{nn'} \quad \text{und} \quad \frac{m}{n} \cdot \frac{m'}{n'} := \frac{m \cdot m'}{n \cdot n'}.$$

Besonders ausgezeichnet sind die rationalen Zahlen

$$1 := \frac{1}{1} = \frac{n}{n} \quad \text{und} \quad 0 := \frac{0}{1} = \frac{0}{n} \quad (\text{wobei } n > 0).$$

Ist $a = \frac{m}{n} \in \mathbb{Q}$, so erklärt man weiterhin negative und inverse Zahlen

$$-a := \frac{-m}{n} \quad \text{und für } a \neq 0 \text{ setzt man } a^{-1} := \begin{cases} \frac{n}{m} & \text{falls } m > 0, \\ \frac{-n}{-m} & \text{falls } m < 0. \end{cases}$$

Für die weiteren Rechnungen benützt man die leicht aus den obigen Definitionen folgenden

Rechenregeln Sind $a, b, c \in \mathbb{Q}$, so gilt

A1	$(a + b) + c = a + (b + c)$	<i>Assoziativität der Addition</i>
A2	$a + b = b + a$	<i>Kommutativität der Addition</i>
A3	$a + 0 = a$	
A4	$a + (-a) = 0$	
M1	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$	<i>Assoziativität der Multiplikation</i>
M2	$a \cdot b = b \cdot a$	<i>Kommutativität der Multiplikation</i>
M3	$a \cdot 1 = a$	
M4	$a \cdot a^{-1} = 1, \text{ falls } a \neq 0$	
D	$a \cdot (b + c) = a \cdot b + a \cdot c$	<i>Distributivität</i>

All das wird in 1.3.2 präzise begründet. Eine Menge von Zahlen, die diesen Regeln genügt, wird dann ein **Körper** genannt.

Wie wir gesehen haben, kann man in \mathbb{Q} Gleichungen der Form $a \cdot x = b$ mit $a \neq 0$ eindeutig lösen. Eine solche Gleichung heißt **linear**, weil x nur mit der ersten Potenz vorkommt. Anders ist das bei einer quadratischen Gleichung, etwa

$$x^2 = b \text{ mit } b \in \mathbb{Q}.$$

Der klassische Problemfall ist $b = 2$; er tritt auf, wenn man die Länge der Diagonalen in einem Quadrat berechnen will. Dass diese aus geometrischen Gründen real existierende Zahl $x = \sqrt{2}$ nicht rational sein kann, folgt aus der schon bei EUKLID [EU, X, §115a] zu findenden

Bemerkung Es gibt keine natürlichen Zahlen m, n , so dass

$$\left(\frac{m}{n}\right)^2 = 2.$$

Beweis Angenommen, es gäbe doch solche Zahlen; dann könnte man gemeinsame Teiler kürzen. Also kann man annehmen, dass m und n teilerfremd sind. Aus

$$m^2 = 2n^2$$

folgt, dass m^2 gerade ist. Daher muss auch m gerade sein, denn für ungerades $m = 2k + 1$ mit $k \in \mathbb{N}$ wäre

$$m^2 = (2k + 1)^2 = 4k^2 + 4k + 1$$

ungerade. Also ist m gerade und aus $m = 2k$ folgt

$$m^2 = 4k^2 = 2n^2, \text{ also } n^2 = 2k^2.$$

Daher ist n^2 gerade und somit auch n . Also hätten m und n den gemeinsamen Teiler 2, im Widerspruch zur Annahme. ■

In der Analysis lernt man Verfahren zur Berechnung von Wurzeln, etwa von $\sqrt{2}$ (vgl. z.B. [FO₁, §6]). Dazu betrachtet man die rekursiv definierte Folge x_n rationaler Zahlen mit

$$x_0 = 1 \quad \text{und} \quad x_{n+1} = \frac{1}{2} \left(x_n + \frac{2}{x_n} \right) = \frac{x_n}{2} + \frac{1}{x_n}.$$

In rationalen Zahlen gerechnet ist

$$\begin{array}{llll} x_1 = \frac{3}{2}, & \text{also} & x_1^2 = \frac{9}{4} & \text{und} & x_1^2 - 2 = \frac{1}{4}, \\ x_2 = \frac{17}{12}, & \text{also} & x_2^2 = \frac{289}{144} & \text{und} & x_2^2 - 2 = \frac{1}{144}, \\ x_3 = \frac{577}{408}, & \text{also} & x_3^2 = \frac{332\,929}{166\,464} & \text{und} & x_3^2 - 2 = \frac{1}{166\,464}. \end{array}$$

Daran erkennt man, wie schnell und einfach beliebig gute rationale Näherungswerte x_n für $\sqrt{2}$ erhalten werden können, das ist genug für die praktische Rechnung. Für die Theorie stellt sich jedoch das Problem der Konvergenz, damit sind wir in der Analysis gelandet.

Dass die Folge rationaler Zahlen x_n^2 gegen 2 konvergiert, ist recht einfach zu sehen, das ist eine kleine Übungsaufgabe. Aber nach den Regeln der Analysis kann die Folge x_n nicht gegen eine rationale Zahl konvergieren, da $\sqrt{2}$ irrational ist. Damit steht man an der Schwelle des Übergangs von rationalen zu **reellen Zahlen**. Dafür gibt es in der Analysis mehrere gleichwertige Methoden; wir wollen den Übergang zunächst nur aus einer sehr praktischen Sicht beleuchten.

Jede natürliche Zahl n hat eine **Dezimalentwicklung** mit **Ziffern** $z_i \in \{0, \dots, 9\}$, d.h. eine Darstellung

$$n = z_N z_{N-1} \dots z_1 z_0,$$

was eine Abkürzung dafür ist, dass n sich in eindeutiger Weise als endliche Summe

$$n = z_N \cdot 10^N + z_{N-1} \cdot 10^{N-1} + \dots + z_1 \cdot 10^1 + z_0 \cdot 10^0 = \sum_{i=0}^N z_i \cdot 10^i$$

schreiben lässt. Dabei ist natürlich der größte auftretende Exponent N von 10 mit $z_N \neq 0$ abhängig von n .

Durch wiederholte Division mit Rest sieht man, dass jede rationale Zahl $\frac{m}{n}$ eine Darstellung als **Dezimalbruch** hat, der unendlich werden kann, also

$$\frac{m}{n} = \pm \left(z_N \cdot 10^N + \dots + z_0 \cdot 10^0 + z_{-1} \cdot 10^{-1} + z_{-2} \cdot 10^{-2} + \dots \right) = \pm \sum_{i=N}^{-\infty} z_i \cdot 10^i.$$

Wie wir später in 1.3.3 näher ausführen werden, ist die Dezimalbruchentwicklung einer rationalen Zahl stets periodisch; die Länge der Periode ist höchstens gleich $n - 1$. Für die oben berechnete Folge der Näherungen von $\sqrt{2}$ haben wir

$$x_1 = \frac{3}{2} = 1.5\bar{0},$$

$$x_2 = \frac{17}{12} = 1.4\overline{16},$$

$$x_3 = \frac{577}{408} = 1.414\overline{2156862745098039},$$

wobei der Querstrich die Periode anzeigt. Als Grenzwert erhält man einen Dezimalbruch, der keine Periode mehr hat; er beginnt mit

$$\lim_{n \rightarrow \infty} x_n = 1.414\,213\,562\dots$$

Nach dieser Erfahrung ist es eine naheliegende Idee, eine **reelle Zahl** zu definieren als beliebigen (nicht notwendig periodischen) Dezimalbruch. Bezeichnet \mathbb{R} die Menge aller solcher reeller Zahlen, so wird

$$\mathbb{Q} \subset \mathbb{R}$$

eine Teilmenge, indem man die rationalen Zahlen identifiziert mit den periodischen Dezimalbrüchen. Das klingt sehr einfach, ist aber voll von Tücken. Etwa das Problem nach der Konvergenz einer unendlichen Reihe der Form

$$\sum_{i=N}^{-\infty} z_i \cdot 10^i,$$

oder die Frage, wie man reelle Zahlen addiert und multipliziert. Bei endlichen Dezimalbrüchen kann man ganz hinten anfangen, bei unendlichen gibt es kein "ganz hinten".

All diese Fragen werden in der elementaren Analysis geklärt, in Kapitel 1 kommen wir nochmal darauf zurück. Was wir für die Theorie zunächst nur benötigen, sind folgende Eigenschaften der reellen Zahlen:

1. In \mathbb{R} hat man eine Addition und eine Multiplikation, damit wird \mathbb{R} zu einem Körper (d.h. es gelten die oben für \mathbb{Q} festgehaltenen Rechenregeln).
2. (a) Für jede reelle Zahl $x \in \mathbb{R}$ gilt $x > 0$ oder $x = 0$ oder $-x > 0$.
(b) Sind $x, y \in \mathbb{R}$ mit $x > 0$ und $y > 0$, so folgt $x + y > 0$ und $x \cdot y > 0$.
3. Jede Zahl $a \in \mathbb{R}$ mit $a \geq 0$ hat eine Quadratwurzel, d.h. es gibt ein $x \in \mathbb{R}$ mit $x^2 = a$. Für $a > 0$ sind $\pm x$ zwei verschiedene Wurzeln; mit \sqrt{a} bezeichnet man üblicherweise den positiven Wert.

Einzelheiten dazu findet man etwa bei [FO₁, §§3, 6]. In der Praxis kann man immer nur mit endlich vielen Stellen der Dezimalbruchentwicklung einer reellen Zahl rechnen, da wirken sich die theoretischen Probleme nicht aus. Als Ergebnis dieses Abschnitts halten wir noch einmal fest, welche **Zahlbereiche** behandelt wurden:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

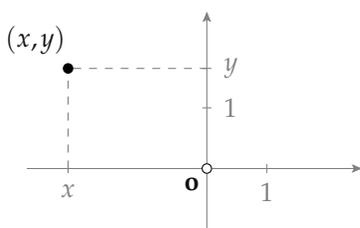
In 1.3.6 werden wir sehen, wie man \mathbb{R} erweitern kann zum Körper \mathbb{C} der **komplexen Zahlen**, um etwa die Gleichung

$$x^2 = -1$$

lösen zu können.

0.1.2 Der Vektorraum \mathbb{R}^n

Die Menge \mathbb{R} aller reellen Zahlen wird auch als „Zahlengerade“ bezeichnet. Bei den elementarsten Fragen der Geometrie untersucht man die gegenseitigen Lagen verschiedener Geraden in der Ebene und im dreidimensionalen Raum. In der so genannten „Analytischen Geometrie“ benützt man zur Beschreibung und Untersuchung geometrischer Sachverhalte „Koordinaten“, die es gestatten, mit Punkten zu rechnen. Es wird sich zeigen, dass dadurch viele Aussagen präziser beschrieben und einfacher bewiesen werden können, als mit rein geometrischen Argumenten.



Als Ebene stellt man sich zunächst die Zeichenebene vor, etwa als großes Blatt Papier. Zur Einführung von Koordinaten muss man einen Punkt **o** als **Ursprung** wählen und durch diesen zwei senkrechte Geraden als **Achsen** zeichnen. Schließlich werden die beiden Achsen skaliert durch reelle Zahlen. Dabei kann man die Wahl des Ursprungs und die Skalen dem zu untersuchenden geometrischen Problem anpassen. Im Ergebnis entsprechen dann Punkte der Ebene **geordneten Paaren** (x, y) von reellen Zahlen x und y . Man nennt sie **kartesische Koordinaten**, nach R. DESCARTES, auf den dieses Wechselspiel zwischen Geometrie und Analysis zurückgeht.

Nach diesen Vorbereitungen können wir die **Standardebene** erklären als **Menge der geordneten Paare reeller Zahlen**, in Zeichen

$$\mathbb{R}^2 := \{(x, y) : x, y \in \mathbb{R}\}.$$

Die Elemente von \mathbb{R}^2 heißen **Punkte**. Man beachte dabei, was ein **geordnetes Paar** genau bedeutet:

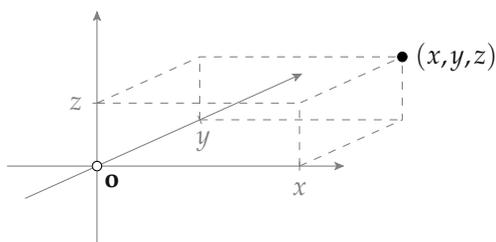
$$(x, y) = (x', y') \Leftrightarrow x = x' \text{ und } y = y'.$$

So ist etwa $(1, 2) \neq (2, 1)$ für Punkte in der Ebene, für Mengen natürlicher Zahlen gilt dagegen in der Notation mit geschweiften Klammern:

$$\{1, 2\} = \{2, 1\} \subset \mathbb{N}.$$

Ganz analog können wir nun **geordnete Tripel** (x, y, z) reeller Zahlen betrachten und dadurch die Punkte des „Raumes“ beschreiben, das ergibt

$$\mathbb{R}^3 := \{(x, y, z) : x, y, z \in \mathbb{R}\}.$$



Das entspricht den kartesischen Koordinaten im Raum.

Nach diesen Definitionen von Punkten in der Ebene bzw. im Raum als geordnete Paare bzw. Tripel von reellen Zahlen wird ein kritischer Leser hoffentlich Bedenken anmelden: In den benutzten Bildern wurden schon weit kompliziertere geometrische Gebilde als Punkte verwendet: Geraden, rechte Winkel, Parallele. Das ist ein grundlegender Zwiespalt in der analytischen Geometrie: Bilder sind die eine Seite, die geometrische; aus ihnen erhält man Ideen und Motivationen. Damit wird dann auf der anderen Seite, der analytischen, formal gerechnet. Die Bilder können entscheidende Anregungen für die Rechnung geben, aber sie dürfen die formalen Argumente nicht ersetzen. Was bleibt als Ergebnis: **Punkte** in der Ebene und im Raum sind erklärt als Paare oder Tripel reeller Zahlen. Mehr weiß man offiziell noch nicht. Sehr viel mehr zu diesem Thema findet man bei [BR, §4].

Nun ist es klar, dass man nach Paaren und Tripeln reeller Zahlen für beliebig große $n \in \mathbb{N}^*$ auch n -Tupel (x_1, \dots, x_n) reeller Zahlen betrachten kann. Das hat zwar keine unmittelbare geometrische Bedeutung mehr, aber dadurch wurden der linearen Algebra ungeahnte neue Anwendungen eröffnet. Wir begnügen uns hier mit einem ganz einfachen Beispiel. Eine Bank führt Konten für n Kunden, die Kontostände zu einem bestimmten Zeitpunkt sind gegeben durch reelle Zahlen x_1, \dots, x_n , wobei x_i der Kontostand des Kunden i ist. Der Saldo ist dann gegeben durch

$$x_1 + x_2 + \dots + x_n.$$

In diesem Sinne definieren wir den **n -dimensionalen reellen Standardraum**

$$\mathbb{R}^n := \{(x_1, \dots, x_n) : x_1, \dots, x_n \in \mathbb{R}\}$$

als Menge der **geordneten n -Tupel** reeller Zahlen. Geordnet bedeutet dabei, dass

$$(x_1, \dots, x_n) = (y_1, \dots, y_n) \Leftrightarrow x_1 = y_1, \dots, x_n = y_n.$$

Die Elemente des \mathbb{R}^n nennt man auch **Punkte**.

Wie schon angekündigt, ist es nun entscheidend, dass man mit den Punkten des \mathbb{R}^n rechnen kann. Grundlegend sind zwei Arten von Operationen. Erstens hat man eine **Addition**:

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) := (x_1 + y_1, \dots, x_n + y_n).$$

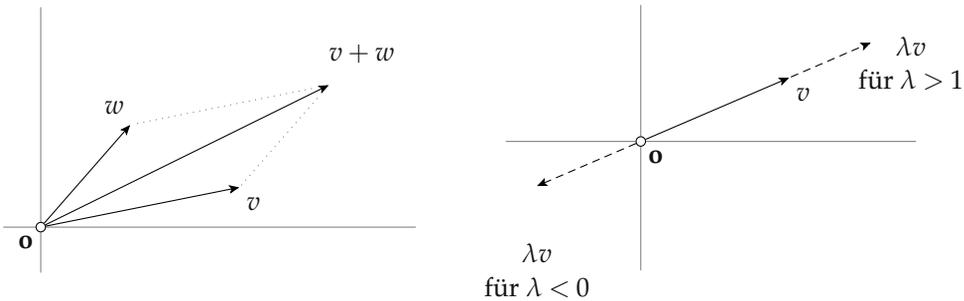
Dabei bedeutet $+$ auf der rechten Seite die Addition reeller Zahlen, das $+$ auf der linken Seite die neu definierte Addition von Punkten.

Zweitens kann man eine **Multiplikation mit reellen Zahlen** (oder **Skalaren**) erklären durch

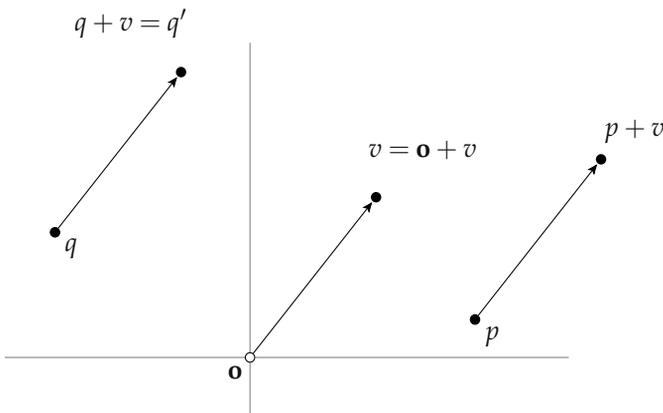
$$\lambda \bullet (x_1, \dots, x_n) := (\lambda \cdot x_1, \dots, \lambda \cdot x_n).$$

Wieder steht rechts die alte Multiplikation in \mathbb{R} , links die neue Multiplikation.

Diese beiden Rechenoperationen kann man schön geometrisch beschreiben, indem man jeden Punkt $v = (x_1, \dots, x_n)$ des \mathbb{R}^n als **Vektor** betrachtet, das ist geometrisch gesehen ein Pfeil vom **Ursprung** $\mathbf{o} = (0, \dots, 0)$ nach v .



Der Leser mag zu Recht einwenden, dass es verwirrend sein kann, nicht zwischen Punkten und Pfeilen zu unterscheiden. Im Rahmen der affinen Geometrie kann man diese beiden Begriffe klar auseinanderhalten: Die Pfeile (oder Vektoren) operieren auf der Menge der Punkte als **Translationen**, d.h. ein Vektor v ordnet jedem Punkt p einen Bildpunkt $p + v$ zu; dadurch wird die Menge der Punkte parallel verschoben. Für zwei Punkte $q, q' \in \mathbb{R}^n$ ist dann $v := q' - q$ der Vektor, der q in q' überführt. Der Name „vector“ wurde wohl zum ersten Mal von W. HAMILTON um 1845 benutzt. Er ist ein „Träger“, der den Punkt q nach q' „trägt“.



Zunächst aber wollen wir diese Unterscheidung von Punkten und Vektoren unterdrücken und die Eigenschaften der Vektoren als Elemente des \mathbb{R}^n näher betrachten. Die Frage, was ein Vektor an sich ist, macht nicht viel Sinn: Vektor zu sein, ist keine „individuelle“, sondern eine „soziale“ Eigenschaft. Das heißt genauer gesagt, es geht um die Regeln zwischen verschiedenen Vektoren, die durch Addition oder Multiplikation mit Skalaren verknüpft sind. In der Physik treten Vektoren etwa zur Beschreibung von Kräften auf. Auch dort ist es entscheidend, wie verschiedene Kräfte zusammenwirken.

Zur Unterscheidung von der Addition und Multiplikation in \mathbb{R} hatten wir die Verknüpfungen in \mathbb{R}^n mit fetten Symbolen $+$ und \bullet bezeichnet. Außerdem haben wir den

$$\begin{array}{ll} \text{Nullvektor} & \mathbf{o} := (0, \dots, 0) \in \mathbb{R}^n \quad \text{und einen} \\ \text{Negativen} & -v := (-x_1, \dots, -x_n) \in \mathbb{R}^n \quad \text{zu } v = (x_1, \dots, x_n) \in \mathbb{R}^n. \end{array}$$

Wir notieren nun elementare

Rechenregeln für Vektoren

Für $u, v, w \in \mathbb{R}^n$ und $\lambda, \mu \in \mathbb{R}$ gelten die folgenden Beziehungen

$$\begin{array}{ll} \mathbf{1} \quad \mathbf{a)} & (u + v) + w = u + (v + w), \quad \mathbf{b)} \quad v + w = w + v, \\ \quad \mathbf{c)} & v + \mathbf{o} = v, \quad \mathbf{d)} \quad v + (-v) = \mathbf{o}. \\ \mathbf{2} \quad \mathbf{a)} & (\lambda \cdot \mu) \bullet v = \lambda \bullet (\mu \bullet v), \quad \mathbf{b)} \quad \lambda \bullet (v + w) = \lambda \bullet v + \lambda \bullet w, \\ \quad \mathbf{c)} & (\lambda + \mu) \bullet v = \lambda \bullet v + \mu \bullet v, \quad \mathbf{d)} \quad 1 \bullet v = v. \end{array}$$

Die *Beweise* folgen sofort aus den Definitionen und den Rechenregeln in \mathbb{R} aus 0.1.1. Als Beispiel zeigen wir 2a):

$$\begin{aligned} (\lambda \cdot \mu) \bullet (x_1, \dots, x_n) &= ((\lambda \cdot \mu) \cdot x_1, \dots, (\lambda \cdot \mu) \cdot x_n) = (\lambda \cdot (\mu \cdot x_1), \dots, \lambda \cdot (\mu \cdot x_n)) \\ &= \lambda \bullet (\mu \cdot x_1, \dots, \mu \cdot x_n) = \lambda \bullet (\mu \bullet (x_1, \dots, x_n)). \end{aligned}$$

Dabei wurde die Assoziativität der Multiplikation in \mathbb{R} benutzt. ■

Wir werden später in 2.1.1 diese Regeln als Axiome für einen Vektorraum verwenden. Daher ist es gerechtfertigt, die Menge \mathbb{R}^n mit den so erklärten Verknüpfungen als **Vektorraum** zu bezeichnen.

Die Rechenregeln zeigen auch, dass die etwas pedantische Unterscheidung von $+$, \cdot , $-$ und $+$, \bullet , $-$ ohne Gefahr von Missverständnissen aufgegeben werden kann. Wie üblich wird der Malpunkt meist ganz weggelassen.

Schließlich betrachten wir im \mathbb{R}^n noch die ganz speziellen Vektoren

$$e_1 = (1, 0, \dots, 0), \quad e_2 = (0, 1, 0, \dots, 0), \quad \dots, \quad e_n = (0, \dots, 0, 1).$$

Ist $v = (x_1, \dots, x_n) \in \mathbb{R}^n$ beliebig, so folgt

$$v = x_1 \cdot e_1 + x_2 \cdot e_2 + \dots + x_n \cdot e_n.$$

Man sagt über diese Beziehung, v ist **Linearkombination** von e_1, \dots, e_n und man nennt e_1, \dots, e_n die **kanonischen Basisvektoren** von \mathbb{R}^n ; diese Bezeichnung wird in 2.2.1 gerechtfertigt.

0.1.3 Multiplikation von Vektoren

Bei der Addition im \mathbb{R}^n werden zwei Vektoren addiert, das Ergebnis ist ein Vektor. Die Multiplikation mit Skalaren ist dagegen nicht symmetrisch, es wird ein Vektor mit einer Zahl multipliziert. Daher ist es eine naheliegende Frage, ob man nicht auch zwei Vektoren multiplizieren kann. Rein formal ist das kein Problem, man erklärt im \mathbb{R}^n eine Multiplikation $*$ durch

$$v * w := (x_1 \cdot y_1, \dots, x_n \cdot y_n) \quad \text{für } v = (x_1, \dots, x_n) \quad \text{und } w = (y_1, \dots, y_n).$$

Für $n = 1$ ist das die übliche Multiplikation in \mathbb{R} , aber schon für $n = 2$ hat sie keine unmittelbare geometrische Bedeutung, und vom Standpunkt der Algebra unangenehme Eigenschaften. So ist etwa

$$(1,0) * (0,1) = (0,0) = \mathbf{o}.$$

Die beiden Faktoren sind von Null verschieden, das Produkt ist Null. Solche Faktoren nennt man **Nullteiler**. Weiter hat man in \mathbb{R} eine **Kürzungsregel**: Für $a, x, y \in \mathbb{R}$ und $a \neq 0$ gilt

$$a \cdot x = a \cdot y \quad \Rightarrow \quad x = y.$$

Auch diese Regel ist schon in \mathbb{R}^2 mit $*$ verletzt:

$$(1,0) * (0,1) = (1,0) * (0,0), \quad \text{aber } (0,1) \neq (0,0).$$

Nach diesem problematischen Versuch, im \mathbb{R}^2 eine Multiplikation zu erklären, geben wir noch einen kurzen Ausblick auf höchst nützliche Multiplikationen besserer Art.

Die reelle Ebene \mathbb{R}^2 kann man auch als **komplexe Zahlenebene** ansehen, die entsprechende Multiplikation $*$ ist dann formal gegeben durch

$$(x,y) * (x',y') := (x \cdot x' - y \cdot y', \quad y \cdot x' + x \cdot y').$$

Die geometrische Beschreibung der komplexen Zahlen ist vor allem durch C. F. GAUSS bekannt geworden, darauf kommen wir in 1.3.6 zurück.

Nach langen vergeblichen Versuchen im \mathbb{R}^3 entdeckte W. R. HAMILTON eine Multiplikation in \mathbb{R}^4 mit vielen guten Eigenschaften, die allerdings nicht kommutativ ist. Diese **Quaternionen** werden ausführlich in [EB, Kap. 7] beschrieben.

In 0.3 werden wir noch zwei andere geometrisch relevante Multiplikationen beschreiben. Zunächst für beliebiges n ein **Skalarprodukt**, das ist eine Abbildung

$$\mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$$

und für $n = 3$ ein **Vektorprodukt**

$$\mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}^3$$

mit etwas eigenartigen algebraischen Eigenschaften.

0.2 Geraden

0.2.1 Ausblick

Das zentrale Problem der elementaren linearen Algebra betrifft die Lösung eines Systems linearer Gleichungen der Form

$$\begin{aligned} a_{11}x_1 + \dots + a_{1n}x_n &= b_1, \\ \vdots & \\ a_{m1}x_1 + \dots + a_{mn}x_n &= b_m. \end{aligned} \quad (*)$$

Dabei sind die *Koeffizienten* a_{ij} und b_i vorgegebene (zunächst reelle) Zahlen, die x_1, \dots, x_n sind die *Unbekannten*. Genauer gesagt sind all die Vektoren $(x_1, \dots, x_n) \in \mathbb{R}^n$ gesucht, die alle m Bedingungen des Systems $(*)$ erfüllen. Die Menge $L \subset \mathbb{R}^n$ aller derartigen Lösungen nennt man den *Lösungsraum*. Gesucht ist eine möglichst effiziente Methode, diese Menge L „explizit“ zu beschreiben. Was soll das heißen?

„Implizit“ ist L durch $(*)$ gegeben. Das heißt, man könnte theoretisch alle Vektoren (x_1, \dots, x_n) in $(*)$ einsetzen und prüfen, ob sie alle m Bedingungen erfüllen. Diejenigen, die es tun, kommen zu L , die anderen nicht. Für die Praxis ist diese Idee wertlos, denn dann hätte man viel zu viele Vektoren zu prüfen, und die Wahrscheinlichkeit, dabei einen „guten“ zu finden, wäre gleich Null.

Aber generell sagt man, eine Gleichung sei „gelöst“, wenn man die Lösungen „explizit“ angeben kann. Ist etwa $m = n = 1$, so hat man

$$a \cdot x = b, \quad \text{und} \quad x = \frac{b}{a}, \quad \text{falls} \quad a \neq 0,$$

ist die „explizite“ Lösung. Für allgemeines m und n ist das Problem selbstverständlich viel komplizierter, aber ein nach GAUSS benanntes Eliminationsverfahren zur Lösung wurde im Lauf des 19. Jahrhunderts weiterentwickelt und im 20. Jahrhundert perfektioniert. Das beschreiben wir in 0.5.

In den folgenden Abschnitten behandeln wir zunächst einfache Spezialfälle. Dadurch wird der geometrische Hintergrund klarer, es können nebenbei einige elementargeometrische Fragen durch Vektorrechnung beantwortet werden, und schließlich wird deutlich, dass man für den allgemeinen Fall passende technische Werkzeuge benötigt. Damit beschäftigen sich dann die späteren Kapitel bis zum endgültigen theoretischen Ergebnis in 2.3.5.

0.2.2 Geraden im \mathbb{R}^n

Als Prototyp einer Geraden hatten wir die reelle Zahlengerade \mathbb{R} angesehen. Mit Hilfe der Vektorrechnung kann man sie auch in die Ebene \mathbb{R}^2 , den „Raum“ \mathbb{R}^3 oder ganz

b) Seien $L = v + \mathbb{R} \cdot w \subset \mathbb{R}^n$ und $L' = v' + \mathbb{R} \cdot w' \subset \mathbb{R}^n$ zwei Geraden. Dann gilt $L = L'$ genau dann, wenn

$$L \cap L' \neq \emptyset \quad \text{und es gibt ein} \quad \mu \in \mathbb{R}^*, \quad \text{so dass} \quad w' = \mu w.$$

Kurz ausgedrückt: Den Aufhängepunkt darf man auf der Geraden beliebig verschieben, den Richtungsvektor darf man mit einem beliebigen Faktor $\neq 0$ multiplizieren.

Beweis Die Aussage erscheint geometrisch völlig klar, aber das ist kein Beweis im Sinne der analytischen Geometrie. Hier muss ein Nachweis gefunden werden, der nur die Definitionen und die Rechenregeln für Vektoren benützt. Die geometrische Anschauung kann dabei natürlich Ideen für den Gang der Rechnung geben. Die genaue Ausführung des Beweises ohne zusätzliche Hilfsmittel ist leider etwas mühsam.

Ad a) Zunächst bedeutet $v' \in L$, dass es ein $\lambda' \in \mathbb{R}$ gibt mit $v' = v + \lambda'w$. Setzen wir

$$L' := v' + \mathbb{R} \cdot w,$$

so lautet die Behauptung $L = L'$. Solch eine Gleichheit von Mengen kann man in zwei Schritten beweisen:

$L \subset L'$: Ist $u \in L$, so ist $u = v + \lambda w$ mit einem $\lambda \in \mathbb{R}$. Um zu zeigen, dass auch $u \in L'$ gilt, muss man ein $\alpha \in \mathbb{R}$ finden, so dass $u = v' + \alpha w$. Das folgt aus der einfachen Rechnung

$$u = v + \lambda w = (v' - \lambda'w) + \lambda w = v' + (\lambda - \lambda')w,$$

denn daher kann man $\alpha := \lambda - \lambda'$ setzen.

$L' \subset L$: Mit einer analogen Begründung folgt das aus

$$u = v' + \lambda w = (v + \lambda'w) + \lambda w = v + (\lambda' + \lambda)w.$$

Ad b) Hier sind zwei Richtungen zu beweisen:

„ \Rightarrow “ Sei $L = L'$. Dann ist $L \cap L' \neq \emptyset$ klar. Um den gesuchten Faktor μ zu finden, benutzen wir die Gleichung

$$w' = v' + w' - v'. \quad (*)$$

Da $v' + w' \in L$ und $v' \in L$, gibt es $\lambda, \lambda' \in \mathbb{R}$, so dass

$$v' + w' = v + \lambda w \quad \text{und} \quad v' = v + \lambda'w.$$

Da $w' \neq 0$ ist $v' + w' \neq v'$, also $\lambda \neq \lambda'$. In (*) eingesetzt erhält man

$$w' = v + \lambda w - v - \lambda'w = (\lambda - \lambda')w.$$

Also ist $\mu := \lambda - \lambda' \neq 0$ der gesuchte Faktor.

„ \Leftarrow “ Sei $v^* \in L \cap L'$. Nach Teil a) ist $L = v^* + \mathbb{R} \cdot w$ und $L' = v^* + \mathbb{R} \cdot w'$. Zum Nachweis von $L = L'$ genügen die folgenden Rechnungen:

$$\begin{aligned} L \subset L' : \quad u \in L &\Rightarrow u = v^* + \lambda w = v^* + \frac{\lambda}{\mu} \mu w' \in L'. \\ L' \subset L : \quad u \in L' &\Rightarrow u = v^* + \lambda w' = v^* + \lambda \mu w \in L. \end{aligned}$$

Nach diesen Vorbereitungen ist es klar, wie man eine Gerade durch zwei verschiedene Punkte $v_1, v_2 \in \mathbb{R}^n$ legt. Man wählt einen davon, etwa v_1 , als Aufhängepunkt und $w := v_2 - v_1$ als Richtungsvektor, und man definiert

$$L := v_1 + \mathbb{R} \cdot (v_2 - v_1) = v_1 + \mathbb{R} \cdot w.$$

Dann ist $v_1 = v_1 + 0 \cdot w \in L$ und $v_2 = v_1 + 1 \cdot w \in L$.

Nun ist einfach zu sehen, dass L durch v_1 und v_2 eindeutig bestimmt ist. Angenommen,

$$v_1, v_2 \in L' = v' + \mathbb{R} \cdot w'.$$

Nach Teil a) der obigen Bemerkung können wir $v_1 = v'$ annehmen. Nach Teil b) genügt es zu zeigen, dass $w' = \mu w$ für ein $\mu \in \mathbb{R}^*$. Für v_2 hat man die Darstellungen

$$v_2 = v_1 + 1 \cdot w = v_1 + \lambda w'.$$

Da $w \neq 0$, ist $\lambda \neq 0$ und $w' = \frac{1}{\lambda} w$; also kann man $\mu := \frac{1}{\lambda}$ setzen. Damit ist bewiesen:

Folgerung *Durch zwei verschiedene Punkte des \mathbb{R}^n geht genau eine Gerade.* ■

Bezeichnen $v, w \in \mathbb{R}^n$ die beiden verschiedenen Punkte, so kann man die Gerade $L \subset \mathbb{R}^n$ mit $v, w \in L$ noch etwas einfacher beschreiben. Da $v + \lambda(w - v) = (1 - \lambda)v + \lambda w$, ist

$$\begin{aligned} L &= \{(1 - \lambda)v + \lambda w : \lambda \in \mathbb{R}\} \quad \text{und} \\ [v, w] &:= \{(1 - \lambda)v + \lambda w : \lambda \in [0, 1]\} \end{aligned}$$

ist die **Strecke** zwischen v und w .

Der Leser mag sich wundern, warum so viel Aufwand getrieben wird, um eine scheinbar „klare“ Aussage wie die obige Folgerung nachzuweisen. Aber was eine Gerade ist, erscheint zwar klar, muss aber erst einmal präzise definiert werden, um einem stichhaltigen Beweis zugänglich gemacht zu werden. Wir werden später einige Beispiele dafür geben, dass sich Aussagen, die geometrisch gar nicht so klar sind, durch geschickte Rechnung sehr leicht zeigen lassen. Das ist dann der Lohn für die Mühsal.

Schließlich wollen wir noch erklären, wann zwei Geraden parallel heißen.

Ist $L = v + \mathbb{R} \cdot w \subset \mathbb{R}^n$ eine Gerade, so betrachten wir dazu die Gerade

$$L_0 := \mathbb{R} \cdot w$$

durch den Ursprung \mathbf{o} . Die Geraden $L = v + \mathbb{R} \cdot w$ und $L' = v' + \mathbb{R} \cdot w'$ heißen *parallel*, wenn $\mathbb{R} \cdot w = \mathbb{R} \cdot w'$, in Zeichen

$$L \parallel L' \quad :\Leftrightarrow \quad L_0 = L'_0.$$

Aus Teil b) der obigen Bemerkung folgt, dass parallele Geraden im \mathbb{R}^n mit einem gemeinsamen Punkt gleich sind. Für $n \geq 3$ gibt es nicht parallele Geraden ohne Schnittpunkt, etwa im \mathbb{R}^3

$$L = \mathbb{R} \cdot e_1 \quad \text{und} \quad L' = e_2 + \mathbb{R} \cdot e_3,$$

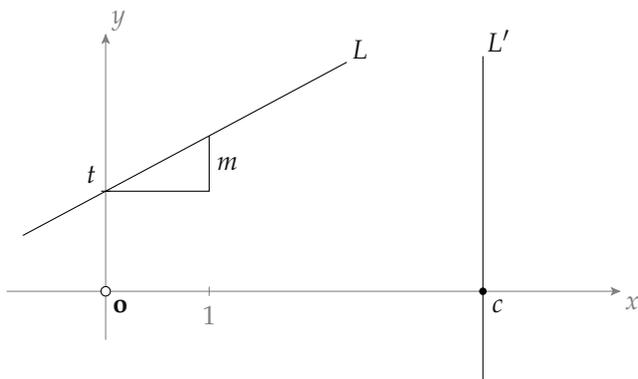
wobei e_1, e_2, e_3 die kanonischen Basisvektoren aus 0.1.2 sind. Darauf kommen wir in 0.3.8 zurück.

0.2.3 Geraden in der Ebene

Geraden im \mathbb{R}^n hatten wir für alle $n \geq 1$ durch eine Parametrisierung beschrieben. Für $n = 2$ kann man das auch durch eine lineare Gleichung erreichen. Dabei bezeichnen wir nach alter Gewohnheit die Koordinaten im \mathbb{R}^2 mit x und y , in Zeichen

$$\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}.$$

Zunächst unterscheiden wir zwei Arten von Geraden:



Die Gerade L hat die Steigung m und den Achsenabschnitt t , sie beschreibt die lineare Funktion

$$y = mx + t.$$

Die Gerade L' hat unendliche Steigung, sie ist beschrieben durch $x = c$. Die allgemeine Form einer solchen Gleichung ist

$$ax + by = c \quad \text{mit} \quad a, b, c \in \mathbb{R}, \quad (a, b) \neq (0, 0).$$

Wir müssen nun nachweisen, dass diese Art von Geraden mit unserer allgemeinen Definition aus 0.2.2 im Fall $n = 2$ verträglich ist. Auch das ist geometrisch ziemlich klar, muss aber dennoch mit Hilfe von präzisen Rechnungen bewiesen werden.

Satz Eine Teilmenge $L \subset \mathbb{R}^2$ ist genau dann eine Gerade, wenn es $a, b, c \in \mathbb{R}$ gibt mit $(a, b) \neq (0, 0)$ derart, dass

$$L = \{(x, y) \in \mathbb{R}^2 : ax + by = c\}.$$

Beweis Zunächst ein Hinweis zur Voraussetzung $(a, b) \neq (0, 0)$. Im Fall $a = b = 0$ lautet die Gleichung $0 = c$. Für die Menge L der Lösungen gilt dann

$$L = \emptyset \quad \text{falls } c \neq 0 \quad \text{und} \quad L = \mathbb{R}^2 \quad \text{falls } c = 0.$$

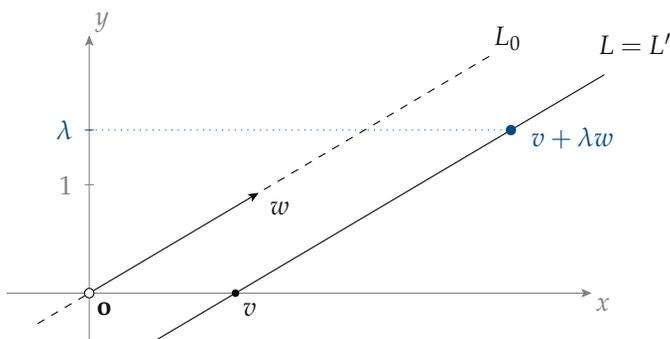
Im *ersten Teil* bestimmen wir aus der Gleichung eine Parametrisierung. Das ist ein Beispiel dafür, wie man eine lineare Gleichung mit den zwei Unbekannten x und y „lösen“ kann (also $n = 2, m = 1$). Wesentlich dabei ist es, dass es viele Lösungen gibt: Der Lösungsraum ist eine Gerade.

Ist $a = 0$, so muss $b \neq 0$ sein und die Gleichung lautet

$$by = c, \quad \text{also} \quad y = \frac{c}{b}.$$

Setzt man $v := (0, \frac{c}{b})$ und $w := (1, 0)$, so ist offensichtlich $L = v + \mathbb{R} \cdot w$.

Ist $a \neq 0$, so setzen wir $y = 0$ und erhalten die Gleichung $ax = c$, also $x = \frac{c}{a}$. Das liefert uns einen Punkt $v := (\frac{c}{a}, 0) \in L$, den wir als Aufhängepunkt wählen können.



Um einen Richtungsvektor w zu finden, setzen wir $c = 0$ und betrachten

$$L_0 := \{(x, y) \in \mathbb{R}^2 : ax + by = 0\}.$$

Offensichtlich ist $\mathbf{o} \in L_0$, und indem wir $y = 1$ setzen, erhalten wir

$$w := \left(-\frac{b}{a}, 1\right) \in L_0.$$

Nun betrachten wir die Gerade $L' := v + \mathbb{R} \cdot w$. Aus der Wahl von v und w folgt, dass der Parameter λ gleich der y -Koordinate des Punktes ist. Daraus folgt leicht $L = L'$:

$L' \subset L$: Ist $(x, y) \in L'$, so gilt

$$(x, y) = v + \lambda w = \left(\frac{c - \lambda b}{a}, \lambda \right).$$

Dieser Punkt erfüllt die Gleichung $ax + by = c$, also $(x, y) \in L$.

$L \subset L'$: Erfüllt (x, y) die Gleichung $ax + by = c$, so folgt wie oben

$$(x, y) = v + yw \in L'.$$

Im *zweiten Teil* müssen wir zu einer Geraden

$$L = v + \mathbb{R} \cdot w \quad \text{mit} \quad v = (x_0, y_0) \quad \text{und} \quad w = (x_1, y_1) \neq (0, 0)$$

eine lineare Gleichung $ax + by = c$ finden. Mit Hilfe einer geometrischen Überlegung suchen wir Kandidaten für die Koeffizienten a, b, c . Ein allgemeiner Punkt von L ist gegeben durch

$$(x, y) = v + \lambda w = (x_0 + \lambda x_1, y_0 + \lambda y_1). \quad (*)$$

Die Steigung der Geraden kann man mit Hilfe eines jeden Punktes $(x, y) \neq (x_0, y_0)$ berechnen als

$$\frac{y - y_0}{x - x_0} = \frac{\lambda y_1}{\lambda x_1} = \frac{y_1}{x_1}.$$

Das gilt zwar nur für $x \neq x_0$ und $x_1 \neq 0$, aber in jedem Fall ist

$$(y - y_0)x_1 = (x - x_0)y_1, \quad \text{also} \quad y_1x - x_1y = x_0y_1 - x_1y_0.$$

Daher setzen wir $a := y_1$, $b := -x_1$ und $c := x_0y_1 - x_1y_0$. Da $w \neq \mathbf{o}$ ist $(a, b) \neq \mathbf{o}$. Ist nun

$$L' := \{(x, y) \in \mathbb{R}^2 : ax + by = c\},$$

so scheint es klar zu sein, dass $L = L'$ gilt. Aber sicherheitshalber muss man es nachrechnen.

$L \subset L'$: Dazu genügt es, die Koordinaten aus $(*)$ in die Gleichung einzusetzen:

$$y_1(x_0 + \lambda x_1) - x_1(y_0 + \lambda y_1) = x_0y_1 - x_1y_0.$$

$L' \subset L$: Zu (x, y) mit $ax + by = c$ muss man ein $\lambda \in \mathbb{R}$ finden, so dass $(x, y) = v + \lambda w$. Aus der Bedingung $y = y_0 + \lambda y_1$ folgt im Fall $a = y_1 \neq 0$, dass

$$\lambda := \frac{y - y_0}{y_1}$$

der passende Parameter sein muss. Durch einfache Rechnung findet man

$$x_0 + \lambda x_1 = \frac{c - by}{a} = x.$$

Ist $a = y_1 = 0$, so ist $b = -x_1 \neq 0$ und eine analoge Rechnung liefert das gleiche Ergebnis. ■

Der gerade bewiesene Satz zeigt, dass es zwei gleichberechtigte, aber sehr verschiedenartige Methoden gibt, eine Gerade im \mathbb{R}^2 zu beschreiben: Durch eine lineare Gleichung oder durch eine Parameterdarstellung. Die Parameterdarstellung kann dabei als die „Lösung“ der linearen Gleichung angesehen werden, weil sie zu jedem Parameter λ genau einen Punkt der Geraden liefert. Der Beweis zeigt auch, dass es etwas Mühe erfordert, das präzise zu begründen.

Man beachte, dass die Lösungsmenge

$$L = \{(x_1, \dots, x_n) \in \mathbb{R}^n : a_1x_1 + \dots + a_nx_n = b\}$$

einer linearen Gleichung mit $(a_1, \dots, a_n) \neq (0, \dots, 0)$ im \mathbb{R}^n für $n \geq 3$ keine Gerade mehr ist. Für $n = 3$ erhält man eine Ebene, für allgemeines n eine so genannte „Hyperebene“.

Wir überlassen dem Leser den Nachweis der folgenden

Bemerkung *Zwei Gleichungen*

$$ax + by = c \quad \text{und} \quad a'x + b'y = c'$$

beschreiben genau dann die gleiche Gerade in \mathbb{R}^2 , wenn es ein $\mu \in \mathbb{R}^$ gibt, so dass*

$$(a', b', c') = \mu \cdot (a, b, c).$$

Zum *Beweis* betrachte man die Steigung und die Schnittpunkte mit den Koordinatenachsen $x = 0$ und $y = 0$. Außerdem kann man die Folgerung aus 0.2.2 benutzen.

0.3 Abstände und Winkel

0.3.1 Das Skalarprodukt im \mathbb{R}^n

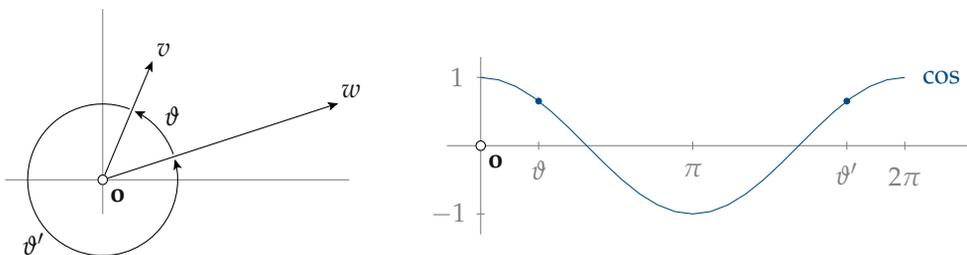
Den Abstand eines Punktes $v = (x_1, x_2) \in \mathbb{R}^2$ vom Ursprung \mathbf{o} kann man nach dem Satz von PYTHAGORAS berechnen. Das ist die **Norm**

$$\|v\| := \sqrt{x_1^2 + x_2^2},$$

oder auch **Länge** des Vektors v . Sind zwei Vektoren $v, w \in \mathbb{R}^2$ gegeben, so kann man versuchen, ein **Skalarprodukt** durch

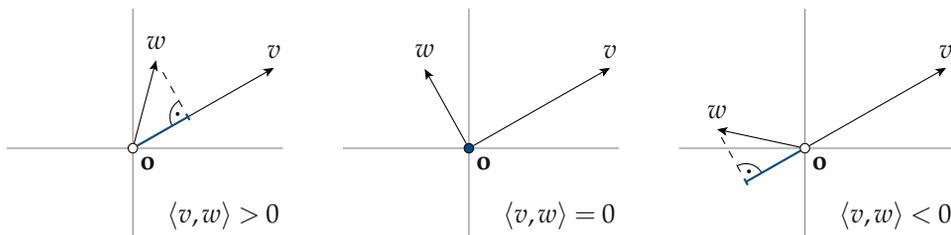
$$\langle v, w \rangle := \|v\| \cdot \|w\| \cdot \cos \vartheta$$

zu erklären, wobei ϑ ein **Winkel** zwischen v und w ist.



Dabei ist es gleichgültig, welchen der beiden Winkel ϑ oder ϑ' man verwendet, denn wegen $\vartheta + \vartheta' = 2\pi$ ist $\cos \vartheta = \cos \vartheta'$. Ist $v = 0$ oder $w = 0$, so gibt es keinen Winkel; dann ist $\langle v, w \rangle = 0$.

Problematisch an dieser geometrischen „Definition“ ist, dass man den Winkel im Bogenmaß und den Cosinus als Wert einer Potenzreihe kennen muss; dazu sind nicht triviale Hilfsmittel aus der Analysis nötig. Aber der Vorteil ist, dass man den Wert von $\langle v, w \rangle$ in Abhängigkeit von $\|v\|, \|w\|$ und ϑ leicht sehen kann. Ist $v \neq 0$, so ist $\|w\| \cdot \cos \vartheta$ die mit Vorzeichen versehene Länge der senkrechten Projektion von w auf die Gerade $\mathbb{R} \cdot v$. Wenn wir v festhalten, gibt es für w drei typische Fälle



Nach diesen Vorbemerkungen geben wir eine formal viel einfachere rein algebraische Definition des Skalarprodukts, die auch im \mathbb{R}^n funktioniert.

Definition Für $v = (x_1, \dots, x_n)$ und $w = (y_1, \dots, y_n) \in \mathbb{R}^n$ heißt

$$\langle v, w \rangle := x_1 \cdot y_1 + \dots + x_n \cdot y_n \in \mathbb{R}$$

das **Skalarprodukt** von v und w .

Vorsicht! Das Skalarprodukt ist eine Abbildung

$$\mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}, \quad (v, w) \mapsto \langle v, w \rangle.$$

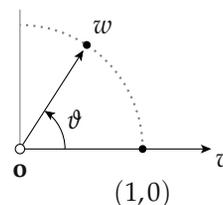
Dagegen ist die *Multiplikation mit Skalaren* aus 0.1.2 eine Abbildung

$$\mathbb{R} \times \mathbb{R}^n \rightarrow \mathbb{R}^n, \quad (\lambda, v) \mapsto \lambda \cdot v.$$

Dass die Definition des Skalarprodukts etwas mit Längen und Winkeln zu tun hat, sieht man sofort am Beispiel $v = (\lambda, 0)$ mit $\lambda > 0$, $w = (\cos \vartheta, \sin \vartheta)$; da ist

$$\|v\| = \lambda, \|w\| = 1 \text{ und}$$

$$\langle v, w \rangle = \lambda \cdot \cos \vartheta = \|v\| \cdot \|w\| \cdot \cos \vartheta.$$



Zunächst notieren wir einige

Rechenregeln für das Skalarprodukt Für $u, v, w \in \mathbb{R}^n$ und $\lambda \in \mathbb{R}$ gilt

- 1) $\langle v, w \rangle = \langle w, v \rangle$
- 2) $\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$
 $\langle \lambda \cdot v, w \rangle = \lambda \cdot \langle v, w \rangle$
- 3) $\langle u, v + w \rangle = \langle u, v \rangle + \langle u, w \rangle$
 $\langle u, \lambda \cdot v \rangle = \lambda \cdot \langle u, v \rangle$
- 4) $\langle v, v \rangle \geq 0$, und es gilt $\langle v, v \rangle = 0 \Leftrightarrow v = \mathbf{o}$

Beweis 1) bis 3) erfordert nur elementare Rechnungen. Auch 4) ist ganz einfach: Ist $v = (x_1, \dots, x_n)$, so folgt

$$\langle v, v \rangle = x_1^2 + \dots + x_n^2 \geq 0 \quad \text{und} \quad \langle v, v \rangle = 0 \Leftrightarrow x_1 = \dots = x_n = 0$$

nach den Regeln für Quadrate in \mathbb{R} (vgl. 0.1.1). ■

Vorsicht! Für das Skalarprodukt gilt keine Kürzungsregel, d.h. aus $\langle v, w \rangle = \langle v, w' \rangle$ folgt nicht $w = w'$. Als Beispiel betrachte man $v = (1, 0)$, $w = (0, 1)$ und $w' = (0, 2)$ im \mathbb{R}^2 .

Wie wir gesehen haben, hängt das Skalarprodukt $\langle v, v \rangle$ mit dem Satz des PYTHAGORAS zusammen. So definiert man für $v = (x_1, \dots, x_n) \in \mathbb{R}^n$ die **Norm** von v durch

$$\|v\| := \sqrt{\langle v, v \rangle} = \sqrt{x_1^2 + \dots + x_n^2}.$$

Aus den obigen Regeln für das Skalarprodukt folgen sofort

Rechenregeln für die Norm Für $v \in \mathbb{R}^n$ und $\lambda \in \mathbb{R}$ gilt

$$\mathbf{1)} \quad \|\lambda \cdot v\| = |\lambda| \cdot \|v\|. \quad \mathbf{2)} \quad \|v\| = 0 \Leftrightarrow v = \mathbf{o}.$$

Nun kann man als **Abstand** zwischen v und w aus \mathbb{R}^n die Norm der Differenz erklären, in Zeichen

$$d(v, w) := \|w - v\|.$$

Ist $v = (x_1, \dots, x_n)$ und $w = (y_1, \dots, y_n)$, so ist

$$d(v, w) = \sqrt{(y_1 - x_1)^2 + \dots + (y_n - x_n)^2}.$$

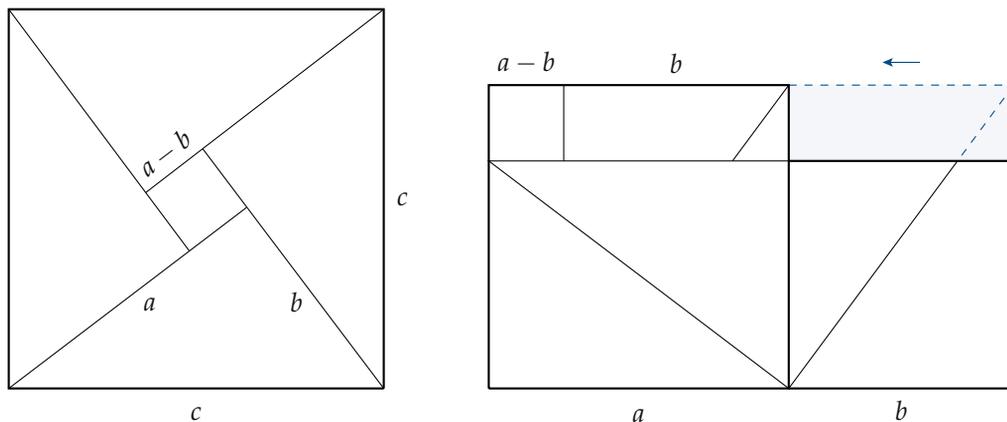
Schließlich noch eine nützliche Bezeichnung. Ein Vektor $v \in \mathbb{R}^n$ heißt **normiert**, wenn $\|v\| = 1$. Man kann einen beliebigen Vektor $\mathbf{o} \neq v \in \mathbb{R}^n$ normieren zu

$$v_1 := \frac{1}{\|v\|} \cdot v \quad \text{mit} \quad \|v_1\| = \frac{1}{\|v\|} \cdot \|v\| = 1.$$

0.3.2 Anwendungen in der Elementargeometrie

Nun wollen wir anhand von einigen klassischen Beispielen zeigen, wie sich einfache Aussagen über Längen und Abstände mit Hilfe der in 0.3.1 bereitgestellten Rechenregeln sehr kurz und präzise beweisen lassen. Dabei ist zu bedenken, dass der klassische Satz des PYTHAGORAS stets implizit verwendet wird, weil Abstände auf seiner Grundlage definiert sind.

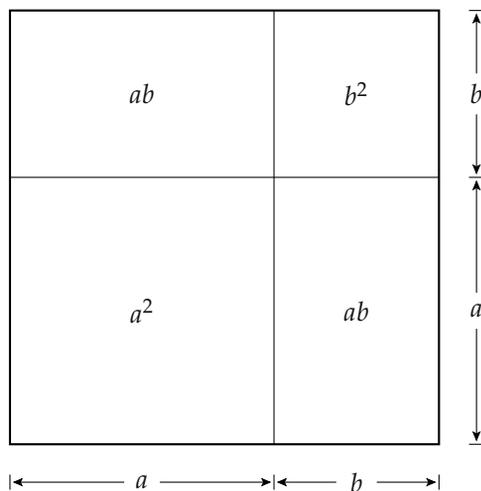
Besonders schön ist ein *Beweis* des **Satzes von PYTHAGORAS**, der auf indische Quellen aus dem 12. Jahrhundert zurückgeht:



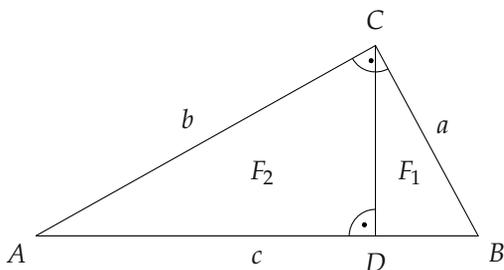
Man kann die Beziehung $c^2 = a^2 + b^2$ an dem Bild ablesen, aber auch mit Hilfe der Binomischen Formel nachrechnen: Zwei rechtwinklige Dreiecke mit den Seiten a, b, c ergeben zusammen ein Rechteck der Fläche $a \cdot b$, das kleine Quadrat in der Mitte hat die Kantenlänge $a - b$. Also folgt aus dieser Zerlegung

$$c^2 = 2ab + (a - b)^2 = a^2 + b^2. \quad \blacksquare$$

Dabei sei bemerkt, dass man die Formel $(a + b)^2 = a^2 + 2ab + b^2$ auch geometrisch einsehen kann:



Von den zahllosen Beweisen des Satzes von PYTHAGORAS sei noch ein weiterer erwähnt, den A. EINSTEIN als elfjähriger Schüler gefunden haben soll. Er zeichnet sich dadurch aus, dass er mit einer einzigen Hilfslinie auskommt.



Ist D der Fußpunkt des Lotes von C auf die Strecke AB , so sind die Dreiecke ABC , BCD , und ADC ähnlich, also sind die Flächen proportional zu den Quadraten der Hypotenusen, d.h.

$$\frac{F_1 + F_2}{c^2} = \frac{F_1}{a^2} = \frac{F_2}{b^2} =: \rho > 0.$$

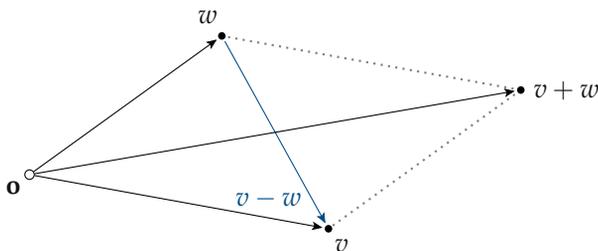
Daraus folgt $\rho c^2 = F_1 + F_2 = \rho a^2 + \rho b^2$ und $c^2 = a^2 + b^2$. ■

Nun zu den versprochenen Anwendungen:

Parallelogramm-Gesetz In einem Parallelogramm ist die Summe der Quadrate der vier Seiten gleich der Summe der Quadrate der zwei Diagonalen.

Mit Hilfe von Vektoren im \mathbb{R}^2 formuliert lautet es so: Für $v, w \in \mathbb{R}^2$ gilt

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



Der Beweis mit Hilfe der Rechenregeln für das Skalarprodukt ist ganz einfach:

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

■

Mit der gleichen Rechnung sieht man, dass

$$\|v + w\| = \|v - w\| \quad \Leftrightarrow \quad \langle v, w \rangle = 0.$$

Wie wir im nächsten Abschnitt sehen werden, bedeutet $\langle v, w \rangle = 0$, dass v und w senkrecht stehen. Daher kann man Rechtecke auf die Genauigkeit der rechten Winkel durch Vermessung der Diagonalen prüfen. Diese Methode kennt jeder gute Handwerker.

Sind zwei verschiedene Punkte $v, w \in \mathbb{R}^n$ gegeben, so kann man auf der Geraden durch v und w den Mittelpunkt u suchen. Da er auf der Geraden durch v und w liegt, ist

$$u = v + \lambda(w - v) = (1 - \lambda)v + \lambda w \quad \text{für ein } \lambda \in \mathbb{R}.$$

Da u Mittelpunkt sein soll, muss $\|u - v\| = \|u - w\|$ sein. Nun ist

$$u - v = \lambda(w - v) \quad \text{und} \quad u - w = (\lambda - 1)(w - v),$$

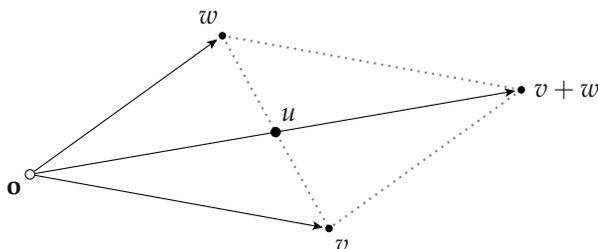
also muss $|\lambda| = |\lambda - 1|$ sein, das geht nur für $\lambda = \frac{1}{2}$. Somit ist

$$u := \frac{1}{2}(v + w)$$

der gesuchte **Mittelpunkt** zwischen v und w und

$$d(u, v) = d(u, w) = \frac{1}{2}\|w - v\|.$$

Im \mathbb{R}^2 kann man das in einem Parallelogramm interpretieren:



Geometrisch gesehen erhält man damit den

Diagonalen-Satz *In einem Parallelogramm schneiden sich die Diagonalen in ihren Mittelpunkten.* ■

Ist ein Dreieck im \mathbb{R}^2 durch die Ecken v_1, v_2, v_3 gegeben, so nennt man

$$s := \frac{1}{3}(v_1 + v_2 + v_3)$$

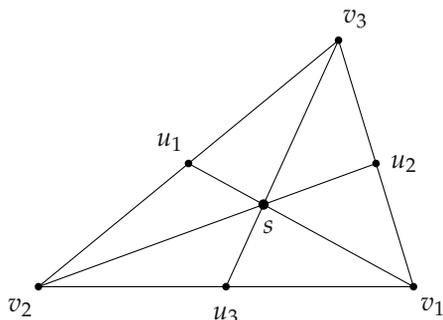
den **Schwerpunkt**. Das ist der Schwerpunkt im physikalischen Sinn, wenn an den drei Ecken gleiche Gewichte befestigt werden.

Schwerpunkt-Satz Die Seitenhalbierenden eines Dreiecks schneiden sich im Schwerpunkt.

Beweis Wie oft in der analytischen Geometrie kann man die Rechnung stark vereinfachen, wenn man die Koordinaten passend wählt. In diesem Fall geht das etwa mit

$$v_1 = (a, 0), \quad v_2 = (-a, 0) \quad \text{und} \quad v_3 = (b, c),$$

wobei $a, b, c \in \mathbb{R}$ mit $a > 0$ und $c > 0$.



Daraus erhält man

$$s = \frac{1}{3}(b, c), \quad u_1 = \frac{1}{2}(b - a, c), \quad u_2 = \frac{1}{2}(a + b, c), \quad u_3 = (0, 0).$$

Dass s auf den drei Seitenhalbierenden liegt, folgt aus

$$s = \frac{1}{3}v_1 + \frac{2}{3}u_1 = \frac{1}{3}v_2 + \frac{2}{3}u_2 = \frac{1}{3}v_3 + \frac{2}{3}u_3,$$

was man ganz leicht nachrechnen kann. ■

Natürlich gibt es auch andere Wahlen der Koordinaten, mit denen die Rechnung vereinfacht werden kann, etwa

$$s = (0, 0) \quad \text{und} \quad v_1 = (0, a).$$

Der Leser möge das zur Übung ausführen.

0.3.3 Winkel im \mathbb{R}^n

Schon in 0.3.1 hatten wir darauf hingewiesen, dass die „naive“ Definition des Skalarproduktes

$$\langle v, w \rangle = \|v\| \cdot \|w\| \cdot \cos \vartheta \tag{*}$$

problematisch ist, weil sie die Kenntnis des Winkels im Bogenmaß erfordert. Für die Theorie ist es geschickter, die algebraischen Definitionen von Skalarprodukt und Norm voranzustellen, und dann den Winkel so zu erklären, dass die Gleichung (*) erfüllt ist. Bei diesem Kniff gibt es eine Hürde, die überwunden wird durch die

Ungleichung von CAUCHY-SCHWARZ Für $v, w \in \mathbb{R}^n$ gilt $|\langle v, w \rangle| \leq \|v\| \cdot \|w\|$.

Als unmittelbare Folgerung erhält man die Ungleichungen

$$-1 \leq \frac{\langle v, w \rangle}{\|v\| \cdot \|w\|} \leq 1,$$

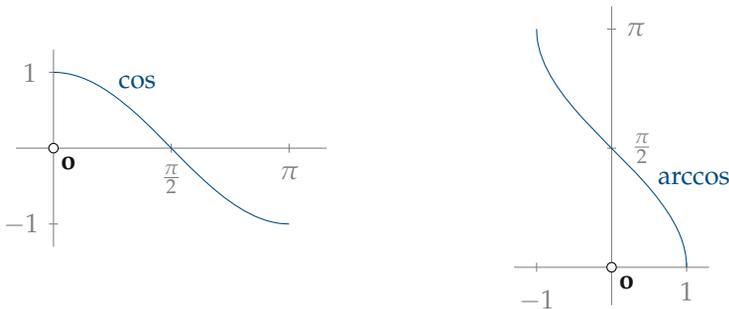
falls $v \neq \mathbf{o}$ und $w \neq \mathbf{o}$. Also gibt es in diesem Fall genau ein $\vartheta \in [0, \pi]$, so dass

$$\cos \vartheta = \frac{\langle v, w \rangle}{\|v\| \cdot \|w\|}, \quad \text{d.h.} \quad \vartheta := \arccos \frac{\langle v, w \rangle}{\|v\| \cdot \|w\|}$$

kann man als **Winkel** zwischen v und w , in Zeichen

$$\angle(v, w) := \arccos \frac{\langle v, w \rangle}{\|v\| \cdot \|w\|} \in [0, \pi]$$

erklären.



Man beachte bei dieser Definition des Winkels, welche Hilfsmittel aus der Analysis zur Berechnung nötig sind: Man muss Wurzeln ziehen und man benötigt die Potenzreihe des Arcuscosinus.

Offensichtlich ist $\angle(v, w) = \angle(w, v)$, der so erklärte Winkel ist also „nicht orientiert“. Wollte man das auch noch berücksichtigen, müsste man prüfen, wie weit v in einer festzulegenden Richtung gedreht werden muss, bis w erreicht ist.

Insgesamt ergibt sich – jetzt präzise begründet – für das **Skalarprodukt** von $v, w \in \mathbb{R}^n$ die Formel

$$\langle v, w \rangle = \|v\| \cdot \|w\| \cdot \cos \angle(v, w).$$

Insbesondere können wir nun sagen, wann v und w aus \mathbb{R}^n *senkrecht* stehen:

$$v \perp w \Leftrightarrow \langle v, w \rangle = 0.$$

Für $v \neq 0$ und $w \neq 0$ bedeutet das $\angle(v, w) = \frac{\pi}{2}$, der Nullvektor steht nach Definition auf jedem anderen senkrecht.

Was nun nachgeholt werden muss, ist der

Beweis der Cauchy-Schwarzschen-Ungleichung (kurz „CSU“)

Die Ungleichung ist von der Form $a \leq b$ mit $a, b \in \mathbb{R}_+$. Da die Quadratwurzel eine monotone Funktion ist, genügt es dazu, $a^2 \leq b^2$, also $b^2 - a^2 \geq 0$ zu zeigen.

Für $n = 1$ ist $v = x$ und $w = y$, also

$$|\langle v, w \rangle| = |x \cdot y| = |x| \cdot |y| = \|x\| \cdot \|y\|.$$

Für $n = 2$ muss man etwas mehr rechnen. Ist $v = (x_1, x_2)$ und $w = (y_1, y_2)$, so folgt

$$\|v\|^2 \cdot \|w\|^2 - \langle v, w \rangle^2 = (x_1^2 + x_2^2)(y_1^2 + y_2^2) - (x_1y_1 + x_2y_2)^2 = (x_1y_2 - x_2y_1)^2 \geq 0.$$

Für $n = 3$ werden wir in 0.3.6 einen Beweis geben, bei dem auch der Wert von

$$\|v\|^2 \cdot \|w\|^2 - \langle v, w \rangle^2$$

geometrisch interpretiert wird.

Für allgemeines n wird die Rechnung mit den Koordinaten zu kompliziert, hier hilft ein Trick. Im Fall $w = \mathbf{o}$ sind beide Seiten gleich Null; es genügt also, den Fall $w \neq \mathbf{o}$ zu behandeln, wir setzen

$$\lambda := \langle w, w \rangle > 0 \quad \text{und} \quad \mu := -\langle v, w \rangle.$$

Dann ist

$$\begin{aligned} 0 &\leq \langle \lambda v + \mu w, \lambda v + \mu w \rangle = \lambda^2 \langle v, v \rangle + 2\lambda\mu \langle v, w \rangle + \mu^2 \langle w, w \rangle \\ &= \lambda(\langle v, v \rangle \cdot \langle w, w \rangle - 2\langle v, w \rangle^2 + \langle v, w \rangle^2) = \lambda(\langle v, v \rangle \cdot \langle w, w \rangle - \langle v, w \rangle^2). \end{aligned}$$

Da $\lambda > 0$ folgt daraus $\langle v, v \rangle \cdot \langle w, w \rangle - \langle v, w \rangle^2 \geq 0$ und wegen der Monotonie der Quadratwurzel erhält man die behauptete Ungleichung. ■

Mit der Frage, wann die Ungleichung von CAUCHY-SCHWARZ eine Gleichung ist, beschäftigen wir uns in 0.3.6 und 0.3.7. Aus dem obigen Beweis halten wir schon einmal fest, dass für $w \neq \mathbf{o}$ und $\lambda = \langle w, w \rangle > 0$ gilt, dass

$$\|\lambda v + \mu w\|^2 = \lambda(\|v\|^2 \cdot \|w\|^2 - \langle v, w \rangle^2), \text{ also}$$

$$\|v\|^2 \cdot \|w\|^2 = \langle v, w \rangle^2 \Leftrightarrow \lambda v + \mu w = \mathbf{o}.$$

Der klassische Satz von PYTHAGORAS gilt im rechtwinkligen Dreieck. Als Verallgemeinerung erhält man einen

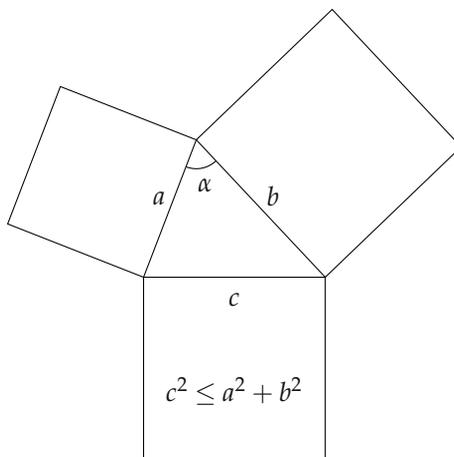
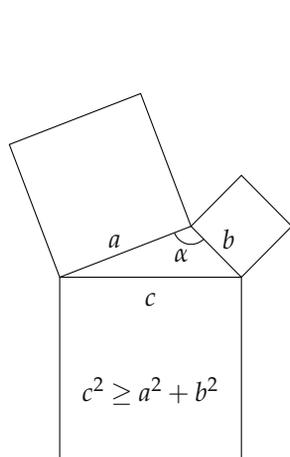
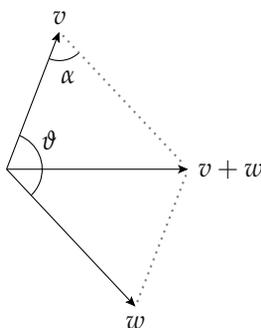
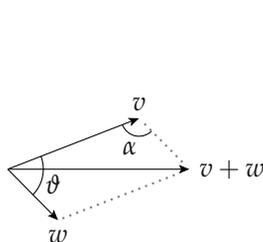
Satz nach PYTHAGORAS Für $v, w \in \mathbb{R}^n$ gilt

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

insbesondere $\|v + w\|^2 = \|v\|^2 + \|w\|^2$, falls $v \perp w$.

Die Abweichung vom rechtwinkligen Fall ist also durch den Term $2\langle v, w \rangle$ gegeben. Nach der Definition des Winkels $\vartheta = \angle(v, w)$ und $\alpha := \pi - \vartheta$ kann man zwei Fälle unterscheiden:

$$0 \leq \vartheta \leq \frac{\pi}{2}, \pi \geq \alpha \geq \frac{\pi}{2}, \langle v, w \rangle \geq 0 \quad \Bigg| \quad \frac{\pi}{2} \leq \vartheta \leq \pi, \frac{\pi}{2} \geq \alpha \geq 0, \langle v, w \rangle \leq 0$$



Geometrisch ist das klar: Wenn man bei festem a und b den Winkel α kleiner macht, wird c kürzer und umgekehrt. Der *Beweis* ist ganz einfach:

$$\|v + w\|^2 = \langle v + w, v + w \rangle = \langle v, v \rangle + \langle w, w \rangle + 2\langle v, w \rangle = \|v\|^2 + \|w\|^2 + 2\langle v, w \rangle \quad \blacksquare$$

Da $\langle v, w \rangle = \|v\| \cdot \|w\| \cdot \cos \vartheta$ und $\cos \vartheta = -\cos \alpha$, kann man die obige Gleichung auch in der Form

$$c^2 = a^2 + b^2 - 2ab \cos \alpha$$

schreiben. Das ist der sogenannte *Cosinussatz*.

Da nach der Cauchy-Schwarzschen-Ungleichung auch $\langle v, w \rangle \leq \|v\| \cdot \|w\|$ gilt, ergibt obige Rechnung die Abschätzung

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

Wieder wegen der Monotonie der Quadratwurzel folgt daraus die

Dreiecksungleichung für die Norm Für $v, w \in \mathbb{R}^n$ gilt $\|v + w\| \leq \|v\| + \|w\|$. ■

An der obigen Rechnung erkennt man auch, dass

$$\|v + w\| = \|v\| + \|w\| \Leftrightarrow \langle v, w \rangle = \|v\| \cdot \|w\| \Leftrightarrow \angle(v, w) = 0.$$

Ist $v = \mathbf{o}$ oder $w = \mathbf{o}$, so ist das stets der Fall. Sind v, w beide von \mathbf{o} verschieden, so ist $\angle(v, w) = 0$ gleichbedeutend damit, dass

$$w = \mu v \quad \text{mit} \quad \mu > 0.$$

Mit Hilfe des in 0.3.1 eingeführten Abstandes d erhält man die

Dreiecksungleichung für den Abstand Für $v_1, v_2, v_3 \in \mathbb{R}^n$ gilt

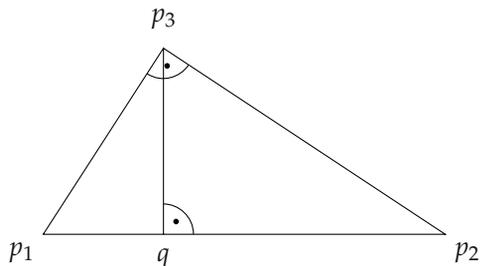
$$d(v_1, v_3) \leq d(v_1, v_2) + d(v_2, v_3).$$

Zum *Beweis* genügt es $v := v_2 - v_1$ und $w := v_3 - v_2$ zu setzen. Dann ist $v + w = v_3 - v_1$, also

$$d(v_1, v_3) = \|v + w\| \leq \|v\| + \|w\| = d(v_1, v_2) + d(v_2, v_3). \quad \blacksquare$$

Informell ausgedrückt besagt die Dreiecksungleichung, dass man durch einen Umweg nichts einsparen kann. Offenbar gilt die Gleichheit genau dann, wenn v_2 zwischen v_1 und v_3 liegt.

Wir geben noch zwei Beispiele dafür, wie man mit Hilfe des Skalarproduktes Sätze der Elementargeometrie einfach beweisen kann. Der erste betrifft ein rechtwinkliges Dreieck.



Höhensatz im rechtwinkligen Dreieck Ist q der Fußpunkt des Lotes von p_3 auf die Hypotenuse, so gilt

$$d(p_3, q)^2 = d(p_1, q) \cdot d(p_2, q).$$

Anders ausgedrückt: Das Quadrat der Höhe ist gleich dem Produkt der Hypotenusenabschnitte.

Beweis Wir können die Koordinaten so wählen, dass

$$q = (0, 0), \quad p_1 = (-\alpha, 0), \quad p_2 = (\beta, 0) \quad \text{und} \quad p_3 = (0, \gamma) \quad \text{mit} \quad \alpha, \beta, \gamma > 0.$$

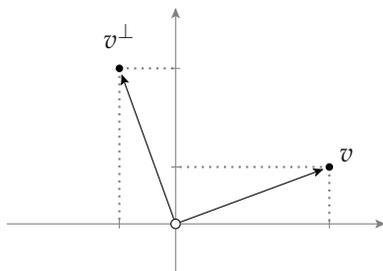
Da das Dreieck rechtwinklig ist, gilt

$$(0, \gamma) - (-\alpha, 0) = (\alpha, \gamma) \perp (-\beta, \gamma) = (0, \gamma) - (\beta, 0), \quad \text{also}$$

$$0 = \langle (\alpha, \gamma), (-\beta, \gamma) \rangle = -\alpha \cdot \beta + \gamma^2 \quad \text{und} \quad \gamma^2 = \alpha \cdot \beta.$$

■

Ist $v = (x, y) \in \mathbb{R}^2$, so definieren wir einen dazu senkrechten Vektor $v^\perp := (-y, x) \in \mathbb{R}^2$.



Offensichtlich gilt $\langle v, v^\perp \rangle = 0$ und $\|v^\perp\| = \|v\|$, v^\perp steht also senkrecht zu v und hat die gleiche Länge. Dass neben v^\perp nur noch $-v^\perp$ diese beiden Eigenschaften hat, folgt aus der

Bemerkung Ist $w = (a, b) \in \mathbb{R}^2$ mit $w \neq \mathbf{o}$ gegeben, so gilt für $s = (x, y)$

$$s \perp w \Leftrightarrow s = \lambda(-b, a) \quad \text{mit} \quad \lambda \in \mathbb{R}.$$

Beweis Nach Definition gilt

$$s \perp w \Leftrightarrow \langle s, w \rangle = 0 \Leftrightarrow ax + by = 0.$$

„ \Leftarrow “ ist klar, denn $\langle (a, b), \lambda(-b, a) \rangle = 0$.

„ \Rightarrow “ Sei $ax + by = 0$ und $a \neq 0$. Dann folgt $x = -\frac{b}{a}y$. Setzt man ein beliebiges y in der Form $y = \lambda a$ ein, so ergibt sich

$$x = -\lambda b, \quad \text{also} \quad (x, y) = (-\lambda b, \lambda a) = \lambda(-b, a).$$

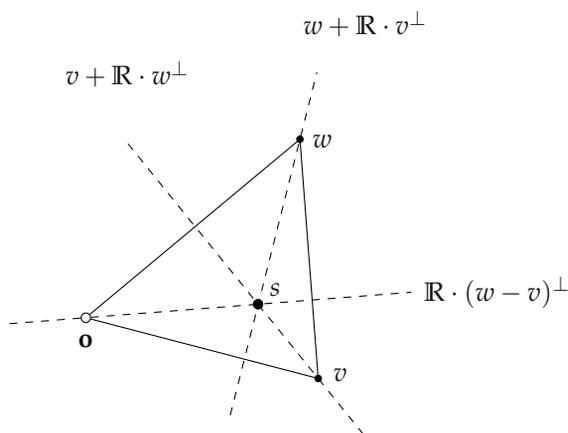
Ist $a = 0$, so folgt $b \neq 0$, und eine analoge Rechnung liefert das Ergebnis. ■

Diese Bemerkung bedeutet, dass es im \mathbb{R}^2 zur Geraden $L = \mathbb{R} \cdot (a, b)$ nur eine zu L senkrechte Gerade durch \mathbf{o} gibt, nämlich $\mathbb{R} \cdot (-b, a)$. In höheren Dimensionen gibt es natürlich mehr senkrechte Geraden.

Nach dieser Vorbereitung kommen wir zum zweiten Beispiel.

Höhenschnittpunkt-Satz *In einem Dreieck schneiden sich die drei Höhen in einem Punkt.*

Beweis Wir können das Dreieck so legen, dass eine Ecke im Ursprung \mathbf{o} liegt; die beiden anderen Ecken sind gegeben durch die Vektoren v und w , die nicht Vielfache voneinander sind.



Die Höhen des Dreiecks liegen dann auf den Geraden

$$v + \mathbb{R} \cdot w^\perp, \quad w + \mathbb{R} \cdot v^\perp \quad \text{und} \quad \mathbb{R} \cdot (w - v)^\perp.$$

Die Geraden $v + \mathbb{R} \cdot w^\perp$ und $w + \mathbb{R} \cdot v^\perp$ haben einen Schnittpunkt s , also ist

$$s = v + \lambda w^\perp = w + \mu v^\perp \quad \text{mit} \quad \lambda, \mu \in \mathbb{R}.$$

Es bleibt zu zeigen, dass $s \in \mathbb{R} \cdot (w - v)^\perp$, d.h. $\langle s, w - v \rangle = 0$. Dazu berechnen wir

$$\langle s, w \rangle = \langle v + \lambda w^\perp, w \rangle = \langle v, w \rangle \quad \text{und} \quad \langle s, v \rangle = \langle w + \mu v^\perp, v \rangle = \langle w, v \rangle.$$

Also ist $\langle s, w - v \rangle = \langle s, w \rangle - \langle s, v \rangle = 0$. ■

0.3.4 Senkrechte Vektoren und Abstände

Den Abstand zwischen v und w im \mathbb{R}^n hatten wir in 0.3.1 erklärt durch

$$d(v, w) := \|w - v\|.$$

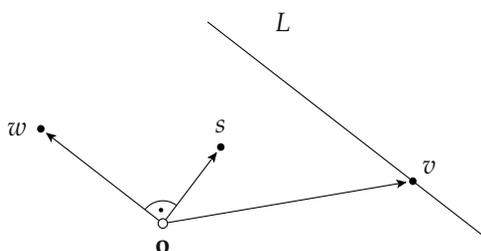
Ist nun $L \subset \mathbb{R}^n$ eine Gerade und $v' \in \mathbb{R}^n$, so ist der Abstand von v' und L erklärt durch

$$d(v', L) := \min\{d(v', u) : u \in L\}$$

als minimaler Abstand von v' zu den Punkten von L . Es ist geometrisch ziemlich klar, dass ein Punkt $u_0 \in L$ mit minimalem Abstand zu v' eindeutig bestimmt ist. Mit den Hilfsmitteln der linearen Algebra ist das einfach zu beweisen. Dazu erklären wir, wann ein Vektor *senkrecht* auf einer Geraden steht: Ist $L = v + \mathbb{R} \cdot w \subset \mathbb{R}^n$ eine Gerade und $s \in \mathbb{R}^n$, so sei

$$s \perp L \quad :\Leftrightarrow \quad s \perp w, \quad \text{d.h.} \quad \langle s, w \rangle = 0.$$

Mit Teil b) der Bemerkung aus 0.2.2 sieht man sofort, dass diese Definition bei festem L unabhängig von der Auswahl von w ist.



Lemma Der senkrechte Abstand eines Punktes v' von einer Geraden L im \mathbb{R}^n ist der kürzeste. Genauer gilt

- Es gibt genau ein $u_0 \in L$, so dass $(u_0 - v') \perp L$.
- $d(v', L) = d(v', u_0)$.

Man nennt dieses u_0 den *Fußpunkt* des Lotes von v' auf L .

Beweis Ist $L = v + \mathbb{R} \cdot w$, so lauten die Bedingungen für u_0 :

$$u_0 = v + \lambda_0 w \quad \text{mit} \quad \lambda_0 \in \mathbb{R} \quad \text{und} \quad \langle u_0 - v', w \rangle = 0.$$

Fasst man sie zusammen, so erhält man

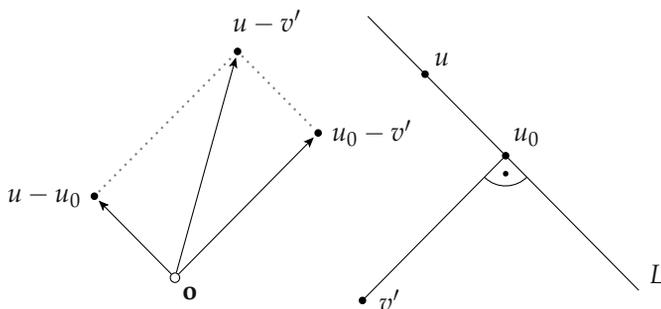
$$0 = \langle u_0 - v', w \rangle = \langle v + \lambda_0 w - v', w \rangle = \langle v - v', w \rangle + \lambda_0 \langle w, w \rangle,$$

also folgt

$$\lambda_0 = \frac{\langle v' - v, w \rangle}{\langle w, w \rangle}, \quad \text{denn} \quad \langle w, w \rangle \neq 0.$$

Dieses λ_0 ist die eindeutige Lösung der durch die Bedingungen an u_0 erhaltenen Gleichung, also ist auch u_0 eindeutig bestimmt.

Zum Beweis der Minimalität haben wir $d(v', u_0)$ mit $d(v', u)$ für ein beliebiges $u \in L$ zu vergleichen:



Da $(u - u_0) \perp (u_0 - v')$, ist nach dem Satz von PYTHAGORAS

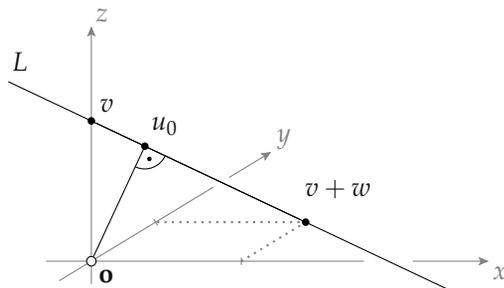
$$d(v', u)^2 = \|u - v'\|^2 = \|u_0 - v'\|^2 + \|u - u_0\|^2 \geq \|u_0 - v'\|^2 = d(v', u_0)^2,$$

und die Behauptung $d(v', u_0) \leq d(v', u)$ folgt aus der Monotonie der Quadratwurzel. ■

Aus dem obigen Beweis kann man sofort ein Verfahren zur Berechnung des Abstandes herleiten. Wir geben ein ganz einfaches

Beispiel Ist $v := (0, 0, 1)$, $w := (1, 1, -1)$ und $v' := (0, 0, 0)$ im \mathbb{R}^3 , so erhält man

$$\lambda_0 = \frac{1}{3}, \quad u_0 = \frac{1}{3}(1, 1, 2) \quad \text{und} \quad d(v', L) = \|u_0\| = \frac{1}{3}\sqrt{6} = 0.816\dots$$



0.3.5 Die HESSEsche Normalform einer Geradengleichung

Wir wollen nun die Gleichung einer Geraden im \mathbb{R}^2 vom Standpunkt des Skalarprodukts betrachten. Der einfachste Fall ist eine Gerade

$$L = \{(x, y) \in \mathbb{R}^2 : ax + by = 0\}$$

durch den Ursprung. Die naheliegende Idee ist es nun, nicht nur Punkte $v = (x, y) \in \mathbb{R}^2$, sondern auch das Paar a, b der Koeffizienten als Vektor $s := (a, b) \in \mathbb{R}^2$ zu betrachten, wobei nach der allgemeinen Voraussetzung $(a, b) \neq (0, 0)$ ist. Dann gilt offensichtlich

$$v \in L \Leftrightarrow ax + by = 0 \Leftrightarrow \langle s, v \rangle = 0,$$

d.h. wenn v senkrecht zu s ist. Der Wert von $\langle s, v \rangle$ hat aber für alle Punkte $v \in \mathbb{R}^2$ eine geometrische Bedeutung. Sie wird besonders einfach, wenn s normiert wird, d.h. man betrachtet

$$s_1 := \frac{1}{\|s\|} \cdot s = (a_1, b_1) \quad \text{mit} \quad a_1 := \frac{a}{\sqrt{a^2 + b^2}} \quad \text{und} \quad b_1 := \frac{b}{\sqrt{a^2 + b^2}}.$$

Um für einen beliebigen Punkt $v \in \mathbb{R}^2$ den Abstand $d(v, L)$ zu bestimmen, genügt es, den eindeutig bestimmten Fußpunkt $v_0 \in L$ zu bestimmen mit $(v - v_0) \perp L$. Dann ist nach dem Lemma aus 0.3.4

$$d(v, L) = \|v - v_0\|.$$

Nach der Bemerkung aus 0.2.3 sind die Koeffizienten a, b der Geradengleichung bis auf einen gemeinsamen Faktor eindeutig bestimmt. Für ein beliebiges $u \in \mathbb{R}^2$ gilt daher

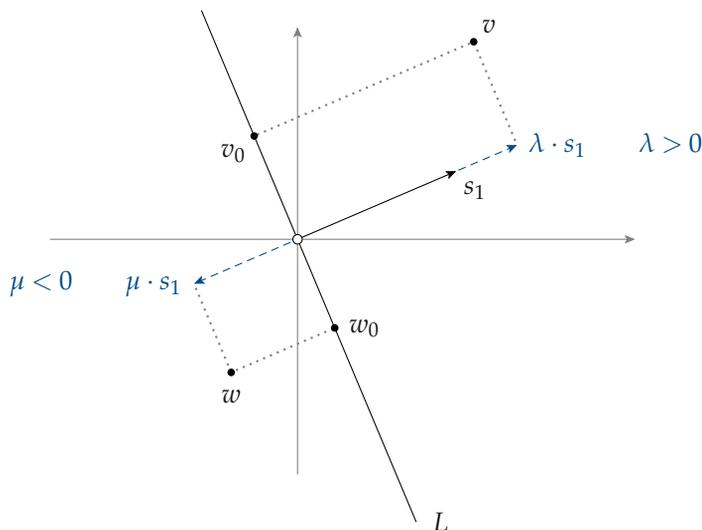
$$u \perp L \Leftrightarrow u = \lambda \cdot s_1 \quad \text{mit} \quad \lambda \in \mathbb{R}.$$

Setzt man $u = v - v_0$, so folgt $v - v_0 = \lambda s_1$ und $v_0 = v - \lambda s_1$. Wegen $v_0 \in L$ und $\langle s_1, s_1 \rangle = 1$ ist

$$0 = \langle s_1, v_0 \rangle = \langle s_1, v - \lambda s_1 \rangle = \langle s_1, v \rangle - \lambda, \quad \text{also} \quad \lambda = \langle s_1, v \rangle.$$

Schließlich erhält man mit $v = (x, y)$

$$d(v, L) = \|v - v_0\| = |\lambda| = |\langle s_1, v \rangle| = |a_1 x + b_1 y|.$$



Der Betrag des Skalarproduktes $\langle s_1, v \rangle$ gibt also den Abstand von v zu L an; v liegt genau dann auf L , wenn der Abstand gleich Null ist. Aber das Skalarprodukt $\langle s_1, v \rangle$ hat auch ein Vorzeichen: Ist $\langle s_1, v \rangle > 0$, so liegt v in Richtung von s_1 , ist $\langle s_1, w \rangle < 0$, so liegt w in der entgegengesetzten Richtung.

Nach diesen Vorüberlegungen betrachten wir eine beliebige Gerade

$$L = \{(x, y) \in \mathbb{R}^2 : ax + by = c\}, \quad (a, b) \neq (0, 0).$$

Wir können die Koeffizienten a, b, c ersetzen durch

$$a_1 := \frac{a}{\sqrt{a^2 + b^2}}, \quad b_1 := \frac{b}{\sqrt{a^2 + b^2}}, \quad \text{und} \quad c_1 := \frac{c}{\sqrt{a^2 + b^2}}, \quad (1)$$

erhalten also für L die neue Gleichung

$$a_1 x + b_1 y = c_1. \quad (*)$$

Dies Gleichung $(*)$ kann man in verschiedener Weise interpretieren. Zunächst ist $s_1 := (a_1, b_1)$ normiert, und wir behaupten, dass für einen beliebig gewählten festen Punkt $v' \in L$ und $v \in \mathbb{R}^2$ genau dann $v \in L$ gilt, wenn

$$\langle s_1, v - v' \rangle = 0. \quad (**)$$

Dazu ist zu zeigen, dass für $v = (x, y)$ die Bedingungen zu $(*)$ und $(**)$ gleichwertig sind. Das ist jedoch klar, denn für $v' = (x', y')$ gilt

$$\langle s_1, v - v' \rangle = \langle s_1, v \rangle - \langle s_1, v' \rangle = a_1 x + b_1 y - (a_1 x' + b_1 y') = a_1 x + b_1 y - c_1.$$

Insbesondere ist die Gerade L senkrecht zu s_1 , sie ist also parallel zu

$$L_0 := \{(x, y) \in \mathbb{R}^2 : ax + by = 0\} = \{v \in \mathbb{R}^2 : \langle s_1, v \rangle = 0\}.$$

Auch der Wert von c_1 hat eine geometrische Bedeutung. Dazu berechnen wir für einen beliebigen Punkt $u = (x, y)$ den Abstand $d(u, L)$. Der Fußpunkt $u_0 = (x_0, y_0) \in L$ des Lotes von u auf L erfüllt die Bedingungen

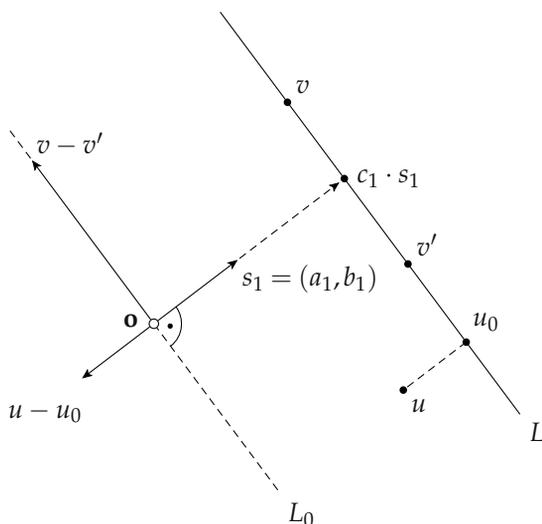
$$a_1x_0 + b_1y_0 = c_1 \quad \text{und} \quad (x_0, y_0) = u - \lambda s_1.$$

Daraus erhält man

$$a_1(x - \lambda a_1) + b_1(y - \lambda b_1) = c_1, \quad \text{also} \quad \lambda = a_1x + b_1y - c_1, \quad \text{da} \quad a_1^2 + b_1^2 = 1.$$

Schließlich folgt

$$d(u, L) = \|u - u_0\| = \|\lambda s_1\| = |\lambda| = |a_1x + b_1y - c_1|.$$



Insgesamt erhalten wir ein von L. O. HESSE im Jahr 1861 gefundenes Ergebnis:

HESSEsche Normalform einer Geradengleichung Wird die Gleichung $ax + by = c$ einer Geraden L im \mathbb{R}^2 nach (1) normiert zu

$$a_1x + b_1y = c_1 \quad \text{mit} \quad a_1^2 + b_1^2 = 1,$$

so ist $s_1 := (a_1, b_1)$ ein zu L senkrechter normierter Vektor. Für einen beliebigen Punkt $u = (x, y) \in \mathbb{R}^2$ ist

$$d(u, L) = |a_1x + b_1y - c_1|, \quad \text{insbesondere} \quad d(\mathbf{o}, L) = |c_1|.$$



0.3.6 Lineare Unabhängigkeit

Bei der Ungleichung von CAUCHY-SCHWARZ war die Frage offen geblieben, wann sie eine Gleichung ist. Das ist sicher dann der Fall, wenn einer der beiden Vektoren v und w der Nullvektor ist, oder wenn es ein $\rho \in \mathbb{R}$ gibt, so dass $v = \rho \cdot w$. Denn dann gilt

$$|\langle v, w \rangle| = |\langle \rho \cdot w, w \rangle| = |\rho| |\langle w, w \rangle| = |\rho| \cdot \|w\| \cdot \|w\| = \|v\| \cdot \|w\|.$$

Diese spezielle gegenseitige Lage von Vektoren führt zu folgender

Definition Zwei Vektoren $v, w \in \mathbb{R}^n$ heißen **linear abhängig**, wenn sich einer von beiden als skalares Vielfaches des anderen beschreiben lässt, d.h. es gilt

$$v = \rho \cdot w \quad \text{oder} \quad w = \sigma \cdot v, \quad \text{wobei } \rho, \sigma \in \mathbb{R}.$$

Dagegen heißen v und w **linear unabhängig**, wenn sie nicht linear abhängig sind.

Ist etwa $v = \mathbf{o}$, so sind v, w für beliebiges w linear abhängig, denn $v = 0 \cdot w$. Die Bedingung aus der Definition ist für Beweise etwas umständlich zu handhaben, weil man immer zwei mögliche Fälle betrachten muss. Eine handlichere Bedingung ergibt die

Bemerkung 1 Zwei Vektoren $v, w \in \mathbb{R}^n$ sind genau dann linear unabhängig, wenn aus

$$\lambda v + \mu w = \mathbf{o} \quad \text{folgt, dass} \quad \lambda = \mu = 0.$$

Beweis Formal einfacher ist zu zeigen, dass

$$v, w \text{ linear abhängig} \Leftrightarrow \lambda v + \mu w = \mathbf{o} \quad \text{mit} \quad (\lambda, \mu) \neq (0, 0).$$

„ \Rightarrow “ Ist $v = \rho \cdot w$, so folgt $1 \cdot v - \rho \cdot w = \mathbf{o}$.

Also kann man $(\lambda, \mu) = (1, -\rho)$ setzen. Der Fall $w = \sigma \cdot v$ geht analog.

„ \Leftarrow “ Ist $\lambda v + \mu w = \mathbf{o}$ und sei dabei etwa $\mu \neq 0$. Dann folgt

$$w = \sigma \cdot v, \quad \text{mit} \quad \sigma := -\frac{\lambda}{\mu}. \quad \blacksquare$$

Das Kriterium aus obiger Bemerkung kann man für

$$v = (x_1, \dots, x_n) \quad \text{und} \quad w = (y_1, \dots, y_n)$$

konkret nachprüfen; so ergibt die Bedingung $\lambda v + \mu w = \mathbf{o}$ die Gleichungen

$$\begin{array}{rcl} x_1\lambda & + & y_1\mu & = & 0 \\ \vdots & & \vdots & & \vdots \\ x_n\lambda & + & y_n\mu & = & 0. \end{array}$$

Das sind n lineare Gleichungen für λ, μ mit den x_i und y_i als Koeffizienten. Eine allgemeine Methode zur Entscheidung, ob es eine Lösung $(\lambda, \mu) \neq (0, 0)$ gibt, werden wir später kennenlernen. Im Fall $n = 1$ sind zwei Vektoren v, w stets linear abhängig, für $n = 2$ gibt es ein nützliches Kriterium:

Lemma Zwei Vektoren $v = (x_1, x_2)$ und $w = (y_1, y_2)$ sind genau dann linear unabhängig, wenn $x_1y_2 - x_2y_1 \neq 0$.

Die für lineare Unabhängigkeit entscheidende Zahl ist offenbar die *Determinante*

$$d := x_1y_2 - x_2y_1 = \det \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}$$

der 2×2 -Matrix mit den Vektoren v und w als Zeilen. Ihr Betrag gibt die Fläche des von v und w aufgespannten Parallelogramms an (vgl. 3.1.2).

Beweis Wir zeigen: v, w linear abhängig $\Leftrightarrow x_1y_2 - x_2y_1 = 0$.

„ \Rightarrow “ Sei $\lambda v + \mu w = \mathbf{o}$, wobei $\mu \neq 0$. Dann folgt $w = \rho \cdot v$ mit $\rho := -\frac{\lambda}{\mu}$, also $y_1 = \rho x_1, y_2 = \rho x_2$ und $x_1y_2 - x_2y_1 = x_1\rho x_2 - \rho x_1x_2 = 0$.

„ \Leftarrow “ Ist $v = \mathbf{o}$, so sind v, w linear abhängig. Wir können also $x_1 \neq 0$ voraussetzen. Dann ist

$$y_2 = \rho x_2 \quad \text{mit} \quad \rho := \frac{y_1}{x_1} \quad \text{also} \quad y_1 = \rho x_1 \quad \text{und} \quad w = \rho \cdot v.$$

■

Die lineare Unabhängigkeit hat auch etwas mit den Winkeln zu tun:

Bemerkung 2 Sind $v, w \in \mathbb{R}^n$ von \mathbf{o} verschieden, so gilt

$$v \perp w \quad \Rightarrow \quad v, w \text{ linear unabhängig.}$$

Beweis Angenommen, $\lambda v + \mu w = \mathbf{o}$. Bildung des Skalarprodukts von beiden Seiten dieser Gleichung mit v ergibt

$$0 = \langle v, \lambda v + \mu w \rangle = \lambda \langle v, v \rangle + \mu \langle v, w \rangle = \lambda \langle v, v \rangle.$$

Da $\langle v, v \rangle \neq 0$, muss $\lambda = 0$ sein. Durch Bildung des Skalarprodukts mit w folgt analog, dass $\mu = 0$.

■

Nach der Definition des Winkels $\vartheta = \angle(v, w)$ für $v, w \neq \mathbf{o}$ ist die Ungleichung von CAUCHY-SCHWARZ genau dann eine Gleichung, wenn $\cos \vartheta = \pm 1$, d.h. $\vartheta = 0$ oder $\vartheta = \pi$. Ohne Benutzung von Winkeln kann man das für beliebige v, w so formulieren:

Zusatz zur Ungleichung von CAUCHY-SCHWARZ Für $v, w \in \mathbb{R}^n$ gilt

$$|\langle v, w \rangle| = \|v\| \cdot \|w\| \Leftrightarrow v, w \text{ linear abhängig.}$$

Beweis Für $n = 1$ sind v, w immer linear abhängig. Für $n = 2$ hatten wir in 0.3.3 mit $v = (x_1, x_2)$ und $w = (y_1, y_2)$

$$|\langle v, w \rangle| = \|v\| \cdot \|w\| \Leftrightarrow x_1 y_2 - x_2 y_1 = 0$$

erhalten. Also folgt die Behauptung aus dem obigen Lemma.

Für $n = 3$ werden wir in 0.3.7 einen Beweis mit Hilfe des Vektorprodukts geben. Für allgemeines n kann man den Beweis aus 0.3.3 mit $w \neq \mathbf{o}$, $\lambda := \langle w, w \rangle > 0$ und $\mu := -\langle v, w \rangle$ fortsetzen. Danach ist

$$|\langle v, w \rangle| = \|v\| \cdot \|w\| \Rightarrow \lambda v + \mu w = \mathbf{o}.$$

Da $\lambda \neq 0$ folgt die lineare Abhängigkeit. Die umgekehrte Richtung ist offensichtlich:

$$w = \rho \cdot v \Rightarrow |\langle v, w \rangle| = |\langle \rho v, w \rangle| = \|v\| \cdot \|w\|.$$

■

Den für die lineare Algebra grundlegenden Begriff der linearen Unabhängigkeit werden wir bei den folgenden geometrischen Untersuchungen nicht nur für zwei, sondern auch für drei Vektoren benötigen. Wir erklären ihn daher gleich für beliebig viele, analog zur obigen Bemerkung 1.

Definition Vektoren $v_1, \dots, v_m \in \mathbb{R}^n$ heißen **linear unabhängig**, wenn aus

$$\lambda_1 v_1 + \dots + \lambda_m v_m = \mathbf{o} \quad \text{mit} \quad \lambda_1, \dots, \lambda_m \in \mathbb{R} \quad \text{folgt, dass} \quad \lambda_1 = \dots = \lambda_m = 0.$$

Dagegen heißen v_1, \dots, v_m **linear abhängig**, wenn sie nicht linear unabhängig sind. Das bedeutet, dass es eine Darstellung des Nullvektors

$$\lambda_1 v_1 + \dots + \lambda_m v_m = \mathbf{o} \quad \text{gibt mit} \quad (\lambda_1, \dots, \lambda_m) \neq (0, \dots, 0).$$

Die Handhabung dieser Definition erfordert etwas Übung. Für $m = 2$ und $n = 3$ werden wir in 0.3.7 eine Charakterisierung mit Hilfe des Vektorproduktes geben. Im Fall $m = n = 3$ werden wir in 0.4.4 aus den Komponenten von v_1, v_2, v_3 eine Zahl berechnen, die über die lineare Unabhängigkeit entscheidet.

0.3.7 Das Vektorprodukt im \mathbb{R}^3

Nach dem Lemma aus 0.3.6 sind zwei Vektoren $v = (x_1, x_2)$ und $w = (y_1, y_2)$ im \mathbb{R}^2 genau dann linear unabhängig, wenn

$$\det \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix} := x_1 y_2 - x_2 y_1 \neq 0.$$

Es ist eine naheliegende Frage, ob es ein ähnliches Kriterium im \mathbb{R}^3 gibt. Sind zwei Vektoren

$$v = (x_1, x_2, x_3) \text{ und } w = (y_1, y_2, y_3)$$

im \mathbb{R}^3 gegeben, so kann man sie in Form einer „Matrix“

$$A = \begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{pmatrix}$$

untereinander schreiben. Indem man jeweils eine Spalte streicht, kann man insgesamt drei Determinanten berechnen, und damit einen neuen Vektor, das **Vektorprodukt** (oder **Kreuzprodukt**)

$$\begin{aligned} v \times w &:= \left(\det \begin{pmatrix} x_2 & x_3 \\ y_2 & y_3 \end{pmatrix}, -\det \begin{pmatrix} x_1 & x_3 \\ y_1 & y_3 \end{pmatrix}, \det \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix} \right) \\ &= (x_2 y_3 - x_3 y_2, x_3 y_1 - x_1 y_3, x_1 y_2 - x_2 y_1) \in \mathbb{R}^3 \end{aligned}$$

erklären. Zwei Fragen stellen sich sofort: Warum wird die zweite Komponente negativ genommen und was ist die geometrische Bedeutung des Vektors $v \times w$? Eine erste Antwort darauf geben die folgenden

Rechenregeln Für $u, v, w \in \mathbb{R}^3$ und $\lambda \in \mathbb{R}$ gilt

- 1) $w \times v = -(v \times w)$, insbesondere $v \times v = \mathbf{0}$.
- 2) $(u + v) \times w = u \times w + v \times w$, $u \times (v + w) = u \times v + u \times w$.
 $\lambda v \times w = \lambda(v \times w) = v \times \lambda w$.
- 3) $\langle v \times w, v \rangle = 0$ und $\langle v \times w, w \rangle = 0$.

Beweis Es genügt, die Komponenten der Vektoren in die Formel für die Definition des Vektorprodukts einzusetzen und ganz elementar zu rechnen. Als Beispiel beweisen wir die erste Regel von 3). Ist $v = (x_1, x_2, x_3)$ und $w = (y_1, y_2, y_3)$, so wird

$$\langle v \times w, v \rangle = (x_2 y_3 - x_3 y_2)x_1 + (x_3 y_1 - x_1 y_3)x_2 + (x_1 y_2 - x_2 y_1)x_3 = 0.$$



Regel 3) bedeutet, dass $v \times w$ auf v und w senkrecht steht. Bleibt die Frage nach der Länge und der Richtung von $v \times w$. Der einfachste Fall ist

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

Vorsicht! Für das Vektorprodukt gilt keine Kürzungsregel, d.h. aus $v \times w = v \times w'$ folgt nicht $w = w'$. Als Beispiel kann $w = v$ und $w' = 2v$ mit $v \neq \mathbf{o}$ dienen!

Weiter ist das Vektorprodukt nicht assoziativ: $(e_1 \times e_1) \times e_2 = \mathbf{o}$, aber $e_1 \times (e_1 \times e_2) = e_1 \times e_3 = -e_2$.

Als erste Anwendung beweisen wir eine Art von Verallgemeinerung des Lemmas 0.3.6.

Lemma 1 Für Vektoren $v, w \in \mathbb{R}^3$ gilt

$$v, w \text{ linear unabhängig} \Leftrightarrow v \times w \neq \mathbf{o}.$$

Beweis Sind v, w linear abhängig, so können wir annehmen, dass $w = \rho \cdot v$ mit $\rho \in \mathbb{R}$. Aus den Rechenregeln folgt

$$v \times w = v \times \rho \cdot v = \rho \cdot (v \times v) = \rho \cdot \mathbf{o} = \mathbf{o}.$$

Sind v, w linear unabhängig, so ist $v \neq \mathbf{o}$; außerdem ist $w + \rho \cdot v \neq 0$ für alle $\rho \in \mathbb{R}$. Ist

$$v = (x_1, x_2, x_3) \quad \text{und} \quad w = (y_1, y_2, y_3),$$

so können wir weiter $x_1 \neq 0$ annehmen. Mit

$$\rho := -\frac{y_1}{x_1} \text{ wird } w + \rho \cdot v = (0, y'_2, y'_3) \neq (0, 0, 0).$$

Wieder nach den Rechenregeln ist

$$v \times (w + \rho v) = v \times w + v \times \rho v = v \times w + \mathbf{o} = v \times w$$

Ist etwa $y'_2 \neq 0$, so ist somit die dritte Komponente von $v \times w$ gleich $x_1 y'_2 - 0 \cdot x_2 = x_1 y'_2 \neq 0$, also folgt $v \times w \neq \mathbf{o}$. ■

Zusammen mit dem Lemma aus 0.3.6 kann man dieses Ergebnis so beschreiben: Bezeichnet v_i, w_i für $i = 1, 2, 3$ das Paar von Vektoren, bei dem jeweils die i -te Koordinate von v, w gleich 0 gesetzt wurde, so sind v, w genau dann linear unabhängig, wenn mindestens eines der drei Paare v_i, w_i linear unabhängig ist.

Vom Standpunkt des Beobachters sieht man das Paar v_i, w_i ebener Vektoren, wenn man das räumliche Paar v, w aus der i -ten Koordinatenrichtung betrachtet.

Sind die zwei Vektoren $v, w \in \mathbb{R}^3$ linear unabhängig, so sind auch die drei Vektoren $v, w, v \times w \in \mathbb{R}^3$ linear unabhängig. Das folgt aus dem allgemeinen

Lemma 2 *Im \mathbb{R}^n seien zwei linear unabhängige Vektoren v, w und ein weiterer Vektor $u \neq \mathbf{o}$ gegeben. Ist $u \perp v$ und $u \perp w$, so sind u, v, w linear unabhängig.*

Beweis Angenommen, u, v, w wären linear abhängig. Dann gibt es eine nicht triviale Relation

$$\lambda_1 u + \lambda_2 v + \lambda_3 w = \mathbf{o}.$$

Da v, w linear unabhängig sind, ist $\lambda_1 \neq 0$. Also gibt es λ, μ mit $u = \lambda v + \mu w$. Daraus folgt

$$\langle u, u \rangle = \langle u, \lambda v + \mu w \rangle = \lambda \langle u, v \rangle + \mu \langle u, w \rangle = 0 + 0 = 0,$$

und somit $u = \mathbf{o}$, im Widerspruch zur Voraussetzung. ■

In der Bemerkung aus 0.3.3 hatten wir gezeigt, dass es zu einem Vektor $w \in \mathbb{R}^2$ mit $w \neq \mathbf{o}$ bis auf einen Faktor nur einen senkrechten Vektor s gibt. Im \mathbb{R}^3 gibt es eine ähnliche Aussage:

Satz *Seien $v, w \in \mathbb{R}^3$ linear unabhängig und sei $s \in \mathbb{R}^3$ gegeben mit $\langle s, v \rangle = \langle s, w \rangle = 0$. Dann gibt es ein $\lambda \in \mathbb{R}$ so, dass*

$$s = \lambda \cdot (v \times w).$$

Beweis Wir wählen folgende Bezeichnungen:

$$v = (a_1, a_2, a_3), \quad w = (b_1, b_2, b_3) \quad \text{und} \quad s = (x_1, x_2, x_3).$$

Die Bedingungen $\langle s, v \rangle = 0$ und $\langle s, w \rangle = 0$ ergeben die linearen Gleichungen

$$a_1 x_1 + a_2 x_2 + a_3 x_3 = 0, \quad \text{I}$$

$$b_1 x_1 + b_2 x_2 + b_3 x_3 = 0. \quad \text{II}$$

Da v, w linear unabhängig sind, ist $v \times w \neq \mathbf{o}$ nach dem Lemma 1, wir können also $a_1 b_2 - a_2 b_1 \neq 0$ und außerdem $a_1 \neq 0$ annehmen. Wie wir im Beweis des Lemmas 1 gesehen haben, sind für $\rho \neq 0$ auch $v, w + \rho v$ linear unabhängig und $\langle s, w + \rho v \rangle = 0$. Setzt man $\rho := -\frac{b_1}{a_1}$, so kann man also die Gleichung II ersetzen durch

$$0 \cdot x_1 + (a_1 b_2 - b_1 a_2) x_2 + (a_1 b_3 - b_1 a_3) x_3 = 0. \quad \tilde{\text{II}}$$

Bei jeder möglichen Lösung (x_1, x_2, x_3) der Gleichungen I und $\tilde{\text{II}}$ und damit I und II kann man

$$x_3 = \lambda \cdot (a_1 b_2 - b_1 a_2) \quad \text{mit} \quad \lambda \in \mathbb{R}$$

annehmen, denn das ergibt alle möglichen reellen Werte. Setzt man dieses x_3 in $\tilde{\text{II}}$ ein, so erhält man

$$x_2 = \lambda \cdot (b_1 a_3 - a_1 b_3),$$

und setzt man schließlich diese Werte von x_3 und x_2 in I ein, so ergibt sich

$$x_1 = \lambda \cdot (a_2 b_3 - b_2 a_3), \quad \text{also} \quad s = \lambda \cdot (v \times w).$$

■

Dieser Satz ist ein weiteres Beispiel für eine scheinbar klare Aussage: Zu zwei linear unabhängigen Vektoren im \mathbb{R}^3 gibt es nur noch eine einzige mögliche senkrechte Richtung. Wenn man $v \times w$ als senkrecht nachgewiesen hat, muss jeder andere senkrecht stehende Vektor Vielfaches davon sein. Aber vom Standpunkt der analytischen Geometrie muss man das durch eine Rechnung begründen.

In 0.3.3 hatten wir die Ungleichung von CAUCHY-SCHWARZ bereits im \mathbb{R}^n bewiesen. Für $n = 3$ lohnt es sich, einen weiteren Beweis zu geben, weil er eine wichtige Information für das Vektorprodukt ergibt.

Ungleichung von CAUCHY-SCHWARZ im \mathbb{R}^3 Für $v, w \in \mathbb{R}^3$ gilt

$$\|v \times w\|^2 = \|v\|^2 \cdot \|w\|^2 - \langle v, w \rangle^2.$$

Insbesondere ist $|\langle v, w \rangle| \leq \|v\| \cdot \|w\|$ und Gleichheit gilt genau dann, wenn v, w linear abhängig sind.

Beweis Man muss nur geduldig rechnen. Mit $v = (x_1, x_2, x_3)$ und $w = (y_1, y_2, y_3)$ gilt

$$\begin{aligned} \|v \times w\|^2 &= \langle v \times w, v \times w \rangle = (x_2 y_3 - x_3 y_2)^2 + (x_3 y_1 - x_1 y_3)^2 + (x_1 y_2 - x_2 y_1)^2 \\ &= (x_1 y_2)^2 + (x_1 y_3)^2 + (x_2 y_1)^2 + (x_2 y_3)^2 + (x_3 y_1)^2 + (x_3 y_2)^2 \\ &\quad - 2(x_1 x_2 y_1 y_2 + x_1 x_3 y_1 y_3 + x_2 x_3 y_2 y_3) \\ &= (x_1^2 + x_2^2 + x_3^2)(y_1^2 + y_2^2 + y_3^2) - (x_1 y_1 + x_2 y_2 + x_3 y_3)^2 \\ &= \|v\|^2 \cdot \|w\|^2 - \langle v, w \rangle^2. \end{aligned}$$

Wegen der Monotonie der Quadratwurzel folgt $|\langle v, w \rangle| \leq \|v\| \cdot \|w\|$. Gleichheit gilt genau dann, wenn $\|v \times w\| = 0$; nach dem Lemma 1 ist das gleichwertig mit der linearen Abhängigkeit von v und w . ■

Nun sieht man, dass sich obiges Lemma 1 auch aus dem allgemeinen Zusatz zu CAUCHY-SCHWARZ in 0.3.4 folgern lässt.

In 0.3.3 hatten wir für von \mathbf{o} verschiedene Vektoren $v, w \in \mathbb{R}^n$ einen Winkel

$$\vartheta = \angle(v, w) \in [0, \pi] \quad \text{erklärt, so dass} \quad \langle v, w \rangle = \|v\| \cdot \|w\| \cdot \cos \vartheta.$$

Also folgt im \mathbb{R}^3

$$\begin{aligned}\|v \times w\|^2 &= \|v\|^2 \cdot \|w\|^2 - \langle v, w \rangle^2 \\ &= \|v\|^2 \cdot \|w\|^2 \cdot (1 - \cos^2 \vartheta) \\ &= \|v\|^2 \cdot \|w\|^2 \cdot \sin^2 \vartheta.\end{aligned}$$

Korollar 2 Für $0 \neq v, w \in \mathbb{R}^3$ gilt $\|v \times w\| = \|v\| \cdot \|w\| \cdot |\sin \angle(v, w)|$. ■

Damit ist eine geometrische Beschreibung des Vektorprodukts klar:

1. $v \times w$ steht senkrecht auf v und w
2. Die Länge von $v \times w$ ist gleich $\|v\| \cdot \|w\| \cdot \sin \angle(v, w)$, das ist die Fläche des von v und w aufgespannten Parallelogramms. Diese Flächenberechnung wird in 3.1.2 genauer erläutert.

Durch diese beiden Eigenschaften ist $v \times w$ bis auf das Vorzeichen bestimmt. Um zu erklären, welches von beiden zu wählen ist, benötigt man den Begriff der „Orientierung“ im Fall, dass v, w linear unabhängig sind:

3. $v, w, v \times w$ sind „gleichorientiert“ mit e_1, e_2, e_3 .

Geometrisch bedeutet das, dass das „Dreibein“ $v, w, v \times w$ stetig in e_1, e_2, e_3 überführt werden kann (vgl. dazu [F1, 3.4]).

Die naheliegende Frage, warum man das Vektorprodukt nicht besser durch die oben angegebenen drei geometrischen Eigenschaften erklärt, hat sich damit beinahe von selbst beantwortet. Die rein algebraische Definition ist viel einfacher und präziser; sie bedarf allerdings der geometrischen Interpretation. Interessante Anwendungen des Vektorprodukts folgen in den nächsten Abschnitten.

Für eine spätere Anwendung in 5.3.8 notieren wir noch die sogenannte

GRASSMANN-Identität Für Vektoren $u, v, w \in \mathbb{R}^3$ gilt

$$(u \times v) \times w = \langle u, w \rangle \cdot v - \langle v, w \rangle \cdot u.$$

Beweis Ist $u = (x_1, x_2, x_3), v = (y_1, y_2, y_3)$ und $w = (z_1, z_2, z_3)$, so kann man elementar ausrechnen, dass beide Seiten der Identität gleich dem Vektor

$$\begin{pmatrix} x_2 y_1 z_2 + x_3 y_1 z_3 - x_1 y_2 z_2 - x_1 y_3 z_3, \\ x_1 y_2 z_1 + x_3 y_2 z_3 - x_2 y_1 z_1 - x_2 y_3 z_3, \\ x_1 y_3 z_1 + x_2 y_3 z_2 - x_3 y_1 z_1 - x_3 y_2 z_2 \end{pmatrix} \in \mathbb{R}^3$$

sind. Wer besser verstehen will, was sich hinter der Rechnung verbirgt, möge die Identität in den Spezialfällen überprüfen, in denen für u, v, w beliebige Kombinationen der Basisvektoren e_1, e_2, e_3 eingesetzt werden. ■

0.3.8 Abstand von Geraden

In diesem letzten Abschnitt zum Thema Geraden wollen wir uns mit der gegenseitigen Lage von zwei Geraden im \mathbb{R}^3 beschäftigen. Um die möglichen Fälle parallel, mit Schnittpunkt oder windschief algebraisch charakterisieren zu können, ist es von Nutzen, den in 0.3.4 eingeführten Begriff der linearen Unabhängigkeit zu benutzen.

Gegeben seien zwei Geraden

$$L = v + \mathbb{R} \cdot w \quad \text{und} \quad L' = v' + \mathbb{R} \cdot w'$$

im \mathbb{R}^3 , wobei wie immer $w \neq \mathbf{o}$ und $w' \neq \mathbf{o}$ vorausgesetzt ist. In Bemerkung b) aus 0.2.2 hatten wir ein Kriterium dafür angegeben, dass $L = L'$.

Allgemeiner sind L und L' nach 0.2.2 genau dann *parallel*, wenn w und w' linear abhängig sind. Wieder nach 0.2.2 sind parallele Geraden mit einem Schnittpunkt gleich.

Sind L und L' nicht parallel, so können sie einen einzigen oder keinen Schnittpunkt haben. L und L' heißen *windschief*, wenn sie nicht parallel sind und wenn $L \cap L' = \emptyset$.

Lemma 1 $L = v + \mathbb{R} \cdot w$ und $L' = v' + \mathbb{R} \cdot w'$ im \mathbb{R}^3 sind genau dann windschief, wenn

$$(v' - v), w, w' \text{ linear unabhängig sind.}$$

Beweis Um die Logik des Beweises ganz klar zu machen, schreiben wir die Behauptung noch einmal auf:

$$w, w' \text{ linear unabhängig und } L \cap L' = \emptyset \Leftrightarrow (v' - v), w, w' \text{ linear unabhängig.}$$

„ \Rightarrow “ Sind $(v' - v), w, w'$ linear abhängig, so gibt es eine nicht triviale Linearkombination

$$\lambda(v' - v) + \mu w + \mu' w' = \mathbf{o}.$$

Ist $\lambda \neq 0$, so folgt

$$v - \frac{\mu}{\lambda} w = v' + \frac{\mu'}{\lambda} w',$$

das ist ein Schnittpunkt von L und L' . Ist $\lambda = 0$, so ist $(\mu, \mu') \neq (0, 0)$ und somit sind w, w' linear abhängig.

„ \Leftarrow “ Sind w, w' linear abhängig, so sind auch $(v' - v), w, w'$ linear abhängig. Ist $L \cap L' \neq \emptyset$, so gibt es μ, μ' mit

$$v + \mu w = v' + \mu' w', \text{ also } (v' - v) - \mu w + \mu' w' = \mathbf{o}.$$

Also sind $(v' - v), w, w'$ linear abhängig. ■

So, wie wir in 0.3.5 den Abstand eines Punktes von einer Geraden als minimalen Abstand erklärt hatten, können wir nun für Geraden $L, L' \subset \mathbb{R}^n$ den Abstand

$$d(L, L') := \min\{d(u, u') : u \in L, u' \in L'\}$$

erklären, wobei noch nicht nachgewiesen ist, dass dieses Minimum existiert. Das kann man mit Hilfe der Differentialrechnung erledigen, indem man

$$L = v + \lambda w, \quad L' = v' + \lambda' w'$$

setzt und die Funktion $\delta(\lambda, \lambda') := d(v + \lambda w, v' + \lambda' w')$ von den zwei Veränderlichen λ, λ' untersucht. Einfacher geht es mit dem guten alten Satz von PYTHAGORAS.

Lemma 2 Seien $L = v + \mathbb{R} \cdot w$ und $L' = v' + \mathbb{R} \cdot w'$ Geraden im \mathbb{R}^n , wobei $n \geq 2$. Angenommen $u_0 \in L$ und $u'_0 \in L'$ sind Punkte derart, dass

$$u'_0 - u_0 \text{ senkrecht zu } w \text{ und } w'$$

ist. Dann ist $d(L, L') = d(u_0, u'_0)$.

Kurz ausgedrückt: Das Minimum wird in den Fußpunkten eines gemeinsamen Lotes angenommen. Wie man ein gemeinsames Lot finden kann, wird anschließend überlegt.

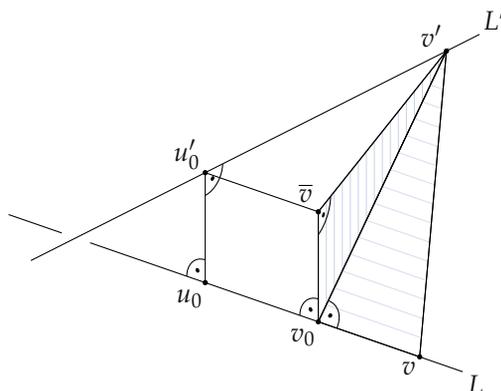
Beweis Haben L und L' einen Schnittpunkt, so ist $u_0 = u'_0$ und $d(L, L') = 0$; es genügt also, den Fall $u_0 \neq u'_0$ zu betrachten. Da v in L und v' in L' beliebig gewählt werden können, genügt es,

$$d(u_0, u'_0) \leq d(v, v')$$

zu beweisen. Im ersten Schritt bestimmen wir wie in 0.3.5 den Fußpunkt v_0 des Lotes von v' auf L . Dann ist

$$\langle v' - v_0, w \rangle = 0 \quad \text{und} \quad d(v', L) = d(v', v_0)$$

nach PYTHAGORAS.



Im zweiten Schritt betrachten wir das Dreieck mit den Ecken $v_0, v', \bar{v} := v_0 + u'_0 - u_0$. Um zu zeigen, dass es einen rechten Winkel an der Ecke \bar{v} hat, ist nachzurechnen, dass die Vektoren

$$\bar{v} - v' = v_0 - u_0 + u'_0 - v' \quad \text{und} \quad \bar{v} - v_0 = u'_0 - u_0$$

aufeinander senkrecht stehen. Das ist jedoch klar nach der Voraussetzung über $u'_0 - u_0$, und da

$$v_0 - u_0 = \lambda w, \quad u'_0 - v' = \lambda' w'.$$

Wieder mit PYTHAGORAS und nach Definition von v_0 folgt

$$d(u_0, u'_0) = d(v_0, \bar{v}) \leq d(v_0, v') \leq d(v, v').$$

■

Sind zwei Geraden $L, L' \subset \mathbb{R}^n$ parallel, so kann man

$$L = v + \mathbb{R} \cdot w \quad \text{und} \quad L' = v' + \mathbb{R} \cdot w$$

schreiben. Daher ist $d(L, L') = d(v, v')$. Für nicht parallele Geraden beschränken wir uns auf den \mathbb{R}^3 , da in diesem Fall das gemeinsame Lot mit Hilfe des Vektorprodukts gefunden werden kann.

Nun wollen wir für windschiefe Geraden

$$L = v + \mathbb{R} \cdot w \quad \text{und} \quad L' = v' + \mathbb{R} \cdot w' \quad \text{im } \mathbb{R}^3$$

die Fußpunkte $u_0 \in L$ und $u'_0 \in L'$ des gemeinsamen Lotes und den Abstand $d(L, L')$ berechnen. Zunächst ist nach dem Satz aus 0.3.7

$$u'_0 - u_0 = \delta \cdot (w \times w'), \quad \text{also} \quad d(L, L') = |\delta| \cdot \|w \times w'\|.$$

Ist $u_0 = v + \lambda_0 w$ und $u'_0 = v' + \lambda'_0 w'$, so folgt

$$\delta \cdot (w \times w') = v' - v + \lambda'_0 w' - \lambda_0 w. \quad (*)$$

Aus dieser Gleichung für Vektoren im \mathbb{R}^3 kann man nun die drei Werte von δ, λ_0 und λ'_0 herauskitzeln. Um δ zu erhalten, bildet man in (*) das Skalarprodukt mit $w \times w'$. Das ergibt

$$\delta \cdot \|w \times w'\|^2 = \langle v' - v, w \times w' \rangle, \quad \text{also} \quad \delta = \frac{\langle v' - v, w \times w' \rangle}{\|w \times w'\|^2}.$$

Daraus folgt $d(L, L') = \frac{|\langle v' - v, w \times w' \rangle|}{\|w \times w'\|}$.

Um λ_0 zu erhalten, multipliziert man (*) zunächst von links vektoriell mit w' :

$$\delta \cdot (w' \times (w \times w')) = w' \times (v' - v) + \lambda_0 (w \times w').$$

Bildet man in dieser Gleichung das Skalarprodukt mit $w \times w'$, so erhält man

$$0 = \langle w' \times (v' - v), w \times w' \rangle + \lambda_0 \|w \times w'\|^2, \text{ also } \lambda_0 = \frac{\langle (v' - v) \times w', w \times w' \rangle}{\|w \times w'\|^2}.$$

Analog erhält man, indem man zuerst mit w multipliziert,

$$\lambda'_0 = \frac{\langle (v' - v) \times w, w \times w' \rangle}{\|w \times w'\|^2}.$$

Das ging erstaunlich flott, aber man sollte sich nicht zu früh freuen: Wir haben mit Vektoren multipliziert, da gilt keine Kürzungsregel! Also erhalten wir zunächst nur notwendige Bedingungen für λ_0 und λ'_0 . Das heißt: Angenommen, die Fußpunkte existieren, dann müssen λ_0 und λ'_0 die berechneten Werte haben. Um die Existenz sicherzustellen, definiert man

$$u_0 := v + \lambda_0 w, \quad u'_0 := v' + \lambda'_0 w',$$

wobei λ_0 und λ'_0 durch die errechneten Brüche definiert sind und prüft nach, dass

$$\langle u_0 - u'_0, w \rangle = \langle u_0 - u'_0, w' \rangle = 0.$$

Diese kleine Strafarbeit wollen wir hier nicht ausführen. Mit Hilfe von etwas Theorie ist der Nachweis ganz einfach (vgl. [FI₁, 6.2.8]).

Wir fassen das Ergebnis noch einmal zusammen:

Satz Seien $L = v + \mathbb{R} \cdot w$ und $L' = v' + \mathbb{R} \cdot w'$ windschiefe Geraden im \mathbb{R}^3 . Dann gibt es eindeutig bestimmte Fußpunkte $u_0 \in L$ und $u'_0 \in L'$ eines gemeinsamen Lotes und es ist $d(L, L') = d(u_0, u'_0)$. Weiter gilt

$$\begin{aligned} u_0 = v + \lambda_0 w \quad \text{mit} \quad \lambda_0 &= \frac{\langle (v' - v) \times w', w \times w' \rangle}{\|w \times w'\|^2}, \\ u'_0 = v' + \lambda'_0 w' \quad \text{mit} \quad \lambda'_0 &= \frac{\langle (v' - v) \times w, w \times w' \rangle}{\|w \times w'\|^2}, \\ d(L, L') &= \frac{|\langle v' - v, w \times w' \rangle|}{\|w \times w'\|}. \end{aligned}$$

Beispiel Für $L = (0, 0, 0) + \mathbb{R} \cdot (1, 0, 0)$ und $L' = (0, 0, 1) + \mathbb{R} \cdot (1, 1, 2)$ ist

$$u_0 = \left(-\frac{2}{5}, 0, 0\right), \quad u'_0 = \left(-\frac{2}{5}, -\frac{2}{5}, \frac{1}{5}\right) \quad \text{und} \quad d(L, L') = \frac{1}{5} \sqrt{5} = 0.447\dots$$

Wie wir oben bemerkt haben, muss man sich überzeugen, dass Fußpunkte $u_0 \in L$ und $u'_0 \in L'$ eines gemeinsamen Lotes tatsächlich existieren. Es gibt ein klassisches elementares Beispiel, wie man ohne Klärung der Existenz Unsinn beweisen kann.

PERRONSches Paradoxon *Angenommen, in $\mathbb{N}^* = \{1, 2, \dots\}$ gibt es eine größte Zahl n . Dann ist $n = 1$.*

Beweis Für $n > 1$ ist

$$n^2 = n \cdot n > n \cdot 1 = n.$$

Da es nach der Annahme ein größtes n gibt, muss $n = 1$ sein! ■

Dieser Beweis ist völlig korrekt, aber die Annahme, dass eine größte Zahl existiert, ist natürlich Unsinn: Für jedes $n \in \mathbb{N}$ ist $n + 1 > n$.

0.4 Ebenen

0.4.1 Ebenen im \mathbb{R}^n

Eine Gerade im \mathbb{R}^n hat einen Aufhängepunkt v und einen Richtungsvektor w ; für eine Ebene benötigt man neben v zwei linear unabhängige Richtungsvektoren w_1, w_2 .

Definition Eine Teilmenge $E \subset \mathbb{R}^n$ heißt **Ebene**, wenn es $v, w_1, w_2 \in \mathbb{R}^n$ gibt, so dass w_1, w_2 linear unabhängig sind und

$$E = v + \mathbb{R} \cdot w_1 + \mathbb{R} \cdot w_2.$$

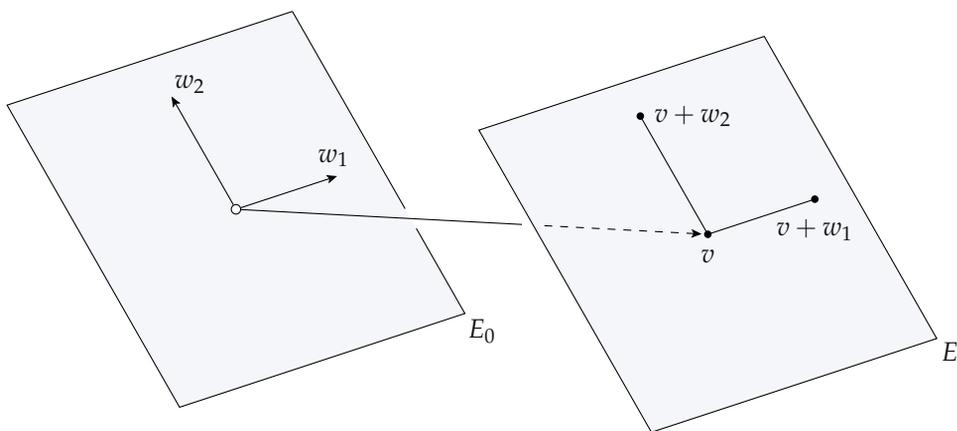
Dabei bedeutet

$$v + \mathbb{R} \cdot w_1 + \mathbb{R} \cdot w_2 := \{u \in \mathbb{R}^n : \text{Es gibt } \lambda_1, \lambda_2 \in \mathbb{R} \text{ so, dass } u = v + \lambda_1 w_1 + \lambda_2 w_2\}.$$

Diese Beschreibung von E nennt man **Parameterdarstellung**, **Parameter** sind die Zahlen λ_1, λ_2 . Zu E gehört

$$E_0 := \mathbb{R} \cdot w_1 + \mathbb{R} \cdot w_2 := \{\lambda_1 w_1 + \lambda_2 w_2 : \lambda_1, \lambda_2 \in \mathbb{R}\},$$

die Menge der **Linearkombinationen** von w_1 und w_2 , das ist eine Ebene durch den Ursprung \mathbf{o} .



In \mathbb{R}^1 sind je zwei Vektoren linear abhängig. Sind $w_1, w_2 \in \mathbb{R}^2$ linear unabhängig, so kann man leicht sehen, dass $\mathbb{R} \cdot w_1 + \mathbb{R} \cdot w_2 = \mathbb{R}^2$ (das sei dem Leser zur Übung empfohlen). Also ist die Untersuchung von Ebenen im \mathbb{R}^n nur für $n \geq 3$ interessant.

In 0.2.2 hatten wir mit etwas Rechnung geklärt, wann zwei Geraden $L = v + \mathbb{R} \cdot w$ und $L' = v' + \mathbb{R} \cdot w'$ gleich sind. Ein analoges Problem stellt sich für zwei Ebenen:

$$E = v + \mathbb{R} \cdot w_1 + \mathbb{R} \cdot w_2 \quad \text{und} \quad E' = v' + \mathbb{R} \cdot w'_1 + \mathbb{R} \cdot w'_2$$

im \mathbb{R}^n . Um dabei die Rechnung zu vereinfachen, ist ein wenig theoretischer Hintergrund hilfreich. Zunächst ein für die lineare Algebra grundlegender Begriff:

Definition Eine Teilmenge $W \subset \mathbb{R}^n$ heißt **Untervektorraum**, wenn $W \neq \emptyset$ und für beliebige $w, w' \in W$ und $\lambda \in \mathbb{R}$ auch $w + w' \in W$ und $\lambda \cdot w \in W$ gilt.

Kurz ausgedrückt: W darf nicht leer sein, und muss abgeschlossen sein unter Addition und Multiplikation mit Skalaren.

Beispiele Wir geben einige Teilmengen $W \subset \mathbb{R}^2$ an; der Leser möge prüfen, welche der Bedingungen für einen Untervektorraum erfüllt sind.

1. $W = \{\mathbf{o}\}$ oder $W = \mathbb{R}^2$.
2. $W = \{v\}$ mit $v \neq \mathbf{o}$.
3. $W = v + \mathbb{R} \cdot w$ mit $w \neq \mathbf{o}$ und $v = \mathbf{o}$ oder $v \neq \mathbf{o}$.
4. $W = \{(x, y) \in \mathbb{R}^2 : x \cdot y \geq 0\}$.
5. $W = \{(x, y) \in \mathbb{R}^2 : x \in \mathbb{Z} \text{ und } y \in \mathbb{Z}\}$.

Als Untervektorräume bleiben nur $\{\mathbf{o}\}$, $v + \mathbb{R} \cdot w$ mit $v = \mathbf{o}$ und \mathbb{R}^2 . Ein weiteres Beispiel im \mathbb{R}^n erhält man aus folgender

Bemerkung Sei $E = v + \mathbb{R} \cdot w_1 + \mathbb{R} \cdot w_2 \subset \mathbb{R}^n$ eine Ebene und $E_0 := \mathbb{R} \cdot w_1 + \mathbb{R} \cdot w_2$. Dann gilt:

- a) $E_0 \subset \mathbb{R}^n$ ist ein Untervektorraum.
- b) $E_0 = V := \{u - u' : u, u' \in E\}$, das ist die Menge der Differenzen aus E .

Aus b) folgt insbesondere, dass der Untervektorraum E_0 durch die Ebene E eindeutig bestimmt ist, d.h. dass er nicht abhängt von der Auswahl der Vektoren w_1 und w_2 .

Beweis a) $E_0 \neq \emptyset$, denn $\mathbf{o} = 0 \cdot w_1 + 0 \cdot w_2 \in E_0$.

Für $w = \lambda_1 w_1 + \lambda_2 w_2$ und $w' = \mu_1 w_1 + \mu_2 w_2$ und $\lambda \in \mathbb{R}^2$ folgt

$$\begin{aligned} w + w' &= (\lambda_1 + \mu_1)w_1 + (\lambda_2 + \mu_2)w_2 \in E_0 \quad \text{und} \\ \lambda(\lambda_1 w_1 + \lambda_2 w_2) &= (\lambda \lambda_1)w_1 + (\lambda \lambda_2)w_2 \in E_0. \end{aligned}$$

- b) $E_0 \subset V$: Ist $w \in E_0$, so folgt $v - w \in E$, also $w = v - (v - w) \in V$.
 $V \subset E_0$: Ist $u - u' \in V$, so folgt $u = v + w$ und $u' = v + w'$ mit $w, w' \in E_0$,
 also $u - u' = w - w' \in E_0$. ■

Mit Hilfe des Untervektorraums E_0 kann man erklären, wann zwei Ebenen $E, E' \subset \mathbb{R}^n$ **parallel** sind:

$$E \parallel E' \quad :\Leftrightarrow \quad E_0 = E'_0.$$

Nun kann man Parametrisierungen $E = v + \mathbb{R} \cdot w_1 + \mathbb{R} \cdot w_2 = v + E_0$ von Ebenen vergleichen.

Lemma a) Ist $E = v + E_0 \subset \mathbb{R}^n$ eine Ebene und $v' \in E$ beliebig, so ist auch

$$E = v' + E_0.$$

b) Für Ebenen $E = v + E_0$ und $E' = v' + E'_0$ gilt

$$E = E' \Leftrightarrow E_0 = E'_0 \quad \text{und} \quad E \cap E' \neq \emptyset.$$

Anders ausgedrückt: Eine Parameterdarstellung einer Ebene E ist festgelegt durch einen beliebigen Punkt $v \in E$ und den Untervektorraum E_0 . Zwei parallele Ebenen sind genau dann gleich, wenn sie sich schneiden.

Beweis Teil a) folgt sofort aus

$$v + w = v' + ((v - v') + w) \quad \text{und} \quad v' + w = v + ((v' - v) + w).$$

wobei $w \in E_0$. In Teil b) ist „ \Rightarrow “ klar nach obiger Bemerkung. Für die andere Richtung wähle man $v \in E \cap E'$. Dann ist nach a)

$$E = v + E_0 = v + E'_0 = v' + E'_0 = E'.$$

■

Eine Gerade $L \subset \mathbb{R}^n$ ist festgelegt durch zwei verschiedene Punkte $v, v_1 \in L$; es ist

$$L = v + \mathbb{R} \cdot (v_1 - v).$$

Zur Festlegung einer Ebene E braucht man drei Punkte $v, v_1, v_2 \in E$, die nicht auf einer Geraden liegen. Wie man schnell sieht, ist das gleichbedeutend damit, dass $v_1 - v$ und $v_2 - v$ linear unabhängig sind. Also erhält man aus obigem Lemma das

Korollar Durch drei Punkte $v, v_1, v_2 \in \mathbb{R}^n$, die nicht auf einer Geraden liegen, geht genau eine Ebene E , nämlich

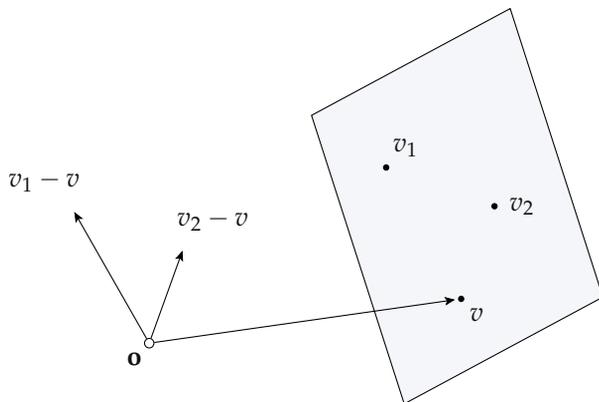
$$E = v + \mathbb{R} \cdot (v_1 - v) + \mathbb{R} \cdot (v_2 - v).$$

Beweis Wir setzen $w_1 := v_1 - v$ und $w_2 := v_2 - v$. Da

$$v_1 = v + w_1 \quad \text{und} \quad v_2 = v + w_2,$$

gilt $v, v_1, v_2 \in E$. Ist $E' = v' + \mathbb{R} \cdot w'_1 + \mathbb{R} \cdot w'_2$ mit linear unabhängigen w'_1, w'_2 eine weitere Ebene mit $v, v_1, v_2 \in E'$, so ist $E' = E$ zu zeigen. Nach dem Lemma kann man zunächst $v' = v$ setzen; dann bleibt zu zeigen, dass

$$E'_0 = E_0, \quad \text{d.h.} \quad \mathbb{R} \cdot w'_1 + \mathbb{R} \cdot w'_2 = \mathbb{R} \cdot w_1 + \mathbb{R} \cdot w_2.$$



Da w_1 und w_2 auch Differenzen aus E' sind, gilt $E_0 \subset E'_0$. Also gibt es Darstellungen

$$\begin{aligned} w_1 &= aw'_1 + bw'_2 \\ w_2 &= cw'_1 + dw'_2 \end{aligned} \quad (*)$$

mit $a, b, c, d \in \mathbb{R}$. Dabei muss $\delta := ad - bc \neq 0$ sein, denn andernfalls wären w_1 und w_2 linear abhängig: Ist etwa $a \neq 0$, so würde aus $\delta = 0$ folgen, dass $w_2 = \frac{c}{a}w_1$.

Aus (*) folgt durch einfache Rechnung

$$\begin{aligned} dw_1 - bw_2 &= \delta w'_1, \\ -cw_1 + aw_2 &= \delta w'_2. \end{aligned}$$

Da $\delta \neq 0$, folgt $E'_0 \subset E_0$; also ist $E'_0 = E_0$. ■

Die gerade bewiesene Aussage, dass durch drei Punkte, die nicht auf einer Geraden liegen, genau eine Ebene geht, steht in engem Zusammenhang zu der in 0.2.2 gezeigten Aussage, dass durch zwei verschiedene Punkte genau eine Gerade geht. Hinter diesen Aussagen ist der noch nicht präzierte Begriff der „Dimension“ versteckt: Eine Gerade hat die Dimension 1, sie ist durch 2 verschiedene Punkte bestimmt; eine Ebene hat die Dimension 2, dafür benötigt man 3 Punkte in „allgemeiner Lage“.

Wenn in Kapitel 2 die Eigenschaften der „Dimension“ eines Vektorraumes benutzt werden können, wird der oben gerade zu Ende geführte Beweis von $E'_0 = E_0$ ganz einfach werden: E_0 und E'_0 sind Vektorräume gleicher Dimension (nämlich 2), also folgt $E'_0 = E_0$ aus $E'_0 \subset E_0$. Dies als kleiner Vorgeschmack auf den Nutzen der allgemeinen Theorie, mit deren Hilfe viele kleine und auch größere Rechnungen vermieden werden können.

Für $n \geq 3$ gibt es im \mathbb{R}^n windschiefe Geraden. Analog nennt man Ebenen *windschief*, wenn sie nicht parallel sind und sich nicht schneiden. Das ist erst ab $n \geq 4$ möglich, ein einfaches Beispiel im \mathbb{R}^4 ist

$$E := \mathbb{R} \cdot e_1 + \mathbb{R} \cdot e_2 \quad \text{und} \quad E' := e_4 + \mathbb{R} \cdot e_2 + \mathbb{R} \cdot e_3.$$

Der Fall von Ebenen im \mathbb{R}^3 wird im folgenden Abschnitt behandelt.

0.4.2 Ebenen im \mathbb{R}^3

In 0.2.3 hatten wir gesehen, dass sich eine Gerade $L \subset \mathbb{R}^2$ durch eine lineare Gleichung beschreiben lässt. In diesem Abschnitt wollen wir eine analoge Aussage für Ebenen im \mathbb{R}^3 zeigen.

Satz Eine Teilmenge $E \subset \mathbb{R}^3$ ist genau dann eine Ebene, wenn es $a_1, a_2, a_3, b \in \mathbb{R}$ gibt, so dass $(a_1, a_2, a_3) \neq (0, 0, 0)$ und

$$E = \{(x_1, x_2, x_3) \in \mathbb{R}^3 : a_1x_1 + a_2x_2 + a_3x_3 = b\}.$$

Beweis Es sind zwei Richtungen zu beweisen:

1. Aus einer Parameterdarstellung $E = v + \mathbb{R} \cdot w_1 + \mathbb{R} \cdot w_2$ muss man passende Koeffizienten a_1, a_2, a_3, b für eine lineare Gleichung finden.
2. Aus einer linearen Gleichung muss man eine Parameterdarstellung bestimmen.

Um nicht zu viel von Hand ausrechnen zu müssen, benutzen wir ein Ergebnis, das später mühelos aus der allgemeinen Theorie folgen wird.

Lemma Sei $(a_1, a_2, a_3) \neq (0, 0, 0)$ und

$$L := \{(x_1, x_2, x_3) \in \mathbb{R}^3 : a_1x_1 + a_2x_2 + a_3x_3 = 0\} \subset \mathbb{R}^3$$

die Menge der Lösungen der linearen Gleichung. Dann ist $L \subset \mathbb{R}^3$ ein Untervektorraum. Hat man zwei linear unabhängige Vektoren $w_1, w_2 \in L$ gefunden, so folgt

$$L = \mathbb{R} \cdot w_1 + \mathbb{R} \cdot w_2. \quad \blacksquare$$

Mit der später eingeführten Terminologie wird gezeigt, dass die Lösungsmenge $L \subset \mathbb{R}^3$ in diesem Fall stets ein 2-dimensionaler Untervektorraum ist.

Ad 1. Zunächst bestimmen wir die Koeffizienten einer linearen Gleichung der Ebene $E_0 = \mathbb{R} \cdot w_1 + \mathbb{R} \cdot w_2$. Der Kniff ist dabei, die gesuchte Gleichung als Skalarprodukt von

$$s := (a_1, a_2, a_3) \quad \text{und} \quad x := (x_1, x_2, x_3)$$

zu betrachten. Sie lautet dann $\langle s, x \rangle = 0$, d.h. $s \perp x$. Daher gibt es nach 0.3.7 den offensichtlichen Kandidaten

$$s := w_1 \times w_2 = (a_1, a_2, a_3) \neq (0, 0, 0).$$

Definieren wir nun

$$L := \{x \in \mathbb{R}^3 : a_1 x_1 + a_2 x_2 + a_3 x_3 = 0\} = \{x \in \mathbb{R}^3 : s \perp x\},$$

so ist $E_0 = L$ zu zeigen. $E_0 \subset L$ ist klar, denn

$$\langle s, \lambda_1 w_1 + \lambda_2 w_2 \rangle = \lambda_1 \langle s, w_1 \rangle + \lambda_2 \langle s, w_2 \rangle = 0 + 0 = 0.$$

Nach dem obigen Lemma folgt $E_0 = L$.

Nebenbei bemerkt kann man nun auch die geometrisch klare Aussage, dass E_0 eine echte Teilmenge von \mathbb{R}^3 ist, algebraisch nachweisen: Nach dem Lemma 2 aus 0.3.7 sind s, w_1, w_2 linear unabhängig, also ist $s \notin E_0$.

Um eine Gleichung für $E = v + E_0$ zu finden, genügt es, $b := \langle s, v \rangle$ zu setzen, denn

$$x \in E \Leftrightarrow x - v \in E_0 \Leftrightarrow 0 = \langle s, x - v \rangle = \langle s, x \rangle - \langle s, v \rangle = \langle s, x \rangle - b.$$

Ad 2. Sei zunächst

$$E_0 := \{(x_1, x_2, x_3) \in \mathbb{R}^3 : a_1 x_1 + a_2 x_2 + a_3 x_3 = 0\},$$

wobei $(a_1, a_2, a_3) \neq (0, 0, 0)$. Gesucht ist eine Parametrisierung von E_0 ; genauer gesagt suchen wir linear unabhängige Vektoren $w_1, w_2 \in E_0$.

Wir können $a_1 \neq 0$ annehmen. Setzen wir $x_2 = 1$ und $x_3 = 0$, so lautet die Gleichung

$$a_1 x_1 + a_2 = 0, \quad \text{also folgt} \quad x_1 = -\frac{a_2}{a_1} \quad \text{und} \quad w_1 := \left(-\frac{a_2}{a_1}, 1, 0\right) \in E_0.$$

Mit $x_2 = 0$ und $x_3 = 1$ erhalten wir

$$a_1 x_1 + a_3 = 0, \quad \text{also folgt} \quad x_1 = -\frac{a_3}{a_1} \quad \text{und} \quad w_2 := \left(-\frac{a_3}{a_1}, 0, 1\right) \in E_0.$$

Es ist ganz einfach zu sehen, dass w_1 und w_2 linear unabhängig sind: Ist

$$\lambda_1 w_1 + \lambda_2 w_2 = \left(-\lambda_1 \frac{a_2}{a_1} - \lambda_2 \frac{a_3}{a_1}, \lambda_1, \lambda_2\right) = (0, 0, 0),$$

so folgt sofort $\lambda_1 = \lambda_2 = 0$. Schließlich folgt aus dem obigen Lemma

$$E_0 = \mathbb{R} \cdot w_1 + \mathbb{R} \cdot w_2.$$

Ist nun $E = \{(x_1, x_2, x_3) \in \mathbb{R}^3 : a_1 x_1 + a_2 x_2 + a_3 x_3 = b\}$ mit $a_1 \neq 0$, so kann man $x_2 = x_3 = 0$ setzen und erhält aus

$$a_1 x_1 = b \quad \text{die Lösung} \quad v := \left(\frac{b}{a_1}, 0, 0\right) \in E.$$

Setzt man wieder $s := (a_1, a_2, a_3)$, so ist $\langle s, v \rangle = b$, also

$$v + w \in E \quad \Leftrightarrow \quad w \in E_0, \quad \text{und somit} \quad E = v + E_0.$$

■

Aus dem obigen Satz und den im Beweis benutzten Argumenten kann man einige wichtige Folgerungen ableiten. Zunächst ein Analogon zur Bemerkung aus 0.2.3, die Geraden in \mathbb{R}^2 betraf.

Korollar 1 Gegeben seien im \mathbb{R}^3 mit $x := (x_1, x_2, x_3)$ Ebenen

$$E := \{x \in \mathbb{R}^3 : a_1 x_1 + a_2 x_2 + a_3 x_3 = b\} \quad \text{und} \\ E' := \{x \in \mathbb{R}^3 : a'_1 x_1 + a'_2 x_2 + a'_3 x_3 = b'\}$$

wobei $s := (a_1, a_2, a_3) \neq \mathbf{0}$ und $s' := (a'_1, a'_2, a'_3) \neq \mathbf{0}$, sowie $b, b' \in \mathbb{R}$ beliebig. Dann gilt:

$$E' = E \Leftrightarrow \text{es gibt ein } \varrho \in \mathbb{R}^*, \text{ so dass } (a'_1, a'_2, a'_3, b') = \varrho \cdot (a_1, a_2, a_3, b).$$

Beweis Zunächst kann man die definierenden Gleichungen einfacher schreiben:

$$E : \langle s, x \rangle = b, \quad E_0 : \langle s, x \rangle = 0, \quad E' : \langle s', x \rangle = b', \quad E'_0 : \langle s', x \rangle = 0.$$

„ \Leftarrow “ Folgt sofort aus $\langle s', x \rangle - b' = \varrho(\langle s, x \rangle - b)$.

„ \Rightarrow “ Aus $E' = E$ folgt $E'_0 = E_0$, sei $E_0 = \mathbb{R} \cdot w_1 + \mathbb{R} \cdot w_2$ mit w_1, w_2 linear unabhängig. Nach dem Satz aus 0.3.7 ist

$$s = \lambda(w_1 \times w_2) \quad \text{und} \quad s' = \lambda'(w_1 \times w_2) \quad \text{mit} \quad \lambda, \lambda' \in \mathbb{R}^*.$$

Daraus folgt $s' = \varrho s$ mit $\varrho = \frac{\lambda'}{\lambda}$. Mit einem beliebigen Punkt $v \in E = E'$ erhält man

$$b' = \langle s', v \rangle = \varrho \cdot \langle s, v \rangle = \varrho \cdot b.$$

■

Wie wir in 0.4.2 gesehen hatten, gibt es im \mathbb{R}^n ab $n \geq 4$ Ebenen, die nicht parallel sind und sich nicht schneiden. Im \mathbb{R}^3 ist das anders:

Korollar 2 Seien wie oben die Ebenen E und $E' \subset \mathbb{R}^3$ gegeben durch die Gleichungen $\langle s, x \rangle = b$ und $\langle s', x \rangle = b'$. Dann gilt:

- a) $E \parallel E' \Leftrightarrow s$ und $s' \in \mathbb{R}^3$ sind linear abhängig.
 b) Sind E, E' nicht parallel, so ist $L := E \cap E'$ eine Gerade, und es gilt

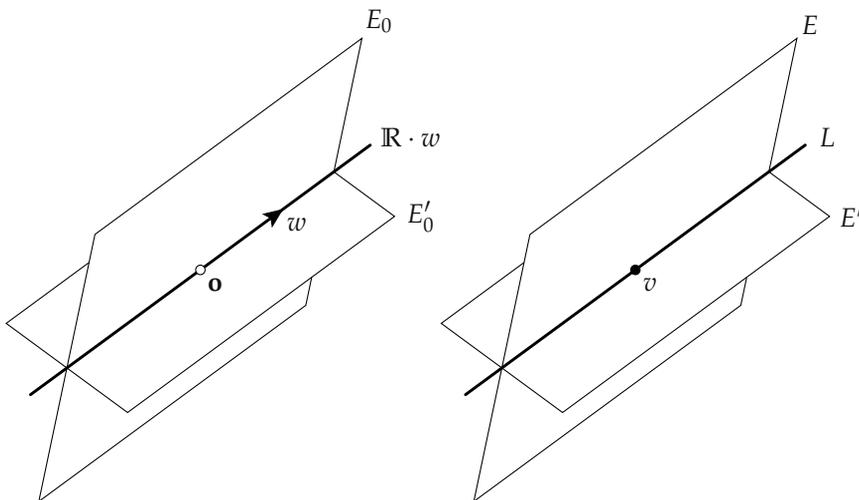
$$L = v + \mathbb{R} \cdot (s \times s'),$$

wenn $v \in L$ beliebig gewählt ist.

- c) Sind $E = v + \mathbb{R} \cdot w_1 + \mathbb{R} \cdot w_2$ und $E' = v + \mathbb{R} \cdot w'_1 + \mathbb{R} \cdot w'_2$ nicht parallel, so ist

$$E \cap E' = v + \mathbb{R} \cdot ((w_1 \times w_2) \times (w'_1 \times w'_2)).$$

Man kann also einen Richtungsvektor der Geraden $E \cap E'$ ganz einfach aus den Koeffizienten von Gleichungen für E und E' berechnen.



Beweis a) ist klar nach Korollar 1.

Zu b) Sind E, E' nicht parallel, so sind s, s' nach a) linear unabhängig. Aus den Gleichungen für E_0 und E'_0 erhält man

$$w \in E_0 \cap E'_0 \Leftrightarrow w \perp s \text{ und } w \perp s'.$$

Nach dem Satz aus 0.3.7 folgt $E_0 \cap E'_0 = \mathbb{R} \cdot (s \times s')$. Wie wir gleich anschließend in 0.5 beweisen werden, haben die beiden Gleichungen für E und E' eine gemeinsame Lösung $v \in E \cap E'$. Somit ist

$$E = v + E_0 \text{ und } E' = v + E'_0, \text{ also } E \cap E' = v + (E_0 \cap E'_0) = v + \mathbb{R} \cdot (s \times s'),$$

das ist eine Gerade.

c) folgt sofort aus b) und der Konstruktion der Gleichungen in obigem Satz. Man beachte dabei, dass das Vektorprodukt nicht assoziativ ist! ■

Beispiel Die beiden Ebenen seien gegeben durch folgende Gleichungen:

$$\begin{aligned} E: \quad 2x_1 + x_2 - x_3 &= 1, \quad \text{also } s = (2, 1, -1), \\ E': \quad 3x_2 + x_3 &= 2, \quad \text{also } s' = (0, 3, 1). \end{aligned}$$

Dann ist $s \times s' = (4, -2, 6)$. Um irgendeinen Punkt $v \in E \cap E'$ zu finden, setzen wir $x_3 = 0$. Dann ist

$$\begin{aligned} 3x_2 &= 2, \quad \text{also } x_2 = \frac{2}{3} \quad \text{nach der zweiten Gleichung und} \\ 2x_1 + \frac{2}{3} &= 1, \quad \text{also } x_1 = \frac{1}{6} \quad \text{nach der ersten Gleichung.} \end{aligned}$$

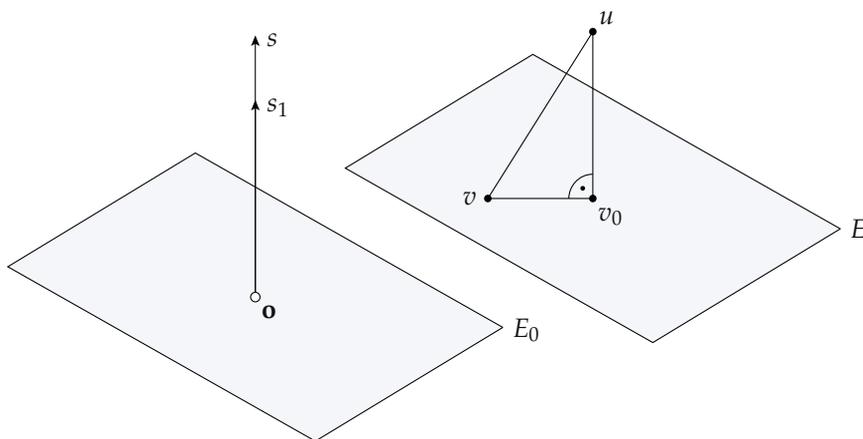
Insgesamt folgt $E \cap E' = \left(\frac{1}{6}, \frac{2}{3}, 0\right) + \mathbb{R} \cdot (2, -1, 3)$.

0.4.3 Abstand eines Punktes von einer Ebene

Ist $E \subset \mathbb{R}^3$ eine Ebene und $u \in \mathbb{R}^3$ ein beliebiger Punkt, so ist der Abstand von u nach E erklärt als

$$d(u, E) := \min\{d(u, v) : v \in E\}.$$

Es ist geometrisch ziemlich klar, dass dieses Minimum existiert und dass es angenommen wird für den Fußpunkt $v_0 \in E$ des Lotes von u auf E . Wir wollen das präzise begründen und die altbekannte Formel für die Berechnung des Abstandes herleiten.



Nach Definition steht ein Vektor $s \in \mathbb{R}^3$ *senkrecht* auf E , in Zeichen $s \perp E$, wenn

$$\langle s, v' - v \rangle = 0 \quad \text{für alle } v, v' \in E,$$

d.h. wenn er auf allen Differenzen aus E senkrecht steht. Ist $E = v + \mathbb{R} \cdot w_1 + \mathbb{R} \cdot w_2$ in Parameterdarstellung gegeben, so bedeutet das nach der Bemerkung aus 0.4.1, dass s senkrecht auf $E_0 = \mathbb{R} \cdot w_1 + \mathbb{R} \cdot w_2$ steht, d.h.

$$\langle s, w_1 \rangle = \langle s, w_2 \rangle = 0.$$

Da w_1, w_2 als linear unabhängig vorausgesetzt waren, folgt aus dem Satz in 0.3.7, dass

$$s \perp E \quad \Leftrightarrow \quad s = \lambda \cdot (w_1 \times w_2).$$

Ein Vektor heißt **Normalenvektor** von E , wenn er auf E senkrecht steht und die Norm 1 hat. Demnach gibt es dafür genau zwei Möglichkeiten, nämlich

$$s_1 := \pm \frac{1}{\|w_1 \times w_2\|} \cdot (w_1 \times w_2).$$

Wie wir in 0.4.2 gesehen hatten, kann man einen Normalenvektor auch ganz einfach aus der linearen Gleichung

$$a_1x_1 + a_2x_2 + a_3x_3 = b$$

für E erhalten. Man setzt $s := (a_1, a_2, a_3)$, und

$$s_1 := \frac{1}{\|s\|} \cdot s = (a'_1, a'_2, a'_3), \text{ also } a'_i = \frac{1}{\sigma} \cdot a_i \text{ mit } \sigma := \sqrt{a_1^2 + a_2^2 + a_3^2},$$

ist ein Normalenvektor von E .

Nun zeigen wir, dass es zu einer Ebene $E \subset \mathbb{R}^3$ und einem beliebigen $u \in \mathbb{R}^3$ einen eindeutig bestimmten Fußpunkt $v_0 \in E$ des Lotes von u auf E gibt. Angenommen man hat so ein v_0 , dann ist für ein beliebiges $v \in E$ nach dem Satz von Pythagoras im rechtwinkligen Dreieck mit den Ecken u, v und v_0

$$d(u, v_0) \leq d(u, v).$$

Also wird das Minimum in v_0 angenommen und es ist $d(u, E) = d(u, v_0)$. Um v_0 zu finden, benutzen wir, dass es ein $\rho \in \mathbb{R}$ geben muss mit

$$u - v_0 = \rho \cdot s_1.$$

Da $u - v = (u - v_0) + (v_0 - v)$, folgt durch Bildung des Skalarprodukts mit s_1

$$\langle s_1, u - v \rangle = \langle s_1, u - v_0 \rangle + 0 = \langle s_1, \rho \cdot s_1 \rangle = \rho \langle s_1, s_1 \rangle = \rho.$$

Man kann also den Faktor ρ mit jedem beliebigen $v \in E$ ausrechnen, der Fußpunkt ist dann durch $v_0 := u - \rho \cdot s_1$ eindeutig bestimmt. Sicherheitshalber sollte man noch einmal nachrechnen, dass dieses v_0 in E liegt und dass $(u - v_0) \perp E$. Wir fassen das Ergebnis zusammen:

Satz Sei $E \subset \mathbb{R}^3$ eine Ebene, $v \in E$, $u \in \mathbb{R}^3$ beliebig und $s_1 \in \mathbb{R}^3$ ein Normalenvektor von E . Ist

$$\rho := \langle s_1, (u - v) \rangle, \quad \text{so gilt } d(u, E) = |\rho|.$$

Der Fußpunkt des Lotes von u auf E ist $v_0 = u - \rho \cdot s_1$. ■

Offensichtlich ist $u \in E$ genau dann, wenn $d(u, E) = 0$. Das ergibt als Korollar die

HESSEsche Normalform einer Ebenengleichung Ist $E \subset \mathbb{R}^3$ eine Ebene, $s_1 \in \mathbb{R}^3$ ein Normalenvektor von E und $v \in E$ beliebig, so ist

$$E = \{u \in \mathbb{R}^3 : \langle s_1, (u - v) \rangle = 0\} \quad \blacksquare$$

Wie wir oben gesehen haben, kann man eine beliebige Gleichung

$$a_1x_1 + a_2x_2 + a_3x_3 = b \quad \text{auf Normalform} \quad a'_1x_1 + a'_2x_2 + a'_3x_3 = b'$$

bringen, indem man mit $\sigma := \sqrt{a_1^2 + a_2^2 + a_3^2}$

$$a'_i = \frac{a_i}{\sigma} \quad \text{für } i = 1, 2, 3 \quad \text{und} \quad b' = \frac{b}{\sigma}$$

setzt. Offensichtlich ist dann $|b'| = d(\mathbf{o}, E)$.

Beispiel Ist $E := \{(x_1, x_2, x_3) \in \mathbb{R}^3 : 6x_1 - 2x_2 + 3x_3 = 27\}$ und $u := (1, 4 - 2)$, so folgt

$$s_1 = \frac{1}{7}(6, -2, 3), \quad d(u, E) = 5 \quad \text{und} \quad d(\mathbf{o}, E) = \frac{27}{7}.$$

0.4.4 Das Spatprodukt

In den vorhergehenden geometrischen Überlegungen hatten wir schon öfters ein Skalarprodukt mit einem Vektorprodukt gebildet. Wir wollen nun die geometrische Bedeutung der aus Vektoren $u, v, w \in \mathbb{R}^3$ entstehenden Zahl

$$\langle u, v \times w \rangle \in \mathbb{R},$$

dem **Spatprodukt** von u, v, w , untersuchen.

Zunächst spannen die beiden Vektoren v, w ein **Parallelogramm**

$$P := \{\lambda v + \mu w \in \mathbb{R}^3 : 0 \leq \lambda \leq 1 \text{ und } 0 \leq \mu \leq 1\}$$

auf. Mit Hilfe von Korollar 2 aus 0.3.7 sieht man, dass der Flächeninhalt von P gleich

$$I_2(P) = \|v\| \cdot \|w\| \cdot |\sin \angle(v, w)| = \|v \times w\|$$

ist. Nimmt man den Vektor u dazu, so erhält man den *Spat*

$$S := \{\lambda v + \mu w + \rho u \in \mathbb{R}^3 : 0 \leq \lambda, \mu, \rho \leq 1\}.$$

Bezeichnet $I_3(S)$ den Rauminhalt von S , so behaupten wir

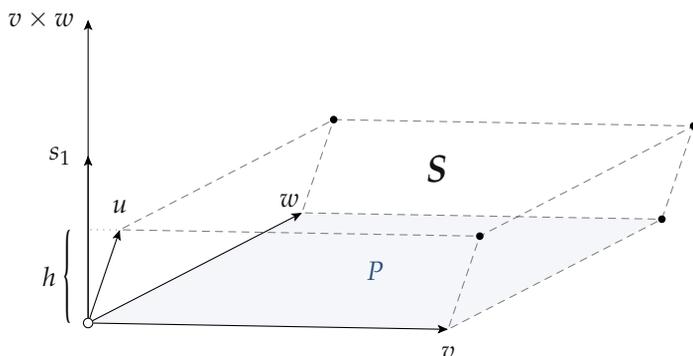
$$I_3(S) = |\langle u, v \times w \rangle|. \quad (*)$$

Nach den elementaren Regeln für Inhalte ist

$$I_3(S) = I_2(P) \cdot h,$$

wobei h die Höhe von S bezeichnet. Sind v, w linear abhängig, so ist $v \times w = \mathbf{o}$ und $I_3(S) = I_2(P) = 0$. Andernfalls ist $E = \mathbb{R} \cdot v + \mathbb{R} \cdot w$ eine Ebene und h ist gleich dem Abstand von u nach E , nach 0.4.3 folgt

$$h = |\langle u, s_1 \rangle|, \text{ wobei } s_1 = \frac{1}{\|v \times w\|} (v \times w).$$



Insgesamt ergibt sich

$$I_3(S) = \|v \times w\| \cdot |\langle u, s_1 \rangle| = |\langle u, v \times w \rangle|. \quad \blacksquare$$

Damit ist folgende Aussage geometrisch plausibel:

Lemma Für $u, v, w \in \mathbb{R}^3$ gilt

$$u, v, w \text{ linear unabhängig} \Leftrightarrow \langle u, v \times w \rangle \neq 0.$$

Beweis Wir geben zunächst an, wie man das Spatprodukt explizit ausrechnen kann. Ist

$$u = (x_1, x_2, x_3), \quad v = (y_1, y_2, y_3), \quad w = (z_1, z_2, z_3),$$

so erhält man nach der Definition des Vektorprodukts

$$\begin{aligned}\langle u, v \times w \rangle &= x_1(y_2z_3 - y_3z_2) - x_2(y_1z_3 - y_3z_1) + x_3(y_1z_2 - y_2z_1) \\ &= x_1y_2z_3 + x_2y_3z_1 + x_3y_1z_2 - x_3y_2z_1 - x_2y_1z_3 - x_1y_3z_2.\end{aligned}$$

Durch diese Summe von Produkten kann man die *Determinante* der Matrix

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{pmatrix}$$

erklären. Wie man daran sieht, ist das Ergebnis ziemlich symmetrisch in den Vektoren u, v, w , was in der Definition des Spatprodukts zunächst nicht klar war. Wenn man die Vorzeichen genau betrachtet, findet man die Regeln

$$\begin{aligned}\langle u, v \times w \rangle &= \langle v, w \times u \rangle = \langle w, u \times v \rangle \\ &= -\langle u, w \times v \rangle = -\langle w, v \times u \rangle = -\langle v, u \times w \rangle.\end{aligned}\tag{**}$$

Damit kann man den Beweis zügig abschließen. Sind u, v, w linear unabhängig, so ist $E = \mathbb{R} \cdot v + \mathbb{R} \cdot w$ eine Ebene durch \mathbf{o} und $u \notin E$. Also folgt nach dem Satz aus 0.4.3

$$0 \neq d(u, E) = \frac{1}{\|v \times w\|} |\langle u, v \times w \rangle|.$$

Sind u, v, w linear abhängig, so gibt es eine nicht triviale Linearkombination

$$\lambda v + \mu w + \rho u = \mathbf{o}.$$

Ist etwa $\rho \neq 0$, so folgt $u \in \mathbb{R} \cdot v + \mathbb{R} \cdot w$ und $\langle u, v \times w \rangle = 0$. Ist nur $\lambda \neq 0$ oder $\mu \neq 0$, so benütze man die Regel (**). ■

Die lineare Unabhängigkeit mit Hilfe des Spatinhalts zu prüfen ist geometrisch sehr plausibel, aber die Berechnung der Determinante ist etwas unangenehm. Außerdem will man ja dabei gar nicht den genauen Wert des Inhalts nennen, es genügt zu wissen, ob er Null ist oder nicht. Verfahren mit weniger Rechenaufwand, die auch im \mathbb{R}^n ausführbar sind, werden wir in 2.1.4 beschreiben.

0.5 Lineare Gleichungssysteme

Schon in den vorhergehenden Abschnitten waren öfters lineare Gleichungen aufgetreten, deren Lösungen zu ermitteln waren. Wir wollen nun eine sehr explizite allgemeine Methode zur Lösung von Systemen linearer Gleichungen beschreiben.

0.5.1 Zwei Geraden in der Ebene

Um den geometrischen Hintergrund des allgemeinen Lösungsverfahrens ganz deutlich zu machen, geben wir ein sehr einfaches Beispiel in der Ebene \mathbb{R}^2 mit Koordinaten (x, y) . Gesucht sind alle Punkte $(x, y) \in \mathbb{R}^2$, die den beiden folgenden Bedingungen genügen:

$$\begin{aligned} (1) \quad x - y &= 1, \\ (2) \quad 2x - y &= 3. \end{aligned}$$

Geometrisch gesehen beschreiben die Gleichungen zwei Geraden $L_1, L_2 \subset \mathbb{R}^2$, als Lösung ist ein einziger Schnittpunkt zu erwarten. Am einfachsten ist es in diesem Fall, wenn man $y = x - 1$ aus Gleichung (1) in Gleichung (2) einsetzt. Das ergibt

$$x = 2, \quad \text{also } y = 1 \quad \text{und} \quad (x, y) = (2, 1)$$

ist der Schnittpunkt. Bei mehreren Unbekannten und Gleichungen wird dieses Verfahren der *Substitution* schnell unübersichtlich; besser ist das Verfahren der *Elimination*. Dazu ersetzt man die Gleichung (2) durch $(2)' = (2) - 2 \cdot (1)$, das ergibt

$$\begin{aligned} (1) \quad x - y &= 1, \\ (2)' \quad y &= 1. \end{aligned}$$

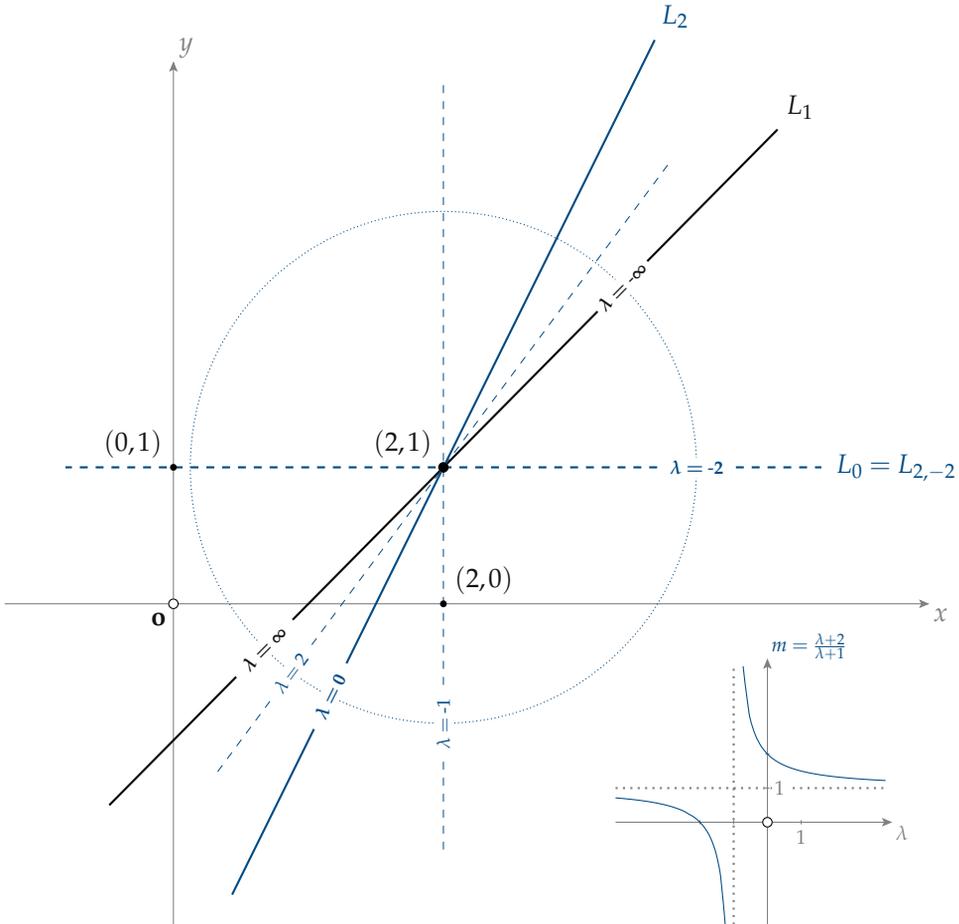
$(2)'$ ergibt sofort $y = 1$, in (1) eingesetzt erhält man $x = 2$.

Das funktioniert sehr gut, aber es bleibt die Frage zu klären, warum man die Gleichung (2) durch $(2)'$ ersetzen darf. Dazu betrachten wir zunächst für ein beliebiges $\lambda \in \mathbb{R}$ die Gleichung

$$(2)_\lambda = (2) + \lambda \cdot (1) : \quad (2 + \lambda)x - (1 + \lambda)y = 3 + \lambda.$$

Das ist die Gleichung einer Geraden $L_{2,\lambda}$, sie geht offensichtlich für jedes beliebige $\lambda \in \mathbb{R}$ durch den Schnittpunkt $(2, 1)$ von L_1 und L_2 . Es bleibt zu zeigen, dass sich auch L_1 und $L_{2,\lambda}$ für alle $\lambda \in \mathbb{R}$ nur in $(2, 1)$ schneiden. Hierzu genügt es, zu überlegen, dass es kein $\lambda \in \mathbb{R}$ gibt, so dass $L_1 = L_{2,\lambda}$. Dazu berechnen wir die Steigungen:

$$L_1 \text{ hat Steigung } 1, \quad L_{2,\lambda} \text{ hat Steigung } m = \frac{\lambda + 2}{\lambda + 1}.$$



Für $\lambda = -1$ wird die Steigung unendlich, d.h. die Gerade steht senkrecht.

Damit ist alles klar: Für sehr große und für sehr kleine λ nähert sich die Steigung von $L_{2,\lambda}$ dem Wert 1 beliebig nahe an, er wird aber nie erreicht, d.h.

$$L_1 \cap L_{2,\lambda} = \{(2,1)\} = L_1 \cap L_2 \quad \text{für alle } \lambda \in \mathbb{R}.$$

Diese Überlegung hat gezeigt, dass man in der Wahl von λ völlig frei ist. Der Wert $\lambda = -2$ ist dadurch ausgezeichnet, dass man damit L_2 ersetzen kann durch $L_0 = L_{2,-2}$, eine Gerade mit Steigung 0. Für die zugehörige Gleichung $(2)_{-2}$ bedeutet das, dass x nicht mehr vorkommt, diese Unbestimmte ist also „eliminiert“.

Der abstrakte Hintergrund der Überlegung mit den beiden Geraden ist folgender:

Bemerkung Sind $s_1, s_2 \in \mathbb{R}^n$ linear unabhängig, so sind für jedes $\lambda \in \mathbb{R}$ auch s_1 und $s_2 + \lambda s_1$ linear unabhängig.

Beweis Angenommen, $\mu_1 s_1 + \mu_2(s_2 + \lambda s_1) = \mathbf{o}$. Daraus folgt

$$(\mu_1 + \mu_2 \lambda) s_1 + \mu_2 s_2 = \mathbf{o}, \quad \text{also} \quad \mu_1 + \mu_2 \lambda = \mu_2 = 0.$$

Also ist $\mu_1 s_1 = \mathbf{o}$ und somit auch $\mu_1 = 0$. ■

0.5.2 Beschreibung durch Matrizen

Ganz allgemein kann ein System linearer Gleichungen aus m Gleichungen für n Unbekannte bestehen. Das bedeutet, dass an ein $x = (x_1, \dots, x_n) \in \mathbb{R}^n$ folgende Bedingungen gestellt werden:

$$\begin{array}{cccc} a_{11}x_1 & + & \cdots & + & a_{1n}x_n & = & b_1, \\ \vdots & & & & \vdots & & \vdots \\ a_{m1}x_1 & + & \cdots & + & a_{mn}x_n & = & b_m. \end{array} \quad (**)$$

Dabei sind die **Koeffizienten** a_{ij} und b_i vorgegebene reelle Zahlen. Der Index $i \in \{1, \dots, m\}$ zeigt die Nummer der Gleichung an, $j \in \{1, \dots, n\}$ ist die Nummer der zugehörigen Unbestimmten x_j . Das System zu „lösen“, bedeutet, die **Lösungsmenge**

$$L := \{x = (x_1, \dots, x_n) \in \mathbb{R}^n : x \text{ erfüllt } (**)\}$$

möglichst explizit anzugeben. Dazu muss vor allem geklärt werden, welche „Struktur“ die Menge L hat. In den einfachsten Fällen der vorhergehenden Abschnitte hatten wir als Lösungsmengen Punkte, Geraden und Ebenen erhalten.

Zunächst wollen wir die Bezeichnungen vereinfachen. Dazu fassen wir die Koeffizienten a_{ij} und b_i zusammen in eine **Matrix** (das lateinische Wort bedeutet „Mutterboden“)

$$A := \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \quad \text{und eine Spalte} \quad b := \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}.$$

Die Matrix A hat m **Zeilen** und n **Spalten**, man nennt sie eine $m \times n$ -Matrix und schreibt abkürzend $A = (a_{ij})$. Der Vektor der Unbestimmten wird als Spalte

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

geschrieben. Dann ist eine Multiplikation der Matrix A mit der Spalte x erklärt durch

$$A \cdot x := \begin{pmatrix} a_{11}x_1 + \cdots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n \end{pmatrix}.$$

Das Ergebnis ist wieder eine Spalte, die m Einträge sind die Skalarprodukte der Zeilen von A mit x . Das Gleichungssystem (***) lautet in dieser Schreibweise

$$A \cdot x = b, \quad (**)$$

die **Lösungsmenge** kann erklärt werden durch

$$\text{Lös}(A, b) := \{x \in \mathbb{R}^n : A \cdot x = b\} \subset \mathbb{R}^n.$$

Es ist von Vorteil, auch die Spalte b in die Koeffizientenmatrix mit aufzunehmen. Dann erhält man eine erweiterte **Koeffizientenmatrix**

$$(A, b) := \left(\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{array} \right),$$

das ist eine $m \times (n + 1)$ -Matrix.

0.5.3 Koeffizientenmatrix in Zeilenstufenform

Zur Bestimmung der Lösungsmenge gibt es eine sehr effiziente Methode: Man eliminiert systematisch Unbekannte. Wir wollen zunächst zeigen, wie einfach die Lösungen erhalten werden können, wenn die Elimination abgeschlossen ist, d.h. die Koeffizientenmatrix (A, b) durch Umformungen auf eine besonders günstige Form gebracht ist.

Man sagt, eine Koeffizientenmatrix (A, b) hat **Zeilenstufenform**, wenn sie von der Form

$$(A, b) = \left(\begin{array}{cccc|c} a_{1j_1} & & & & b_1 \\ & a_{2j_2} & & & b_2 \\ & & \ddots & & \vdots \\ & & & a_{rj_r} & b_r \\ & 0 & & & b_{r+1} \\ & & & & \vdots \\ & & & & b_m \end{array} \right)$$

ist. Die Einträge $a_{1j_1}, \dots, a_{rj_r}$ heißen **Pivots** (auf deutsch Angelpunkte); sie müssen ungleich Null sein, und es gilt

$$1 \leq j_1 < j_2 < \dots < j_r \leq n.$$

Alle Einträge a_{ij} unterhalb der Stufenlinie müssen gleich Null sein. Die Einträge b_1, \dots, b_m und die von den Pivots verschiedenen Einträge a_{ij} oberhalb der Stufenlinie unterliegen keinen Einschränkungen.

Die Lösungsmenge eines linearen Gleichungssystems kann auch leer sein; etwa dann wenn zwei Gleichungen zwei verschiedene parallele Geraden in der Ebene beschreiben. An der Zeilenstufenform sieht man sofort, wann dieser Fall eintreten kann.

Bemerkung Ist (A, b) in Zeilenstufenform und gibt es ein i mit $r + 1 \leq i \leq n$ und $b_i \neq 0$, so ist

$$\text{Lös}(A, b) = \emptyset.$$

Beweis Die Gleichung mit der Nummer i lautet

$$0 \cdot x_1 + \dots + 0 \cdot x_n = b_i \neq 0.$$

Das kann kein x erfüllen, die restlichen Gleichungen können da nichts retten. ■

Wir können im Folgenden also $b_{r+1} = \dots = b_m = 0$ voraussetzen. Bevor wir eine allgemeine Lösungsmenge beschreiben, geben wir ein einfaches

Beispiel 1 Es sei $n = 4, m = r = 2$ und

$$(A, b) = \left(\begin{array}{ccc|c} 0 & 2 & 1 & 4 \\ 0 & 0 & 3 & 6 \end{array} \right).$$

In diesem Fall ist $j_1 = 2, a_{1j_1} = 2$ und $j_2 = 4, a_{2j_2} = 3$. Ausgeschrieben lautet das System

$$\begin{aligned} 2x_2 + x_3 + x_4 &= 4, \\ 3x_4 &= 6. \end{aligned} \quad (**)$$

Man kann erwarten, dass $\text{Lös}(A, b) \subset \mathbb{R}^4$ eine Ebene ergibt, dafür benötigt man zwei Parameter λ_1, λ_2 . Nun unterscheiden wir zwei Arten von Unbestimmten:

x_2 und x_4 stehen in Pivot-Positionen,
 x_1 und x_3 stehen in den verbleibenden Positionen.

Die Nicht-Pivot-Positionen 1 und 3 werden für Parameter freigegeben, man setzt also

$$x_1 = \lambda_1 \quad \text{und} \quad x_3 = \lambda_2.$$

Daraus berechnet man x_2 und x_4 von unten nach oben. Gleichung (2) lautet

$$3x_4 = 6, \quad \text{also ist} \quad x_4 = 2.$$

Gleichung (1) lautet

$$2x_2 + x_3 + x_4 = 4, \quad \text{also} \quad 2x_2 + \lambda_2 + 2 = 4 \quad \text{und} \quad x_2 = 1 - \frac{\lambda_2}{2}.$$

Das ergibt die Lösungen (als Zeile geschrieben)

$$x = (x_1, x_2, x_3, x_4) = \left(\lambda_1, 1 - \frac{\lambda_2}{2}, \lambda_2, 2 \right),$$

wobei $\lambda_1, \lambda_2 \in \mathbb{R}$ frei wählbare Parameter sind.

Um daraus eine Parameterdarstellung einer Ebene in der üblichen Form zu erhalten, benutzen wir die Vektoren

$$v := (0, 1, 0, 2), \quad w_1 := (1, 0, 0, 0) \quad \text{und} \quad w_2 := (0, -\frac{1}{2}, 1, 0).$$

Dann gilt für die oben berechnete Lösung x offensichtlich

$$x = v + \lambda_1 w_1 + \lambda_2 w_2, \quad \text{also ist } E := v + \mathbb{R} \cdot w_1 + \mathbb{R} \cdot w_2 \subset \text{Lös}(A, b).$$

Es ist sehr plausibel, dass die Lösungsmenge gleich der gefundenen Ebene E ist, das werden wir anschließend begründen.

Die Zerlegung $x = v + \lambda_1 w_1 + \lambda_2 w_2$ der Lösung kann man so beschreiben: Neben dem Gleichungssystem $A \cdot x = b$ betrachten wir das zugeordnete *homogene* System $A \cdot x = \mathbf{0}$, ausgeschrieben

$$\begin{aligned} 2x_2 + x_3 + x_4 &= 0, \\ 3x_4 &= 0. \end{aligned} \tag{*}$$

Setzt man hier $\lambda_1 = 1$ und $\lambda_2 = 0$, so erhält man die Lösung w_1 , mit $\lambda_1 = 0$ und $\lambda_2 = 1$ erhält man w_2 . Also ist

$$E_0 := \mathbb{R} \cdot w_1 + \mathbb{R} \cdot w_2 \subset \text{Lös}(A, \mathbf{0}).$$

Schließlich erhält man v als eine spezielle Lösung des ursprünglichen Systems (**), indem man $\lambda_1 = \lambda_2 = 0$ setzt.

Zur Beschreibung einer allgemeinen Lösungsmethode für den Fall, dass die Koeffizientenmatrix Zeilenstufenform hat, setzen wir zur Vereinfachung der Indizes voraus, dass

$$j_1 = 1, \quad j_2 = 2, \quad \dots, \quad j_r = r.$$

Dann ist

$$(A, b) = \left(\begin{array}{cccc|c} a_{11} & & & & b_1 \\ & a_{22} & & & b_2 \\ & & \ddots & & \vdots \\ & & & a_{rr} & b_r \\ & 0 & & & 0 \\ & & & & \vdots \\ & & & & 0 \end{array} \right).$$

Der entscheidende Kniff ist nun der, dass man die Werte von x_{r+1}, \dots, x_n in den Lösungen frei wählen kann, die Werte von x_1, \dots, x_r sind dadurch eindeutig festgelegt. Wir setzen also

$$x_{r+1} = \lambda_1, \dots, x_n = \lambda_k \quad \text{wobei} \quad k := n - r \geq 0.$$

Die Gleichung Nummer r lautet ausgeschrieben

$$a_{rr}x_r + a_{r,r+1}x_{r+1} + \dots + a_{rn}x_n = b_r.$$

Benutzt man $a_{rr} \neq 0$ und setzt man die Parameter ein, so folgt mit $\lambda := (\lambda_1, \dots, \lambda_k)$

$$x_r(\lambda) = \frac{1}{a_{rr}}(b_r - a_{r,r+1}\lambda_1 - \dots - a_{rn}\lambda_k) =: c_r + d_{r1}\lambda_1 + \dots + d_{rk}\lambda_k.$$

Setzt man diesen Wert von x_r und $x_{r+1} = \lambda_1, \dots, x_n = \lambda_k$ in die Gleichung Nummer $r - 1$ ein, so erhält man ein Ergebnis der Form

$$x_{r-1}(\lambda) = c_{r-1} + d_{r-1,1}\lambda_1 + \dots + d_{r-1,k}\lambda_k.$$

Rechnet man nun weiter von unten nach oben, so findet man schließlich

$$x_1(\lambda) = c_1 + d_{11}\lambda_1 + \dots + d_{1k}\lambda_k.$$

Genau genommen muss man die so erhaltenen Ausdrücke

$$x_1(\lambda), \dots, x_r(\lambda) \quad \text{und} \quad x_{r+1} = \lambda_1, \dots, x_n = \lambda_k$$

noch einmal in die Gleichungen einsetzen und kontrollieren, ob sie wirklich erfüllt sind. Das ist der Fall, also erhält man für jedes beliebige k -Tupel $\lambda = (\lambda_1, \dots, \lambda_k)$ eine durch λ eindeutig bestimmte Lösung

$$(x_1(\lambda), \dots, x_r(\lambda), \lambda_1, \dots, \lambda_k).$$

Abstrakter gesehen hat man die Abbildung

$$\varphi : \mathbb{R}^k \rightarrow \text{Lös}(A, b), \quad (\lambda_1, \dots, \lambda_k) \mapsto (x_1(\lambda), \dots, x_r(\lambda), \lambda_1, \dots, \lambda_k).$$

Damit kann man ein entscheidendes Zwischenergebnis formulieren:

Satz Gegeben sei ein lineares Gleichungssystem $Ax = b$ in Zeilenstufenform mit den Pivotpositionen $j_1 = 1, \dots, j_r = r$. Dann gilt

$$\text{Lös}(A, b) \neq \emptyset \quad \Leftrightarrow \quad b_{r+1} = \dots = b_m = 0.$$

Ist das der Fall, so hat die oben konstruierte Abbildung

$$\varphi : \mathbb{R}^k \rightarrow \text{Lös}(A, b), \quad (\lambda_1, \dots, \lambda_k) \mapsto (x_1(\lambda), \dots, x_r(\lambda), \lambda_1, \dots, \lambda_k)$$

folgende Eigenschaften:

- Ist $\lambda = (\lambda_1, \dots, \lambda_k)$ und $\lambda' = (\lambda'_1, \dots, \lambda'_k) \in \mathbb{R}^k$, so folgt aus $\lambda \neq \lambda'$, dass auch $\varphi(\lambda) \neq \varphi(\lambda')$.
- Ist $x^* = (x_1^*, \dots, x_n^*) \in \text{Lös}(A, b)$ irgendeine Lösung, so gibt es ein $\lambda \in \mathbb{R}^k$ mit $x^* = \varphi(\lambda)$.

In der Terminologie aus 1.1.3 besagen die Eigenschaften a) und b), dass die Abbildung φ bijektiv ist. Das bedeutet anders ausgedrückt, dass φ zwischen k -Tupeln von Parametern und den Lösungen des Gleichungssystems eine eindeutige Beziehung vermittelt. Damit kann man das Gleichungssystem als gelöst ansehen.

Noch eine Anmerkung zu den Zahlen m, n und r . Da nicht nur $r \leq m$ ist, sondern auch $r \leq n$ sein muss, ist ein Gleichungssystem mit $m > n$ im allgemeinen *überbestimmt*, d.h. es ist sehr leicht möglich, dass der Lösungsraum leer ist. Dieser Fall wird in 5.3.4 wieder aufgegriffen. Im Fall $m < n$ gibt es im Allgemeinen mehr als eine Lösung. Der Fall $m = n$ wird im anschließenden Korollar behandelt.

Beweis Teil a) ist ganz klar: Ist $\lambda \neq \lambda'$, so unterscheiden sich $\varphi(\lambda)$ und $\varphi(\lambda')$ in den Komponenten von $r + 1$ bis n , also ist $\varphi(\lambda) \neq \varphi(\lambda')$.

Zu b): Ist $x^* = (x_1^*, \dots, x_n^*)$ gegeben, so wählen wir dazu die Parameter

$$\lambda_1 := x_{r+1}^*, \dots, \lambda_k := x_n^*.$$

Das oben angegebene Verfahren zeigt, dass es dazu eindeutig bestimmte Werte

$$x_1(\lambda), \dots, x_r(\lambda)$$

gibt, so dass

$$(x_1(\lambda), \dots, x_r(\lambda), \lambda_1, \dots, \lambda_k) \in \text{Lös}(A, b).$$

Also muss $x_1(\lambda) = x_1^*, \dots, x_r(\lambda) = x_r^*$ sein, und es folgt $\varphi(\lambda_1, \dots, \lambda_k) = x^*$. ■

Wegen der besonderen Bedeutung der Abbildung φ wollen wir sie noch etwas übersichtlicher darstellen. In Matrixschreibweise ist im Fall $k \geq 1$

$$\begin{pmatrix} x_1 \\ \vdots \\ x_r \\ x_{r+1} \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} c_1 \\ \vdots \\ c_r \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} d_{11} & \cdots & d_{1k} \\ \vdots & & \vdots \\ d_{r1} & \cdots & d_{rk} \\ 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_k \end{pmatrix}.$$

Man kann die Abbildung φ auch als Parametrisierung schreiben. Dazu verwendet man (als Zeilen geschrieben) die Vektoren

$$\begin{aligned} v &:= (c_1, \dots, c_r, 0, \dots, 0) & , & & w_1 &:= (d_{11}, \dots, d_{r1}, 1, 0, \dots, 0), \\ & & & & w_2 &:= (d_{12}, \dots, d_{r2}, 0, 1, 0, \dots, 0), \\ & & & & \vdots & \\ & & & & w_k &:= (d_{1k}, \dots, d_{rk}, 0, \dots, 0, 1). \end{aligned}$$

Dann ist $\varphi(\lambda_1, \dots, \lambda_k) = v + \lambda_1 w_1 + \dots + \lambda_k w_k$; das ergibt die Parameterdarstellung

$$\text{Lös}(A, b) = v + \mathbb{R} \cdot w_1 + \dots + \mathbb{R} \cdot w_k.$$

Wie man ganz leicht sieht, sind w_1, \dots, w_k linear unabhängig.

Im Fall $b = 0$ ist $v = 0$. Offensichtlich ist dann

$$\text{Lös}(A, \mathbf{o}) = \mathbb{R} \cdot w_1 + \dots + \mathbb{R} \cdot w_k \subset \mathbb{R}^n,$$

das ist die Lösungsmenge des *homogenen* Systems $A \cdot x = \mathbf{o}$, ein Untervektorraum. Im Fall $b \neq 0$ nennt man v eine spezielle Lösung des *inhomogenen* Systems $A \cdot x = b$. Das kann man schließlich so schreiben:

$$\text{Lös}(A, b) = v + \text{Lös}(A, \mathbf{o}).$$

Besonders wichtig ist der Spezialfall $r = m = n$. In diesem Fall ist

$$(A, b) = \left(\begin{array}{cccc|c} a_{11} & & & & b_1 \\ & a_{22} & & & \vdots \\ & & 0 & \ddots & \vdots \\ & & & & a_{nn} \\ & & & & b_n \end{array} \right)$$

mit $a_{11} \neq 0, \dots, a_{nn} \neq 0$. Es gibt keine Parameter, da $k = n - r = 0$. Die letzte Gleichung lautet

$$a_{nn}x_n = b_n, \quad \text{also muss } x_n = \frac{b_n}{a_{nn}} \text{ sein.}$$

Setzt man diesen Wert in die vorletzte Gleichung ein, erhält man einen Wert für x_{n-1} und schließlich auch für x_1 . Man prüft sofort nach, dass mit diesen Werten alle Gleichungen erfüllt sind. Insbesondere ist $x_n = \dots = x_1 = 0$ für $b_n = \dots = b_1 = 0$. Damit ist bewiesen:

Korollar Ist die Koeffizientenmatrix eines Gleichungssystems mit n Gleichungen für n Unbestimmte in Zeilenstufenform mit $r = n$, so hat das Gleichungssystem genau eine Lösung. Ist das System homogen, so gibt es nur die triviale Lösung $(x_1, \dots, x_n) = (0, \dots, 0)$. ■

Beispiel 2 Wir geben noch eine Variante vom Beispiel 1 an. Es sei

$$(A, b) := \left(\begin{array}{cccc|c} 2 & 1 & 3 & 0 & 4 \\ 0 & 3 & 1 & 3 & 6 \end{array} \right).$$

Hier setzt man $x_3 = \lambda_1$ und $x_4 = \lambda_2$. Damit erhält man

$$x_2 = 2 - \frac{1}{3}\lambda_1 - \lambda_2 \quad \text{und} \quad x_1 = 1 - \frac{4}{3}\lambda_1 + \frac{1}{2}\lambda_2.$$

In Matrizenschreibweise übersetzt ist

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} -\frac{4}{3} & \frac{1}{2} \\ -\frac{1}{3} & -1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix}.$$

Diese Darstellung des Lösungsraumes, einer Ebene $E \subset \mathbb{R}^4$, ist nicht eindeutig. Lässt man das gleiche Beispiel etwa von MAPLE rechnen, erhält man folgendes „Worksheet“:

```
> restart: with (LinearAlgebra):
> A := Matrix([[2,1,3,0],[0,3,1,3]]);
```

$$A := \begin{bmatrix} 2 & 1 & 3 & 0 \\ 0 & 3 & 1 & 3 \end{bmatrix}$$

```
> b := <4,6>;
```

$$b := \begin{bmatrix} 4 \\ 6 \end{bmatrix}$$

```
> LinearSolve(A,b);
```

$$\begin{bmatrix} _t0_1 \\ -2_t0_1 + 4 - 3_t0_3 \\ _t0_3 \\ 2_t0_1 - 2 + \frac{8}{3}_t0_3 \end{bmatrix}$$

Hier werden $x_1 = _t0_1 =: \mu_1$ und $x_3 = _t0_3 =: \mu_3$ als Parameter gewählt, dann ist

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 4 \\ 0 \\ -2 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ -2 & -3 \\ 0 & 1 \\ 2 & \frac{8}{3} \end{pmatrix} \begin{pmatrix} \mu_1 \\ \mu_3 \end{pmatrix}.$$

Anders geschrieben ist das eine Parametrisierung

$$\text{Lös}(A, b) = v' + \mathbb{R} \cdot w'_1 + \mathbb{R} \cdot w'_2$$

mit $v' = (0, 4, 0, -2)$, $w'_1 = (1, -2, 0, 2)$, $w'_2 = (0, -3, 1, \frac{8}{3})$.

Der Leser möge sich zur Übung überlegen, wie man die beiden Parametrisierungen der Ebene $E \subset \mathbb{R}^4$ ineinander umrechnen kann.

0.5.4 Das GAUSSsche Eliminationsverfahren

Nachdem wir gesehen haben, wie übersichtlich sich ein lineares Gleichungssystem lösen lässt, wenn die Koeffizientenmatrix Zeilenstufenform hat, stellt sich die Frage, wie man ein gegebenes Gleichungssystem ohne Veränderung der Lösungsmenge auf diese Form bringen kann. Das geht mit einer *Elimination*, die in einfachen Fällen schon uralt ist, und die GAUSS systematisch als Hilfsmittel für seine „Methode der kleinsten Quadrate“ erstmals in der Himmelsmechanik angewandt hat [GA₂, p. 21]. Eine sehr ausführliche historische Abhandlung dazu findet man bei ([GRC]).

Wir benützen für die erweiterte Koeffizientenmatrix (A, b) eines linearen Gleichungssystems folgende **Zeilenumformungen** (dabei sei $i \neq k$):

- (1) Man vertauscht die Zeilen i und k .
- (2) Man zählt zur Zeile k das λ -fache der Zeile i dazu, wobei $\lambda \in \mathbb{R}$ beliebig ist.

Unser Problem ist gelöst durch folgenden

Hauptsatz

- a) Jede erweiterte Koeffizientenmatrix kann man durch endlich viele Zeilenumformungen vom Typ (1) und (2) auf Zeilenstufenform bringen.
- b) Ist (\tilde{A}, \tilde{b}) aus (A, b) durch elementare Zeilenumformungen entstanden, so gilt

$$\text{Lös}(\tilde{A}, \tilde{b}) = \text{Lös}(A, b).$$

Beweis Wir zeigen zunächst Teil b). Bei einer Umformung von Typ (1) wird nur die Reihenfolge der Bedingungen verändert; sie hat keinen Einfluß auf die Lösungen. Bei einer Umformung vom Typ (2) sind nur zwei der Bedingungen betroffen, die restlichen Bedingungen bleiben unverändert. Wir fassen jede Zeile von A als Vektor

$$s_i := (a_{i1}, \dots, a_{in}) \in \mathbb{R}^n$$

auf. Ist $x = (x_1, \dots, x_n)$, so bedeutet die Gleichung i , dass das Skalarprodukt $\langle s_i, x \rangle = b_i$ sein muss. Zu zeigen bleibt also, dass für alle $x \in \mathbb{R}^n$ bei beliebigem $\lambda \in \mathbb{R}$ gilt, dass

$$\left\{ \begin{array}{l} \langle s_i, x \rangle = b_i \\ \langle s_k, x \rangle = b_k \end{array} \right. \text{ und } \left. \right\} \Leftrightarrow \left\{ \begin{array}{l} \langle s_i, x \rangle = b_i \\ \langle s_k + \lambda s_i, x \rangle = b_k + \lambda b_i \end{array} \right. \text{ und } \left. \right\}.$$

Die beiden ersten Bedingungen sind gleich; es ist also zu zeigen, dass die beiden letzten Bedingungen äquivalent sind, wenn die erste erfüllt ist. Das folgt aus den Rechenregeln für das Skalarprodukt aus 0.3.1:

$$\text{„}\Rightarrow\text{“ } \langle s_k + \lambda s_i, x \rangle = \langle s_k, x \rangle + \lambda \langle s_i, x \rangle = b_k + \lambda b_i.$$

$$\text{„}\Leftarrow\text{“ } \langle s_k, x \rangle = \langle s_k + \lambda s_i - \lambda s_i, x \rangle = \langle s_k + \lambda s_i, x \rangle - \lambda \langle s_i, x \rangle = b_k + \lambda b_i - \lambda b_i = b_k.$$

Wenn die Lösungsmenge bei einer Umformung erhalten bleibt, dann auch bei mehreren hintereinander ausgeführten Umformungen. Damit ist b) bewiesen.

Zum Beweis von Teil a) geben wir eine Methode an, wie man (A, b) durch Umformungen vom Typ (1) und (2) auf Zeilenstufenform bringen kann.

Sind alle $a_{ij} = 0$, so hat (A, b) bereits Zeilenstufenform mit $r = 0$. Andernfalls suche man die von links gezählte erste Spalte mit einem Eintrag ungleich Null. Ist $a_{1j_1} \neq 0$, so nehme man diesen Eintrag als Pivot. Ist $a_{1j_1} = 0$, so nehme man eine Zeile i mit $a_{ij_1} \neq 0$ und vertausche sie mit der Zeile 1. Mit diesem neuen $\tilde{a}_{1j_1} = a_{ij_1}$ als Pivot mache man durch Umformungen vom Typ (2) alle darunter stehenden Einträge $a_{2j_1}, \dots, a_{mj_1}$ zu Null. Ist etwa $a_{2j_1} \neq 0$, so soll $a_{2j_2} + \lambda \tilde{a}_{1j_1} = 0$ sein. Also hat man

$$\lambda := -\frac{a_{2j_2}}{\tilde{a}_{1j_1}}$$

für die Umformung der zweiten Zeile zu wählen.

Im nächsten Schritt betrachtet man die nach den Umformungen entstandene Teilmatrix mit den Zeilen $i \geq 2$ und Spalten $j \geq j_1 + 1$. In dieser Teilmatrix verfährt man wie beim ersten Schritt: Man sucht die erste Spalte j_2 mit einem Eintrag ungleich Null, etc. Hat man schließlich ein Pivot $a_{rj_r} \neq 0$ gefunden, so dass nach den damit ausgeführten Umformungen in den Zeilen $i \geq r + 1$ und den Spalten $j \geq j_r + 1$ nur noch Nullen stehen, ist die Zeilenstufenform erreicht. ■

Man beachte, dass die b -Spalte laufend mit umgeformt wird, ohne Rücksicht auf die entstandenen Werte. Erst am Schluss entscheiden die Werte $\tilde{b}_{r+1}, \dots, \tilde{b}_m$, ob es überhaupt eine Lösung gibt (vgl. 0.5.3.).

Vorsicht! Wie wir gerade gesehen haben, ändern *Zeilenumformungen* der Koeffizientenmatrix nur die Form der Bedingungen für die unbekanntenen Größen x_j ; die Lösungsmenge bleibt unverändert. Ganz anders ist es bei *Spaltenumformungen*: Vertauschungen von Spalten vertauschen die Bedingungen zwischen verschiedenen Unbekannten. Bezeichnet x_1 die Anzahl von Äpfeln und x_2 die Anzahl von Birnen, so muss man bei Vertauschung der ersten und zweiten Spalte die Zuordnung ändern: Dann wird x_1 als Anzahl der Birnen und x_2 als Anzahl der Äpfel angesehen. Die Addition des Vielfachen einer Spalte zu einer anderen würde die Zuordnungen vermischen, das macht keinen Sinn.

Um die Rechnungen offensichtlich zu machen, geben wir ein Beispiel, bei dem alle Koeffizienten ganzzahlig bleiben. Wir wählen $n = 6$ und $m = 4$.

$$(A, b) = \left(\begin{array}{cccccc|c} 0 & 0 & 3 & 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 4 & 0 & 1 & 2 \\ 0 & -1 & 4 & -4 & 4 & 3 & 8 \\ 0 & 2 & 7 & 8 & 2 & 4 & 9 \end{array} \right) \quad j_1 = 2, \quad \text{vertausche Zeilen 1 und 2}$$

$$\left(\begin{array}{cccccc|c} 0 & 1 & 2 & 4 & 0 & 1 & 2 \\ 0 & 0 & 3 & 0 & 1 & 2 & 3 \\ 0 & -1 & 4 & -4 & 4 & 3 & 8 \\ 0 & 2 & 7 & 8 & 2 & 4 & 9 \end{array} \right) \quad 1 \text{ als Pivot}$$

$$\left(\begin{array}{cccccc|c} 0 & 1 & 2 & 4 & 0 & 1 & 2 \\ 0 & 0 & 3 & 0 & 1 & 2 & 3 \\ 0 & 0 & 6 & 0 & 4 & 4 & 10 \\ 0 & 0 & 3 & 0 & 2 & 2 & 5 \end{array} \right) \quad j_2 = 3, \quad 3 \text{ als Pivot}$$

$$\left(\begin{array}{cccccc|c} 0 & 1 & 2 & 4 & 0 & 1 & 2 \\ 0 & 0 & 3 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 2 & 0 & 4 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 \end{array} \right) \quad j_3 = 5, \quad 2 \text{ als Pivot}$$

$$\left(\begin{array}{cccccc|c} 0 & 1 & 2 & 4 & 0 & 1 & 2 \\ 0 & 0 & 3 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 2 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right) = (\tilde{A}, \tilde{b}).$$

In diesem Fall ist $r = 3$. Da $\tilde{b}_4 = 0$ ist die Lösungsmenge nicht leer; die Unbestimmten x_1, x_4 und x_6 können als freie Parameter gewählt werden.

Fazit Wir wollen das Ergebnis zusammenfassen: Ein vorgelegtes lineares Gleichungssystem $Ax = b$ kann man durch elementare Umformungen auf die Form $\tilde{A}x = \tilde{b}$ bringen, wobei \tilde{A} Zeilenstufenform hat. Dabei wird die Lösungsmenge nicht verändert, in Zeichen

$$\text{Lös}(\tilde{A}, \tilde{b}) = \text{Lös}(A, b).$$

Aus \tilde{A} erhält man eine kritische Zahl r von Pivotelementen und es gilt

$$\text{Lös}(A, b) \neq \emptyset \Leftrightarrow \tilde{b}_{r+1} = \dots = \tilde{b}_m = 0.$$

Ist diese Bedingung erfüllt, so erhält man mit $k := n - r$ eine Parametrisierung

$$\varphi: \mathbb{R}^k \rightarrow \text{Lös}(A, b)$$

(Satz aus 0.5.3). Damit ist das Gleichungssystem gelöst, denn man kann mit Hilfe von φ alle Lösungen explizit aufschreiben.

Man sollte nicht übersehen, dass eine wichtige Frage offen bleibt: Bei den Umformungen von (A, b) nach (\tilde{A}, \tilde{b}) gibt es zahlreiche Wahlmöglichkeiten, das Ergebnis (\tilde{A}, \tilde{b}) ist nicht eindeutig bestimmt. Insbesondere ist es nicht offensichtlich, dass die kritische Zahl r und damit $k = n - r$ eindeutig bestimmt ist. In Kapitel 2 wird das bewiesen, dazu ist etwas Theorie nötig:

- Die Zahl r ist der „Rang“ der Matrix A .
- Die Lösungsmenge $\text{Lös}(A, b) \subset \mathbb{R}^n$ ist ein „affiner Unterraum“, die Zahl $k = n - r$ ist seine „Dimension“, falls er nicht leer ist.

Die hier schon angekündigten Begriffe werden in Kapitel 2 entwickelt. Außerdem wird sich zeigen, dass man \mathbb{R} ersetzen kann durch einen beliebigen „Körper“ K . Was das ist, wird in Kapitel 1 erklärt.

Obwohl die Eindeutigkeit der Zahl r noch nicht bewiesen ist, können wir die Methoden zur Berechnung der Lösungen eines linearen Gleichungssystems bereits anwenden. Das wird vor allem bei der Behandlung von Beispielen nützlich sein.

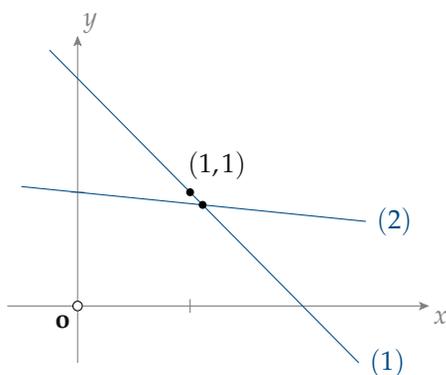
0.5.5 Wahl der Pivots und Rundungsfehler

Bei der Elimination in 0.5.4 hatten wir aus einer Spalte als Pivot einen beliebigen von Null verschiedenen Eintrag gewählt. Für die Theorie ist das ausreichend, weil man durch jede solche Zahl dividieren darf. In der Praxis aber können kleine Nenner unangenehme Rundungsfehler verursachen. Dafür geben wir ein ganz einfaches Beispiel. Wir betrachten die beiden Gleichungen

$$x + y = 2, \quad (1)$$

$$\varepsilon x + y = 1, \quad (2)$$

wobei ε eine kleine positive Zahl sein soll. Die durch die beiden Gleichungen beschriebenen Geraden sehen für $\varepsilon = \frac{1}{10}$ so aus:



Es ist klar, dass der Schnittpunkt der beiden Geraden für klein werdendes ε gegen $(1, 1)$ rückt. Zur Berechnung des Schnittpunkts verwenden wir zwei mögliche Pivots:

Mit 1 als Pivot erhalten wir die Gleichungen

$$x + y = 2, \quad (1)$$

$$(1 - \varepsilon)y = 1 - 2\varepsilon, \quad (\tilde{2})$$

also $y = \frac{1 - 2\varepsilon}{1 - \varepsilon}$ und $x = 2 - y$.

Verwenden wir ε als Pivot, so ergibt sich

$$\left(1 - \frac{1}{\varepsilon}\right)y = 2 - \frac{1}{\varepsilon}, \quad (\tilde{1})$$

$$\varepsilon x + y = 1, \quad (2)$$

also $y = \frac{2 - \frac{1}{\varepsilon}}{1 - \frac{1}{\varepsilon}} = \frac{1 - 2\varepsilon}{1 - \varepsilon}$ und $x = \frac{1}{\varepsilon}(1 - y)$.

Der Wert von y berechnet sich mit beiden Pivots gleich, bei der Berechnung von x mit dem Pivot ε wird die klein werdende Zahl $1 - y$ mit dem groß werdenden Faktor $\frac{1}{\varepsilon}$ multipliziert. Um ganz einfach zu sehen, welche Probleme dabei entstehen können, rechnen wir mit 4-stelligen Dezimalbrüchen und zwar nach der 4. Dezimalstelle entweder *abgeschnitten* oder in der 4. Dezimalstelle mit Hilfe der 5. Dezimalstelle *gerundet*. Zunächst berechnen wir die Werte von y in Abhängigkeit von ε :

ε	10^{-2}	10^{-3}	10^{-4}
y gerundet	0.9899	0.9990	0.9999
y abgeschnitten	0.9898	0.9989	0.9998

Daraus erhält man nach dem Ergebnis mit Pivot 1 die Werte von $x = 2 - y$:

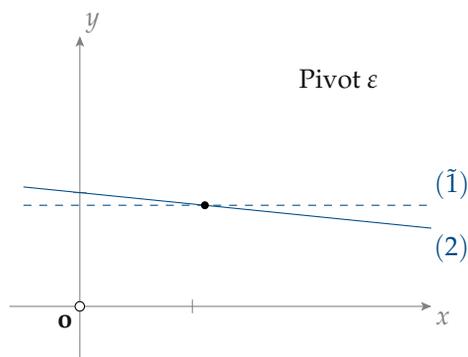
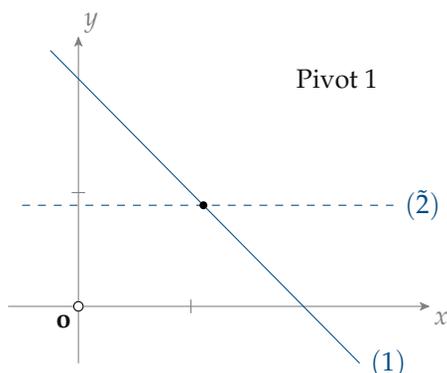
ε	10^{-2}	10^{-3}	10^{-4}
x aus y gerundet	1.0101	1.0010	1.0001
x aus y abgeschnitten	1.0102	1.0011	1.0002

Dagegen erhält man nach dem Ergebnis mit dem Pivot ε die Werte von $x = \frac{1}{\varepsilon}(1 - y)$:

ε	10^{-2}	10^{-3}	10^{-4}
x aus y gerundet	1.0100	1.0000	1.0000
x aus y abgeschnitten	1.0200	1.1000	2.0000

Wie man klar sieht, wirken sich die Schwankungen von y bei der Berechnung von x mit dem Pivot 1 nur in der vierten Dezimalstelle aus, beim Pivot ε werden sie dramatisch größer.

Um den geometrischen Hintergrund zu beleuchten, zeichnen wir die Geraden, die bei den Umformungen entstehen. Daran sieht man, dass mit dem Pivot ε ein „schleifender Schnitt“ entsteht.



Für numerische Rechnungen teuflisch sind die so genannten **HILBERT-Matrizen**, das sind $(n \times n)$ -Matrizen mit den rationalen Einträgen $a_{ij} = (i + j - 1)^{-1}$. Etwa für $n = 3$ ist

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

Ein Gleichungssystem $A \cdot x = b$ mit $b \in \mathbb{Q}^3$ ist durch fehlerfreie Rechnung mit rationalen Zahlen lösbar. Ist etwa $b = (1, 1, 1)$ so verläuft die Elimination wie folgt:

$$(A, b) = \left(\begin{array}{ccc|c} 1 & \frac{1}{2} & \frac{1}{3} & 1 \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & 1 \\ \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & 1 \end{array} \right)$$

$$\left(\begin{array}{ccc|c} 1 & \frac{1}{2} & \frac{1}{3} & 1 \\ 0 & \frac{1}{12} & \frac{1}{12} & \frac{1}{2} \\ 0 & \frac{1}{12} & \frac{4}{45} & \frac{2}{3} \end{array} \right)$$

$$(\tilde{A}, \tilde{b}) = \left(\begin{array}{ccc|c} 1 & \frac{1}{2} & \frac{1}{3} & 1 \\ 0 & \frac{1}{12} & \frac{1}{12} & \frac{1}{2} \\ 0 & 0 & \frac{1}{180} & \frac{1}{6} \end{array} \right)$$

und als exakte Lösung erhält man ohne Problem

$$x = (3, -24, 30).$$

Mehr als kritisch wird es, wenn man mit Dezimalbrüchen rechnet. Wir verwenden Gleitkommazahlen, bei jeder Rechenoperation wird auf zwei Stellen gerundet. Dann verläuft die Elimination wie folgt:

$$(A', b) = \left(\begin{array}{ccc|c} 1 & 0.5 & 0.33 & 1 \\ 0.5 & 0.33 & 0.25 & 1 \\ 0.33 & 0.25 & 0.2 & 1 \end{array} \right)$$

$$\left(\begin{array}{ccc|c} 1 & 0.5 & 0.33 & 1 \\ 0 & 0.08 & 0.08 & 0.5 \\ 0 & 0.08 & 0.09 & 0.67 \end{array} \right) \begin{array}{l} \text{Zeile (2) - 0.5 \cdot Zeile (1)} \\ \text{Zeile (3) - 0.33 \cdot Zeile (1)} \end{array}$$

$$(\tilde{A}', \tilde{b}) = \left(\begin{array}{ccc|c} 1 & 0.5 & 0.33 & 1 \\ 0 & 0.08 & 0.08 & 0.5 \\ 0 & 0 & 0.01 & 0.17 \end{array} \right) \text{Zeile (3) - Zeile (2)}$$

Das ergibt als Lösung von $\tilde{A}' \cdot x = \tilde{b}$

$$x = (0.9, -11, 17).$$

Rechnet man, ausgehend von A' und b , mit rationalen Zahlen, also mit $0.33 = \frac{33}{100}$, so erhält man die exakte Lösung

$$x = \left(\frac{100}{3}, -\frac{3800}{21}, \frac{3700}{21} \right) \approx (33, -181, 176).$$

von $A' \cdot x = b$. Daran ist zu sehen, dass die Rundung in den Einträgen von A in diesem Beispiel weit stärkere Auswirkung hat als die Rundungen bei der Elimination.

*Was beweisbar ist,
soll in der Wissenschaft
nicht ohne Beweis geglaubt werden*
RICHARD DEDEKIND

Kapitel 1

Grundlagen

In diesem Kapitel werden grundlegende Begriffe und Operationen beschrieben, die überall in der Mathematik vorkommen. Beginnend mit dem 19. Jahrhundert hat man versucht, die verwendeten Begriffe präzise zu definieren und möglichst strenge Beweise für alle Aussagen zu geben. Dabei ist die schon in der Antike in Griechenland benutzte Methode der *Axiome* in den Vordergrund gerückt. Gewisse grundlegende Aussagen werden „postuliert“, alles Weitere muss daraus nach den Gesetzen der Logik bewiesen werden.

Wer mehr an der Linearen Algebra und weniger an den Grundlagen interessiert ist, kann dieses ganze Kapitel zunächst überschlagen, mit Kapitel 2 fortfahren und nur bei Bedarf Einzelheiten aus Kapitel 1 nachlesen.

1.1 Mengen, Relationen, Abbildungen

1.1.1 Mengen und Teilmengen

Im Grunde geht es bei allen Fragen der Mathematik um *Mengen* und ihre „Strukturen“. G. CANTOR machte 1895 den folgenden Versuch einer Definition [CA₂]:

Unter einer ‚Menge‘ verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objecten m unsrer Anschauung oder unseres Denkens (welche die ‚Elemente‘ von M genannt werden) zu einem Ganzen.

In Zeichen drücken wir dies so aus:

$$(1) \quad M = \{m\}.$$

Das ist sehr suggestiv und für viele Zwecke ausreichend und unproblematisch.

Die einfachsten Mengen sind die *endlichen* Mengen, man kann sie im Prinzip durch die Liste Ihrer *Elemente* ausschreiben, in der Form

$$M = \{x_1, \dots, x_n\}, \quad x_i \in M \quad \text{für} \quad i \in \{1, \dots, n\}.$$

Dabei ist stets stillschweigend vorausgesetzt, dass alle x_i verschieden sind. Man kann dafür auch genauer sagen, die x_i sind *paarweise verschieden*, das heißt

$$x_i \neq x_j \quad \text{falls} \quad i, j \in \{1, \dots, n\} \quad \text{mit} \quad i \neq j.$$

Die Anzahl der Elemente von M nennt man auch *Mächtigkeit* von M , in Zeichen

$$\#(M) := n.$$

Im extremen Fall $n = 0$ hat M gar keine Elemente, eine solche Menge heißt *leer*, in Zeichen

$$M = \emptyset, \quad \#(\emptyset) = 0.$$

In der uns umgebenden Welt ist letztlich alles endlich. Aber in unserem Denken sind auch Vorgänge möglich, die kein Ende finden; etwa dann, wenn man nicht konkrete Dinge zählt, sondern abstrakt überlegt, dass man immer noch eins darauflegen könnte. Das führt zu unendlichen Mengen, die einfachste davon ist die Menge

$$\mathbb{N} := \{0, 1, 2, \dots\}$$

der natürlichen Zahlen. Für die Mächtigkeit kann man einfach

$$\#(\mathbb{N}) = \infty$$

schreiben. Wir werden später sehen, dass man bei unendlichen Mengen die Mächtigkeit sehr wohl differenzieren kann.

Aus einer Menge M kann man Elemente auswählen, die eine gewisse Eigenschaft E haben; etwa die geraden Zahlen aus $M = \{0, 1, \dots, 100\}$ oder die Primzahlen aus $M = \mathbb{N}$. Das führt zum Begriff der *Teilmenge*

$$M' := \{x \in M : x \text{ hat Eigenschaft } E\} \subset M.$$

Allgemeiner kann man eine Teilmenge abstrakter erklären:

$$M' \subset M \quad :\Leftrightarrow \quad \text{Wenn } x \in M', \text{ so folgt } x \in M.$$

M' heißt *echte Teilmenge* von M , in Zeichen

$$M' \subsetneq M,$$

wenn es mindestens ein $x \in M$ gibt mit $x \notin M'$. Besteht eine Teilmenge $M' \subset M$ aus einem einzigen Element x , so werden wir im Allgemeinen nicht zwischen der Teilmenge $M' = \{x\} \subset M$ und dem Element $x \in M$ unterscheiden.

In 1.2.1 werden wir beweisen, dass es in der endliche Menge $M = \{1, \dots, n\}$ genau 2^n verschiedene Teilmengen gibt. Im Sinn von CANTORS Definition kann man sich zu jeder beliebigen Menge M die Menge

$$\mathcal{P}(M) := \{M' : M' \subset M\}$$

der Teilmengen von M vorstellen; das nennt man die *Potenzmenge* von M .

Nun kann man seiner Phantasie weiter freien Lauf lassen und an die

Menge \mathcal{M} aller Mengen

denken. Jetzt gilt es aber die Luft anzuhalten: Wenn \mathcal{M} eine Menge ist, so gilt $\mathcal{M} \in \mathcal{M}$. Im Allgemeinen gilt für eine Menge jedoch $\mathcal{M} \notin \mathcal{M}$; das sieht man schon an $\mathcal{M} = \emptyset$. Nun wird man verführt, die Teilmenge

$$\mathcal{N} := \{M \in \mathcal{M} : M \notin M\} \subset \mathcal{M}$$

zu betrachten, und es stellt sich die berechnete Frage, ob $\mathcal{N} \in \mathcal{N}$ ist? Den Definitionen entsprechend gilt:

$$\mathcal{N} \in \mathcal{N} \Rightarrow \mathcal{N} \notin \mathcal{N} \quad \text{und} \quad \mathcal{N} \notin \mathcal{N} \Rightarrow \mathcal{N} \in \mathcal{N}, \quad \text{also} \quad \mathcal{N} \in \mathcal{N} \Leftrightarrow \mathcal{N} \notin \mathcal{N}.$$

Das ist die berühmte *Antinomie*, die B. RUSSEL 1903 entdeckt hat. Dadurch wurde die „naive“ Mengenlehre und somit das Fundament der ganzen Mathematik nachhaltig erschüttert. Es hat lange gedauert, bis mit einer axiomatischen Mengenlehre der Boden gefestigt werden konnte. Die Gesamtheit aller Mengen wird dabei nicht mehr als eine Menge angesehen, sondern nur noch als eine *Klasse* (vgl. etwa [EB]). Die Antinomie von RUSSEL kann man auch als *Paradoxon vom Barbier* formulieren, indem man ihn so erklärt:

Der Barbier ist derjenige, der all diejenigen - und nur diejenigen - rasiert, die sich nicht selbst rasieren.

Was dann, wenn dem Barbier sein eigener Bart zu lang geworden ist?

In der linearen Algebra werden wir diese Probleme dadurch umgehen, dass wir keine derart waghalsigen Konstruktionen mit Mengen ausführen. Vielmehr werden wir uns darauf beschränken, aus gegebenen Mengen mit Hilfe von elementaren Operationen neue Mengen zu konstruieren. Der theoretische Hintergrund eines solchen Verfahrens wird in [EB, Kap. 13] skizziert.

1.1.2 Operationen mit Mengen

Aus gegebenen Mengen M_1, \dots, M_n kann man neue konstruieren. Die *Vereinigung* ist erklärt durch

$$M_1 \cup \dots \cup M_n := \{x : x \in M_i \text{ für mindestens ein } i \in \{1, \dots, n\}\},$$

der *Durchschnitt* ist

$$M_1 \cap \dots \cap M_n := \{x : x \in M_i \text{ für alle } i \in \{1, \dots, n\}\}.$$

Im Fall $n = 2$ kann man das auch mit den Bedingungen *und* sowie *oder* ausdrücken, wobei „oder“ nicht das ausschließende „entweder oder“ bedeutet:

$$M_1 \cup M_2 = \{x : x \in M_1 \text{ oder } x \in M_2\}, \quad M_1 \cap M_2 = \{x : x \in M_1 \text{ und } x \in M_2\}.$$

Weiter kann man für zwei Mengen M, N die *Differenz*

$$M \setminus N := \{x \in M : x \notin N\} \subset M$$

bilden. Für diese Operationen gelten die folgenden

Rechenregeln Sind M, N_1, N_2 Mengen, so gilt

- a) $M \cap (N_1 \cup N_2) = (M \cap N_1) \cup (M \cap N_2)$, $M \cup (N_1 \cap N_2) = (M \cup N_1) \cap (M \cup N_2)$.
 b) $M \setminus (N_1 \cup N_2) = (M \setminus N_1) \cap (M \setminus N_2)$, $M \setminus (N_1 \cap N_2) = (M \setminus N_1) \cup (M \setminus N_2)$.

Zum *Beweis* muss man nur die logischen Regeln für „und“ sowie „oder“ benutzen. Wir zeigen die erste Regel von a):

$$\begin{aligned} x \in M \cap (N_1 \cup N_2) &\Leftrightarrow x \in M \text{ und } (x \in N_1 \text{ oder } x \in N_2) \\ &\Leftrightarrow (x \in M \text{ und } x \in N_1) \text{ oder } (x \in M \text{ und } x \in N_2) \\ &\Leftrightarrow (x \in M \cap N_1) \text{ oder } (x \in M \cap N_2) \\ &\Leftrightarrow x \in (M \cap N_1) \cup (M \cap N_2). \end{aligned}$$

Den Nachweis der anderen Regeln überlassen wir dem Leser zur Übung. ■

Sind wieder M_1, \dots, M_n beliebige Mengen, und ist für jedes $i \in \{1, \dots, n\}$ ein $x_i \in M_i$ ausgewählt, so bezeichnet man mit

$$(x_1, x_2, \dots, x_n) \quad \text{ein } \mathbf{geordnetes } n\text{-Tupel}.$$

Die charakteristische Eigenschaft eines geordneten n -Tupels ist die folgende: Sind auch $y_i \in M_i$ ausgewählt, so gilt

$$(x_1, \dots, x_n) = (y_1, \dots, y_n) \Leftrightarrow x_1 = y_1, \dots, x_n = y_n.$$

Als *direktes Produkt* der Mengen M_1, \dots, M_n bezeichnet man die Menge der geordneten n -Tupel, in Zeichen

$$M_1 \times \dots \times M_n := \{(x_1, \dots, x_n) : x_i \in M_i \text{ für } i \in \{1, \dots, n\}\}.$$

Sind die Mengen M_1, \dots, M_n alle gleich einem M , so setzen wir

$$M^n := \underbrace{M \times \dots \times M}_{n\text{-mal}}.$$

1.1.3 Abbildungen

Eine **Abbildung** f von einer Menge M in eine Menge N ist eine Vorschrift, die jedem Element $x \in M$ in eindeutiger Weise ein Element $y = f(x) \in N$ zuordnet. Dafür schreibt man in Zeichen

$$f : M \rightarrow N, \quad x \mapsto f(x).$$

Man beachte die beiden unterschiedlichen Pfeile: \rightarrow steht zwischen den Mengen, \mapsto zwischen einzelnen Elementen.

Genau genommen müsste man noch festlegen, welche Art von Vorschrift zur Definition einer Abbildung erlaubt ist. Aber darauf wollen wir verzichten; auch bei der Erklärung einer Teilmenge durch eine gewisse Eigenschaft haben wir nicht festgelegt, in welcher Form diese Eigenschaft gegeben sein soll. Beide Fragen stehen im Zusammenhang, denn eine Abbildung f kann man auch erklären durch ihren **Graphen**

$$\Gamma_f := \{(x, y) \in M \times N : y = f(x)\} \subset M \times N.$$

Die charakteristische Eigenschaft eines Graphen $\Gamma \subset M \times N$ als Teilmenge ist, dass es zu jedem $x \in M$ genau ein $y \in N$ gibt derart, dass $(x, y) \in \Gamma$.

Aus formalen Gründen betrachtet man für jede Menge M die **identische Abbildung**

$$id_M : M \rightarrow M, \quad x \mapsto x.$$

Ist $f : M \rightarrow N$ eine Abbildung und sind $M' \subset M$ und $N' \subset N$ Teilmengen, so heißt

$$f(M') := \{y \in N : \text{es gibt ein } x \in M' \text{ mit } y = f(x)\} \subset N$$

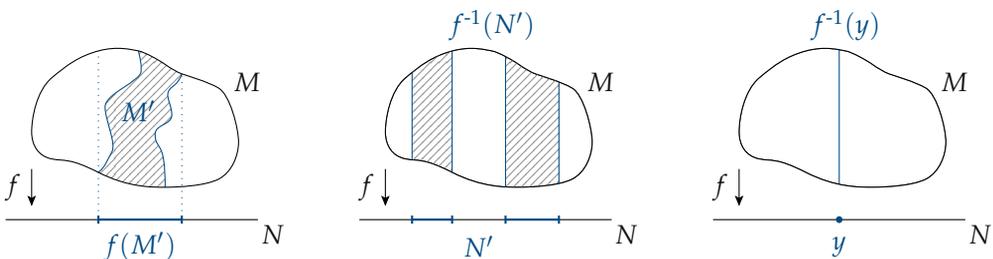
das **Bild** von M' in N und

$$f^{-1}(N') := \{x \in M : f(x) \in N'\} \subset M$$

das **Urbild** von N' in M . Besteht N' nur aus einem Element, so heißt

$$f^{-1}(y) := \{x \in M : f(x) = y\} \subset M$$

die **Faser** von y in M . Ist die Abbildung f durch die senkrechte Projektion gegeben, so kann man diese Teilmengen leicht zeichnen:



Durch **Einschränkung** von $f : M \rightarrow N$ auf eine Teilmenge $M' \subset M$ erhält man eine Abbildung

$$f|_{M'} : M' \rightarrow N \quad \text{mit} \quad (f|_{M'})(x) = f(x) \quad \text{für alle} \quad x \in M'.$$

Die Einschränkung ist formal von f zu unterscheiden, da sie einen kleineren Definitionsbereich haben kann.

Für besonders wichtige Eigenschaften von Abbildungen gibt es eigene Namen.

Definition Eine Abbildung $f : M \rightarrow N$ heißt

- injektiv** $:\Leftrightarrow$ aus $f(x) = f(x')$ folgt $x = x'$,
surjektiv $:\Leftrightarrow$ zu jedem $y \in N$ gibt es mindestens ein $x \in M$ so dass $y = f(x)$,
bijektiv $:\Leftrightarrow$ f ist injektiv und surjektiv,
 d.h. zu jedem $y \in N$ gibt es genau ein $x \in M$ so dass $y = f(x)$.

Die Abbildung

$$f : \mathbb{N} \rightarrow \mathbb{N}, \quad x \mapsto 2x,$$

ist injektiv, aber nicht surjektiv; die Abbildung

$$f : \mathbb{N} \rightarrow \mathbb{N}, \quad f(x) := \begin{cases} x - 1 & \text{für } x \geq 1 \\ 0 & \text{für } x = 0 \end{cases}$$

ist surjektiv, aber nicht injektiv. Für endliche Mengen gilt das auf den ersten Blick erstaunliche

Apfel-Lemma Seien M, N endliche Mengen mit gleich vielen Elementen. Dann sind für eine Abbildung $f : M \rightarrow N$ folgende Aussagen äquivalent:

- i) f ist injektiv,
- ii) f ist surjektiv,
- iii) f ist bijektiv.

Die Aussage wird sehr plausibel, wenn man sich eine konkrete Situation vorstellt: Auf n Personen sollen n Äpfel verteilt werden. Erhält eine Person mehr als einen Apfel, so geht eine andere leer aus. Will eine Person keinen Apfel, muss irgend ein anderer mindestens zwei nehmen.

Sicherheitshalber noch ein abstrakter

Beweis Um die Äquivalenz der drei Aussagen zu zeigen, beweisen wir sie nach dem Schema:

$$\begin{array}{ccc} & i) & \\ & \swarrow & \nwarrow \\ ii) & \Leftrightarrow & iii). \end{array}$$

Mit $n := \#M = \#N$ bezeichnen wir die Anzahl der Elemente. Für $n = 0$ ist nichts zu beweisen, sei also $n \geq 1$.

i) \Rightarrow ii) Ist f nicht surjektiv, so ist

$$m := \#(f(M)) < n.$$

Die Geschichte mit den Äpfeln heißt auch **Schubkastenprinzip** nach DIRICHLET:

Verteilt man n Objekte auf m Schubladen und ist $m < n$, so muss in mindestens einer Schublade mehr als ein Objekt liegen.

Also kann f nicht injektiv sein.

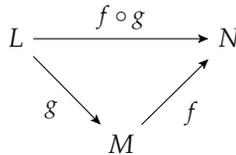
ii) \Rightarrow iii) Angenommen f wäre surjektiv, aber nicht bijektiv, dann wäre f nicht injektiv. Also gäbe es $x, x' \in M$ mit $x \neq x'$, aber $f(x) = f(x')$. Dann wäre aber $\#f(M) < n$, im Widerspruch zur angenommenen Surjektivität.

iii) \Rightarrow i) Folgt aus der Definition. ■

Hat man Mengen L, M, N und Abbildungen $f : M \rightarrow N$, $g : L \rightarrow M$, so kann man eine **Komposition** (oder Hintereinanderschaltung)

$$f \circ g : L \rightarrow N, \quad z \mapsto f(g(z))$$

erklären. Hier ist die Reihenfolge zu bedenken:



Für $f \circ g$ sagt man am besten: „ f nach g “.

Ist $f : M \rightarrow N$ bijektiv, so besteht die Faser $f^{-1}(y)$ für jedes $y \in N$ aus genau einem Element $x \in M$. Auf diese Weise erhält man eine Umkehrabbildung

$$f^{-1} : N \rightarrow M, \quad y \mapsto f^{-1}(y) = x.$$

Man beachte dabei, dass das für die Faser benutzte Symbol f^{-1} in diesem Fall auch für eine Abbildung verwendet wird. Offensichtlich gilt für eine bijektive Abbildung $f : M \rightarrow N$, dass

$$f \circ f^{-1} = id_N \quad \text{und} \quad f^{-1} \circ f = id_M.$$

Das kann man sich auch an dem Diagramm

$$N \xrightarrow{f^{-1}} M \xrightarrow{f} N \xrightarrow{f^{-1}} M$$

klar machen. Nützlich ist die folgende

Bemerkung 1 Sei $f : M \rightarrow N$ eine Abbildung zwischen den nicht leeren Mengen M, N . Dann gilt

- a) f ist genau dann injektiv, wenn es eine Abbildung $g : N \rightarrow M$ gibt, so dass $g \circ f = id_M$.
 b) f ist genau dann surjektiv, wenn es eine Abbildung $g : N \rightarrow M$ gibt, so dass $f \circ g = id_N$.
 c) f ist genau dann bijektiv, wenn es eine Abbildung $g : N \rightarrow M$ gibt, so dass $g \circ f = id_M$ und $f \circ g = id_N$.

Vorsicht! Man beachte, dass die Bedingung aus a) nicht für Surjektivität und die Bedingung b) nicht für die Injektivität hinreichend ist. Der Leser möge sich Gegenbeispiele mit der unendlichen Menge $M = N = \mathbb{N}$ überlegen!

Beweis Ad a) Hier kommt g nach f , man hat also das Diagramm

$$M \xrightarrow{f} N \xrightarrow{g} M.$$

Die Idee ist, dass g nicht mehr auseinander nehmen kann, was f zusammengeworfen hat. Genauer: ist f nicht injektiv, so gibt es $x, x' \in M$ mit $x \neq x'$ und $f(x) = f(x')$. Dann ist für jedes $g : N \rightarrow M$

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

Also kann $g \circ f$ nicht injektiv sein, und $g \circ f = id_M$ ist unmöglich.

Ist dagegen f injektiv, so gibt es zu jedem $y \in f(M)$ genau ein $x \in M$ mit $f(x) = y$, und wir können $g(y) := x$ definieren. Alle $y \in N \setminus f(M)$ können wir mit g auf ein beliebiges $x_0 \in M$ abbilden. Das so definierte g erfüllt die Bedingung $g \circ f = id_M$.

Ad b) Hier kommt g vor f :

$$N \xrightarrow{g} M \xrightarrow{f} N.$$

Lässt f einen Lücke in N , so kann g das nicht auffüllen. Genauer: Ist f nicht surjektiv, so gibt es ein $y_0 \in N \setminus f(M)$. Da offensichtlich

$$(f \circ g)(N) = f(g(N)) \subset f(M) \subsetneq N$$

ist $f \circ g = id_N$ mit keinem g möglich.

Ist umgekehrt f surjektiv, so wählen wir zu jedem $y \in N$ ein $x \in M$ mit $f(x) = y$ aus, und definieren $g(y) := x$. Dann ist $f \circ g = id_N$.

Ad c) Ist f bijektiv, so kann man $g := f^{-1}$ setzen. Ist f nicht bijektiv, so ist es nicht injektiv oder nicht surjektiv und die Behauptung folgt mit Hilfe von a) und b). ■

Ganz einfach zeigt man die

Bemerkung 2 Sind $f : M \rightarrow N$ und $g : L \rightarrow M$ bijektiv, so ist $f \circ g : L \rightarrow N$ bijektiv und $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

1.1.4 Abzählbare Mengen*

Bei der Definition der Mächtigkeit von Mengen in 1.1.1 hatten wir zunächst nur unterschieden, ob sie endlich oder unendlich sind. CANTOR hat in seinen grundlegenden Untersuchungen begonnen, auch die Mächtigkeit unendlicher Mengen zu differenzieren. Insbesondere hat er gezeigt, dass es Mengen gibt, die noch unendlicher sind, als die Menge \mathbb{N} der natürlichen Zahlen. Wir beginnen mit einer naheliegenden

Definition Zwei Mengen M und N heißen **gleichmächtig**, wenn es eine bijektive Abbildung $f : M \rightarrow N$ gibt.

Eine Menge M heißt **abzählbar unendlich**, wenn sie mit \mathbb{N} gleichmächtig ist, d.h. es eine bijektive Abbildung $f : \mathbb{N} \rightarrow M$ gibt.

Eine Menge heißt **abzählbar**, wenn sie endlich oder abzählbar unendlich ist.

Ist M endlich und $M' \subset M$, so sind offensichtlich M und M' genau dann gleichmächtig, wenn $M' = M$. Bei unendlichen Mengen ist das ganz anders. Als ersten Schritt notieren wir die

Bemerkung Die Menge \mathbb{Z} der ganzen Zahlen ist abzählbar unendlich.

Beweis Wir geben eine bijektive Abbildung $f : \mathbb{N} \rightarrow \mathbb{Z}$ an, das entspricht einer Abzählung von \mathbb{Z} . Eine naheliegende Reihenfolge ist

$$\mathbb{Z} = \{0, +1, -1, +2, -2, \dots\}.$$

Dem entspricht formal aufgeschrieben die Abbildung f mit

$$f(n) := \begin{cases} -i & \text{für } n = 2i \\ i + 1 & \text{für } n = 2i + 1 \end{cases}$$



Dass es noch weit „größere“ abzählbare Mengen gibt, zeigt der

Satz 1 Die Menge \mathbb{Q} der rationalen Zahlen ist abzählbar unendlich.

Beweis Wir benutzen das erste **Diagonalverfahren** von CANTOR, bei dem eine surjektive Abbildung

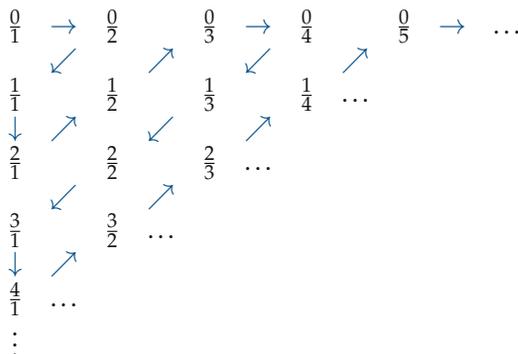
$$g : \mathbb{N} \rightarrow \mathbb{Q}_+ := \left\{ \frac{m}{n} \in \mathbb{Q} : n > 0, m \geq 0 \right\}$$

konstruiert wird. Dass \mathbb{Q}_+ abzählbar ist, folgt dann aus dem später bewiesenen

Lemma Gibt es zu einer Menge M eine surjektive Abbildung $g : \mathbb{N} \rightarrow M$, so ist M abzählbar.

Dass mit \mathbb{Q}_+ auch \mathbb{Q} abzählbar ist, folgt dann wie in der obigen Bemerkung. ■

Man schreibt nun die Brüche in einem unendlichen Schema auf, bei dem die Zeilen dem Zähler und die Spalten dem Nenner entsprechen. Dann zählt man beginnend mit $\frac{0}{1}$ wie durch die Pfeile angedeutet:



Das ergibt eine surjektive Abbildung $g : \mathbb{N} \rightarrow \mathbb{Q}$ mit folgenden Werten:

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	...
$g(i)$	0	0	1	2	$\frac{1}{2}$	0	0	$\frac{1}{3}$	1	3	4	$\frac{3}{2}$	$\frac{2}{3}$	$\frac{1}{4}$	0	...

Da die Darstellung einer rationalen Zahl nicht eindeutig ist, wird bei diesem Verfahren jedes $x \in \mathbb{Q}$ unendlich oft gezählt. Aus g erhält man jedoch leicht eine bijektive Abbildung f , indem man schon in anderer Darstellung gezählte x überspringt. Dann hat f folgende Werte

n	0	1	2	3	4	5	6	7	8	9	...
$f(n)$	0	1	2	$\frac{1}{2}$	$\frac{1}{3}$	3	4	$\frac{3}{2}$	$\frac{2}{3}$	$\frac{1}{4}$...

Etwas formaler erhält man auf diese Weise einen

Beweis des Lemmas Es ist zu zeigen, dass M endlich oder abzählbar unendlich ist. Dazu konstruieren wir eine Folge

$$0 = i_0 < i_1 < \dots < i_k < \dots$$

derart, dass durch $f(k) := g(i_k)$ eine Abbildung

$$f: \mathbb{N} \rightarrow M$$

entsteht, die für unendliches M bijektiv wird.

Wir beginnen mit $i_0 = 0$ und $f(0) := g(i_0) = g(0)$. Da g nicht injektiv sein muss, betrachten wir die Menge

$$A_0 := g^{-1}(g(i_0)) \subset \mathbb{N}.$$

Ist $A_0 = \mathbb{N}$, so ist $M = \{g(0)\}$, also endlich. Andernfalls ist $\mathbb{N} \setminus A_0 \neq \emptyset$; sei $i_1 \in \mathbb{N} \setminus A_0$ die kleinste Zahl. Da $i_0 \in A_0$ ist $i_1 > i_0$ und es folgt

$$f(1) := g(i_1) \neq g(i_0) = f(0).$$

Im nächsten Schritt betrachtet man die Menge

$$A_1 := g^{-1}(g(i_1)).$$

Ist $A_0 \cup A_1 = \mathbb{N}$, so folgt $M = \{g(i_0), g(i_1)\}$. Andernfalls sei i_2 die kleinste Zahl in $\mathbb{N} \setminus (A_0 \cup A_1)$. Setzt man $f(2) := g(i_2)$, so folgt $f(2) \neq f(0)$ und $f(2) \neq f(1)$.

Ganz allgemein hat man folgende Alternative: Stößt man im Verlauf dieses Verfahrens auf eine Zahl $m \in \mathbb{N}$, so dass

$$A_0 \cup \dots \cup A_m = \mathbb{N},$$

so ist $M = \{g(i_0), \dots, g(i_m)\}$, also endlich. Andernfalls wird die durch $f(k) := g(i_k)$ definierte Abbildung bijektiv.

Wir haben im Beweis benutzt, dass jede nicht leere Teilmenge von \mathbb{N} ein kleinstes Element enthält. Das wird in 1.2.1 näher erläutert. ■

Betrachten wir noch einmal die Mengen

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

Wie wir gesehen haben, hat sich die Mächtigkeit von \mathbb{N} bis \mathbb{Q} nicht vergrößert. Anders ist es mit \mathbb{R} :

Satz 2 Die Menge \mathbb{R} der reellen Zahlen ist nicht abzählbar.

Beweis Hier benutzen wir das zweite *Diagonalverfahren* von CANTOR. Zunächst aber zwei Vorbereitungen.

Es genügt zu zeigen, dass das halboffene Intervall $[0,1[$ nicht abzählbar ist. Denn wäre \mathbb{R} abzählbar, so könnte man aus der bijektiven Abbildung $f : \mathbb{N} \rightarrow \mathbb{R}$ durch

$$g(n) := \begin{cases} f(n), & \text{falls } f(n) \in [0,1[, \\ 0, & \text{falls } f(n) \notin [0,1[, \end{cases}$$

eine surjektive Abbildung $g : \mathbb{N} \rightarrow [0,1[$ erhalten und nach dem Lemma wäre $[0,1[$ abzählbar.

Wir wie in 1.3.5 näher begründen werden, hat jede reelle Zahl $x \in [0,1[$ eine eindeutige Darstellung als Dezimalbruch

$$x = 0.a_1a_2\cdots = \sum_{i=1}^{\infty} a_i \cdot 10^{-i}$$

ohne unendliche Neunerperioden. Daher ist das Intervall $[0,1[$ gleichmächtig mit der Menge dieser Dezimalbrüche.

Angenommen $[0,1[$ wäre abzählbar. Damit die Indizes schöner laufen, nehmen wir eine bijektive Abbildung

$$f : \mathbb{N}^* \rightarrow [0,1[, \quad i \mapsto x_i.$$

Für die Dezimalbruchentwicklung der x_i benötigen wir Doppellindizes:

$$\begin{aligned} x_1 &= 0.a_{11}a_{12}a_{13}\cdots \\ x_2 &= 0.a_{21}a_{22}a_{23}\cdots \\ x_3 &= 0.a_{31}a_{32}a_{33}\cdots \\ &\vdots \quad \quad \quad \vdots \end{aligned}$$

Da f als surjektiv angenommen ist, müssen alle $x \in [0,1[$ in dieser Folge vorkommen. Nun betrachten wir aber

$$x := 0.b_1b_2b_3\cdots \quad \text{mit} \quad b_i := \begin{cases} 0, & \text{falls } a_{ii} \neq 0, \\ 1, & \text{falls } a_{ii} = 0. \end{cases}$$

Käme x in der Folge vor, so müsste $x = x_j$ für ein $j \in \mathbb{N}^*$, also $b_j = a_{jj}$ sein. Das widerspricht der Definition von b_j .

Man hüte sich vor dem oft vorgebrachten Einwand, dieses eine x könnte man ja noch nachträglich dazunehmen! Der Beweis ist indirekt: Man nimmt an, alle wären unter dem Hut; dann findet man dennoch ein weiteres x . ■

Dass es so viel mehr reelle als rationale Zahlen gibt, ist geometrisch schwer zu verstehen. Eine Konstruktion der reellen Zahlen aus den rationalen Zahlen wird in 1.3.4 skizziert. Noch erstaunlicher erscheint auf den ersten Blick das

Korollar Für jedes reelle $\varepsilon > 0$ ist das Intervall $[0, \varepsilon[$ nicht abzählbar.

Beweis Die Abbildung

$$[0, 1[\longrightarrow [0, \varepsilon[, \quad x \mapsto \varepsilon \cdot x,$$

ist bijektiv. ■

Der Leser möge zur Übung nachweisen, dass auch die Menge aller $\{0, 1\}$ -Folgen, das ist die Menge der Abbildungen

$$\mathbb{N} \longrightarrow \{0, 1\},$$

nicht abzählbar ist.

1.1.5 Äquivalenzrelationen*

Für eine rationale Zahl gibt es viele verschiedene Darstellungen, etwa

$$\frac{1}{2} = \frac{2}{4} = \frac{17}{34} = \dots$$

Sie sind nicht gleich, aber „gleichwertig“. Auch zwei verschiedene Mengen M, N kann man gleichwertig nennen, wenn es eine bijektive Abbildung $M \rightarrow N$ gibt. Was als gleichwertig oder *äquivalent* betrachtet wird, hängt davon ab, was als wesentlich angesehen wird. Die *Identifikation* von äquivalenten Objekten ist eine in der Mathematik sehr oft angewandte Methode der Vereinfachung. Wir beschreiben hier zunächst den formalen Rahmen.

Für Elemente x, y einer Menge M kann man durch $x \sim y$ eine beliebige *Relation* R anzeigen. Ist etwa M die Menge der Bewohner einer Stadt, so kann die Relation \sim erklärt werden durch

$$x \sim y \Leftrightarrow x \text{ kennt } y.$$

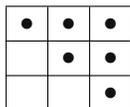
Das kann man schematisch beschreiben durch die Teilmenge

$$R := \{(x, y) \in M \times M : x \sim y\},$$

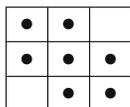
die man den *Graphen* der Relation nennt. Ist M endlich, so kann man den Graphen auch in Form einer Matrix schreiben. Für $M = \{1, 2, 3\}$ geben wir einige Beispiele:

•		
	•	
		•

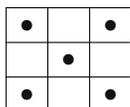
$$x \sim y \Leftrightarrow x = y$$



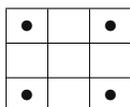
$$x \sim y :\Leftrightarrow x \leq y$$



Jedes x kennt sich selbst.
 1 und 2, sowie 2 und 3 kennen sich.
 1 und 3 kennen sich nicht.



Jedes x kennt sich selbst.
 1 und 3 kennen sich.
 2 kennt nur sich selbst.



1 und 3 kennen sich selbst und kennen einander.
 2 kennt nicht einmal sich selbst.

Um von Gleichwertigkeit sprechen zu können, muss eine Relation besondere Eigenschaften haben.

Definition Eine Relation \sim auf einer Menge M heißt **Äquivalenzrelation**, wenn für alle $x, y, z \in M$ gilt:

- A1 $x \sim x$, *Reflexivität,*
- A2 $x \sim y \Rightarrow y \sim x$, *Symmetrie,*
- A3 $x \sim y$ und $y \sim z \Rightarrow x \sim z$, *Transitivität.*

Das schärfste Beispiel einer Äquivalenzrelation ist die Gleichheit. In diesem Fall ist der Graph die „Diagonale“

$$\Delta = \{(x, y) \in M \times M : x = y\}.$$

Der Leser möge zur Übung prüfen, welche der drei Bedingungen für eine Äquivalenzrelation in den oben angegebenen fünf Beispielen erfüllt sind.

Grundlegend für die Zahlentheorie ist die von GAUSS eingeführte **Kongruenz** als Abschwächung der Gleichheit in \mathbb{Z} . Dazu wird als **Modul** ein $m \in \mathbb{N}$ gewählt und man definiert für $x, y \in \mathbb{Z}$

$$x \equiv y \pmod{m} \quad :\Leftrightarrow \quad m \text{ teilt } y - x, \text{ d.h. es gibt ein } k \in \mathbb{Z} \text{ mit } y - x = k \cdot m.$$

Man sagt dafür „ x kongruent y modulo m “. Offensichtlich gilt

$$x \equiv y \pmod{0} \quad \Leftrightarrow \quad x = y.$$

Bemerkung Die Kongruenz ist für jeden Modul $m \in \mathbb{N}$ eine Äquivalenzrelation in \mathbb{Z} .

Zum Beweis benutzen wir die elementaren Regeln der Teilbarkeit in \mathbb{Z} .

A1 m teilt $x - x = 0$, denn $0 = 0 \cdot m$.

A2 m teilt $y - x$ besagt $y - x = k \cdot m$. Also ist $x - y = -k \cdot m$.

A3 Aus $y - x = k \cdot m$ und $z - y = l \cdot m$ folgt $z - x = (k + l) \cdot m$. ■

Ist in einer Menge M eine Äquivalenzrelation \sim gegeben, so ist es naheliegend, zu einem $x \in M$ die Menge

$$A_x := \{x' \in M : x \sim x'\}$$

der zu x äquivalenten Elemente zu betrachten. Man nennt A_x die **Äquivalenzklasse** von x . Durch die Äquivalenzklassen erhält man eine disjunkte Zerlegung von M . Genauer gilt die

Bemerkung Für Elemente $x, y \in M$ gilt

a) $A_x = A_y \Leftrightarrow x \sim y$.

b) $A_x \cap A_y = \emptyset$ oder $A_x = A_y$.

Beweis Ad a) „ \Rightarrow “ Nach A1 ist $y \in A_y$. Da auch $y \in A_x$ folgt $x \sim y$.

„ \Leftarrow “ $A_y \subset A_x$. Ist $y' \in A_y$, so gilt $y \sim y'$. Wegen $x \sim y$ folgt $x \sim y'$ nach A3, also ist $y' \in A_x$. $A_x \subset A_y$ kann man analog beweisen, denn nach A2 ist auch $y \sim x$.

Ad b) Ist $A_x \cap A_y \neq \emptyset$, so gibt es ein $z \in A_x \cap A_y$. Aus

$$x \sim z \text{ und } y \sim z \text{ folgt } z \sim y \text{ und } x \sim y,$$

also ist $A_x = A_y$ nach a). ■

Nun erfolgt ein Schritt der Abstraktion, der in der Mathematik immer wieder vorkommt, der aber gewöhnungsbedürftig ist: Man betrachtet die Äquivalenzklassen – das sind Teilmengen von M – als Elemente einer neuen Menge der

Menge M/\sim **der Äquivalenzklassen**

nach der gegebenen Äquivalenzrelation \sim . Weiter hat man eine kanonische Abbildung

$$\rho : M \rightarrow M/\sim, \quad x \mapsto A_x,$$

die nach Definition surjektiv ist.

Schwierigkeiten bei der Konstruktion von Äquivalenzklassen bereitet vor allem der Umstand, dass plötzlich Mengen zu Elementen werden. Die RUSSELLsche Antinomie aus 1.1.1 hat gezeigt, wohin es führt, wenn man es zu toll damit treibt. Aber so lange man

bei den Teilmengen einer vorgegebenen Menge bleibt, ist das ungefährlich. Und wie nützlich diese Konstruktion ist, kann man besonders einfach am Beispiel der rationalen Zahlen sehen, die schon in 0.1.1 erklärt wurden und in 1.3.2 noch einmal ausführlicher behandelt werden. Hier nur ein kurzer Hinweis:

$$\text{Was bedeutet die Gleichheit } \frac{1}{2} = \frac{3}{6} ?$$

Die Menge M aller Brüche $\frac{m}{n}$ mit $m \in \mathbb{Z}$ und $n \in \mathbb{N}^*$ kann man formal erhalten aus der Menge von geordneten Paaren

$$M = \mathbb{Z} \times \mathbb{N}^* = \{(m, n) : m \in \mathbb{Z}, n \in \mathbb{N}^*\}.$$

In M hat man eine Äquivalenzrelation

$$(m, n) \sim (m', n') \Leftrightarrow m \cdot n' = n \cdot m',$$

also etwa $(1, 2) \sim (3, 6)$, denn $1 \cdot 6 = 2 \cdot 3$. Bezeichnet man mit

$$\frac{m}{n} \text{ die Äquivalenzklasse von } (m, n),$$

dann hat man für die Gleichheit von Äquivalenzklassen die Regel

$$\frac{m}{n} = \frac{m'}{n'} \Leftrightarrow m \cdot n' = n \cdot m'.$$

Insbesondere gilt $\frac{1}{2} = \frac{3}{6}$. In diesem Sinne kann man eine rationale Zahl ansehen als eine Klasse äquivalenter Bruchdarstellungen, d.h. eine spezielle Teilmenge von $\mathbb{Z} \times \mathbb{N}^*$.

Nach diesem etwas abstrakten Blick auf die guten alten rationalen Zahlen wollen wir in \mathbb{Z} die Äquivalenzklassen unter der Kongruenz nach einem Modul $m \in \mathbb{N}^*$ betrachten. Dazu benützen wir ein in 1.3.1 näher begründetes Verfahren der

Teilung mit Rest in \mathbb{Z} Zu $x \in \mathbb{Z}$ und $m \in \mathbb{N}^*$ gibt es eindeutig bestimmte Zahlen $q \in \mathbb{Z}$ und $r \in \mathbb{N}$ mit

$$x = q \cdot m + r \quad \text{und} \quad 0 \leq r < m.$$

Man kann diese Bezeichnung auch als Gleichung in \mathbb{Q} schreiben:

$$\frac{x}{m} = q + \frac{r}{m}.$$

Die Zahl $q \in \mathbb{Z}$ ist ein „unvollständiger Quotient“, r ist der kleinste nicht negative „Rest“.

Damit kann man die Kongruenzen so beschreiben:

Lemma der kleinsten Reste Für Zahlen $x, y \in \mathbb{Z}$ und $m \in \mathbb{N}^*$ ist $x \equiv y \pmod{m}$ äquivalent dazu, dass x und y bei Teilung durch m den gleichen kleinsten Rest lassen.

Beweis Wir teilen x und y mit Rest durch m :

$$x = q \cdot m + r, \quad y = q' \cdot m + r' \quad \text{mit} \quad 0 \leq r, r' < m.$$

Ist $x \equiv y \pmod{m}$, so ist $y - x = k \cdot m$ mit $k \in \mathbb{Z}$. Also hat man

$$y - x = k \cdot m = (q' - q) \cdot m + (r' - r).$$

Indem man eventuell x und y vertauscht, kann man $r' \geq r$, also $0 \leq r' - r < m$ annehmen. Wegen der Eindeutigkeit der Division mit Rest folgt $q' - q = k$ und $r' - r = 0$, also $r = r'$.

Ist $r = r'$, so folgt $y - x = (q' - q) \cdot m$, also $x \equiv y \pmod{m}$. ■

Dieses Lemma rechtfertigt für die Äquivalenzklassen der Kongruenz modulo m den Namen **Restklassen** von \mathbb{Z} modulo m . Wie man sofort sieht, ist die Restklasse eines $x \in \mathbb{Z}$ gegeben durch

$$x + m \cdot \mathbb{Z} := \{y \in \mathbb{Z} : \text{es gibt ein } k \in \mathbb{Z} \text{ so, dass } y = x + m \cdot k\}.$$

Die Menge aller Restklassen bezeichnet man mit $\mathbb{Z}/m \cdot \mathbb{Z}$, die kanonische Abbildung ist

$$\mathbb{Z} \rightarrow \mathbb{Z}/m \cdot \mathbb{Z}, \quad x \mapsto x + m \cdot \mathbb{Z}.$$

Die Kongruenz war auch für $m = 0$ erklärt worden, da ist sie die Gleichheit; also ist die Restklasse von jedem $x \in \mathbb{Z}$ gleich $\{x\}$ und man kann $\mathbb{Z}/0 \cdot \mathbb{Z}$ mit \mathbb{Z} identifizieren.

Für $m = 1$ sind alle $x \in \mathbb{Z}$ zueinander kongruent, also gibt es nur eine Restklasse, nämlich ganz \mathbb{Z} , das ist die Äquivalenzklasse von 0. Also kann man $\mathbb{Z}/1 \cdot \mathbb{Z} = \{0\}$ schreiben.

Für $m = 2$ gibt es die beiden Restklassen

$$\begin{aligned} 0 + 2 \cdot \mathbb{Z} &= \{x \in \mathbb{Z} : x \text{ ist gerade}\} && \text{und} \\ 1 + 2 \cdot \mathbb{Z} &= \{x \in \mathbb{Z} : x \text{ ist ungerade}\}. \end{aligned}$$

Für allgemeines $m \geq 1$ gibt es m verschiedene Restklassen

$$0 + m \cdot \mathbb{Z}, \quad 1 + m \cdot \mathbb{Z}, \dots, (m-1) + m \cdot \mathbb{Z}.$$

Die kleinsten Reste $0, 1, \dots, m-1$ nennt man **Repräsentanten** der Restklassen.

Stellt man sich die ganzen Zahlen als kleine Knoten im unendlichen Faden der reellen Zahlen vor und wickelt man den (unendlich dünnen) Faden auf eine Rolle vom Umfang m auf, so treffen kongruente Zahlen aufeinander. Für $m = 12$ wird das durch die Uhr mit dem Faden der Zeit und den Knoten der vollen Stunden realisiert.

Eine Analogie der Restklassen zu den Geraden im \mathbb{R}^n ist evident. Ist $\mathbf{o} \neq \mathbf{w} \in \mathbb{R}^n$ fest gewählt, so ist durch

$$v \sim v' \quad :\Leftrightarrow \quad v' - v \in \mathbb{R} \cdot \mathbf{w}$$

eine Äquivalenzrelation im \mathbb{R}^n erklärt. Die Äquivalenzklassen sind die parallelen Geraden $v + \mathbb{R} \cdot \mathbf{w} \subset \mathbb{R}^n$. Die Einzelheiten hierzu sind dem Leser zur Übung empfohlen.

1.2 Halbgruppen und Gruppen

Wie wir gesehen haben, kann man mit Zahlen und Vektoren in mannigfaltiger Weise rechnen. Daraus soll nun ein axiomatisch gerüstetes Gebäude werden. Wir beginnen mit dem Fundament.

1.2.1 Die natürlichen Zahlen*

Nach L. KRONECKER sind die natürlichen Zahlen von Gott gegeben. Sie gehören sicher zu den Dingen, die in der Mathematik nicht erfunden, sondern entdeckt wurden.

Aber wenn man dennoch beginnt darüber nachzudenken, was denn eine Zahl, etwa die 2, „an sich“ ist, so wird man schwer zu einem befriedigenden Ergebnis kommen. Vielmehr kann man einsehen, dass diese Frage gar nicht so relevant ist. Entscheidend ist, was man mit den Zahlen anfangen kann: Zählen und Rechnen, und welche Regeln dafür gelten. Das ist die Idee der von DEDEKIND [DED₂] vorgeschlagenen und von PEANO [PE₂] in Axiome gefassten Beschreibung der natürlichen Zahlen, die aus der Sicht von KRONECKER als Blasphemie erscheinen mag. Im Gegensatz zu DEDEKIND und PEANO beginnen wir nicht mit 1, sondern mit 0.

PEANO-Axiome der natürlichen Zahlen Die natürlichen Zahlen sind eine Menge \mathbb{N} zusammen mit einem ausgezeichneten Element $0 \in \mathbb{N}$ und einer **Nachfolgeabbildung**

$$S : \mathbb{N} \rightarrow \mathbb{N}, \quad n \mapsto S(n) =: n',$$

derart, dass Folgendes gilt:

- P1** S ist injektiv, d.h. aus $m' = n'$ folgt $m = n$.
P2 $0 \notin S(\mathbb{N})$, d.h. 0 hat keinen Vorgänger.
P3 Sei $M \subset \mathbb{N}$ eine Teilmenge mit folgenden Eigenschaften:
 a) $0 \in M$. b) Ist $n \in M$, so ist auch $n' \in M$.
 Dann folgt $M = \mathbb{N}$.

Die Axiome **P1** und **P2** formalisieren das Prinzip des Zählens, $S(n) = n'$ ist in der üblichen Schreibweise gleich $n + 1$. Axiom **P3** ist das Axiom der **vollständigen Induktion** (wofür man meist nur „Induktion“ sagt).

Aus Axiom **P3** ergibt sich das wichtige Prinzip eines *Beweises durch vollständige Induktion*. Ist eine von $n \in \mathbb{N}$ abhängige Aussage $A(n)$ zu beweisen, so kann man wie folgt vorgehen:

Induktions-Beginn Man zeigt $A(0)$, was oft sehr einfach ist.

Induktions-Schluss Man zeigt, dass $A(n + 1)$ unter der **Induktions-Annahme** $A(n)$ folgt.

Wichtig zum Verständnis des Induktions-Schlusses ist, dass die Gültigkeit von $A(n)$ nur angenommen wird, nicht dass sie schon bewiesen wäre!

Es gibt Varianten dieses Prinzips, nämlich, dass $A(n)$ erst ab einem $n \geq n_0$ gilt (etwa $n^2 > n$ für $n \geq n_0 = 2$). Dann ist $A(n_0)$ der Induktionsbeginn. Es kann auch sein, dass man zum Beweis von $A(n+1)$ die Induktionsannahme für alle $m \leq n$ benötigt.

Gründet man die natürlichen Zahlen allein auf den PEANO-Axiomen, so hat man einen mühsamen Weg vor sich. Es ist nachzuweisen, dass die Axiome keinen Widerspruch enthalten, dass die natürlichen Zahlen dadurch eindeutig bestimmt sind und schließlich, dass man alle benötigten Eigenschaften der natürlichen Zahlen daraus ableiten kann. Wir begnügen uns hier mit einigen wesentlichen Schritten, viele Details findet man z.B. in [EB, Kap. 1], [KR] und [R-S].

Um möglichst schnell wieder zur üblichen Schreibweise der natürlichen Zahlen zurückzukommen, erklären wir

$$1 := 0', \quad 2 = 1' = (0')', \quad 3 = 2', \dots$$

Man beachte dabei, dass damit die Dezimaldarstellung ab $10 = 9'$ noch nicht gerechtfertigt ist.

Zur Erklärung der üblichen algebraischen Operationen mit natürlichen Zahlen ist es hilfreich, das Axiom der vollständigen Induktion zu verwenden, um eine *rekursive Definition* zu rechtfertigen. Dazu betrachten wir die Aufgabe, für ein festes $m \in \mathbb{N}$ und ein beliebiges $n \in \mathbb{N}$ die Summe $m+n$ zu erklären. Wir beginnen mit $n=0$ und erklären, wie man von n auf n' kommt:

$$m+0 := m, \quad m+n' := (m+n)'$$

Nach **P3** ist dann $m+n$ für alle n erklärt. Insbesondere ist

$$m+1 = m+0' = (m+0)' = m'$$

Die Multiplikation natürlicher Zahlen kann man auf die Addition zurückführen, auch das geht rekursiv:

$$m \cdot 0 := 0, \quad m \cdot n' := (m \cdot n) + m.$$

Suggestiver geht es mit drei Pünktchen:

$$m \cdot n := \underbrace{n + \dots + n}_{m\text{-mal}} \quad \text{also} \quad n \cdot m = \underbrace{m + \dots + m}_{n\text{-mal}}$$

Man beachte dabei, dass bei den Definitionen von Addition und Multiplikation die linke und m bezeichnete Seite immer fest aber beliebig angenommen wird, die rechte mit n bezeichnete Seite durchläuft rekursiv ganz \mathbb{N} .

Was man benötigt, sind die folgenden

Rechenregeln für natürliche Zahlen

Für $l, m, n \in \mathbb{N}$ gilt:

A	$l + (m + n) = (l + m) + n$		<i>Assoziativität</i>
	$l \cdot (m \cdot n) = (l \cdot m) \cdot n$		
K	$m + n = n + m$		<i>Kommutativität</i>
	$m \cdot n = n \cdot m$		
N	$m + 0 = m$		<i>neutrale Elemente</i>
	$m \cdot 1 = m$		
KR	$l + n = m + n \Rightarrow l = m$		<i>Kürzungsregeln</i>
	$l \cdot n = m \cdot n \Rightarrow l = m, \text{ falls } n \neq 0$		
D	$l \cdot (m + n) = l \cdot m + l \cdot n$		<i>Distributivität</i>

All diese Regeln kann man beweisen, entscheidendes Hilfsmittel ist die vollständige Induktion. Wir führen als Beispiel einen *Beweis für die Kommutativität der Addition* aus. Das geht in mehreren Schritten. Dabei verwenden wir die Abkürzungen D für *Definition der Addition* und I für *Induktionsannahme*.

1. Für alle $n \in \mathbb{N}$ ist $0 + n = n$, insbesondere folgt $0 + n = n + 0$.

Für $n = 0$ ist $0 + 0 = 0$ nach D . Angenommen $0 + n = n$ nach I , so gilt für die Nachfolger

$$(0 + n)' = n', \text{ also } 0 + n' = n' \text{ nach } D.$$

2. Für alle $m, n \in \mathbb{N}$ gilt $m' + n = m + n'$, insbesondere folgt $m' + n = (m + n)'$.

Für $n = 0$ ist $m' + 0 = m'$ und $m + 0' = m + 1 = m'$ nach D . Angenommen $m' + n = m + n'$ nach I , so gilt für die Nachfolger

$$m' + n' = (m + n')', \text{ also } m' + n' = m + (n') = m + (n')' \text{ nach } D.$$

3. Für alle $m, n \in \mathbb{N}$ gilt $m + n = n + m$.

Der Fall $n = 0$ folgt aus 1. Angenommen $m + n = n + m$ nach I , so folgt

$$(m + n)' = (n + m)', \text{ also } m + n' = n + m' = n' + m \text{ nach } D \text{ und } 2..$$

Mit viel Geduld kann man auf ähnliche Weise auch all die anderen Rechenregeln beweisen, das hat schon DEDEKIND [DED₂] ausgeführt.

An dieser Stelle scheint ein warnender Hinweis angebracht. Die Nachweise der Rechenregeln für natürliche Zahlen mit Hilfe der Axiome werden gelegentlich als „Peano-Spielereien“ apostrophiert. Sie dienen der Einsicht, dass eine strenge Begründung ohne Verwendung geometrischer Anschauung möglich ist. Ein Lehrer sollte das wissen, aber er sei gewarnt, seine Schüler damit zu überfordern. Für die Schule ist es sicher überzeugender, die Rechenregeln durch geometrische Analogien mit Längen, Flächen und Rauminhalten zu „zeigen“. Wir begnügen uns hier mit konkreten Zahlenbeispielen:

$$3 + (4 + 2) = (3 + 4) + 2$$

$$3 + 4 = 4 + 3$$

$$4 \cdot 3 = 3 \cdot 4$$

$$(4 \cdot 3) \cdot 2 = 4 \cdot (3 \cdot 2)$$

$$3 \cdot (4 + 2) = 3 \cdot 4 + 3 \cdot 2$$

Die natürlichen Zahlen sind der Größe nach geordnet. Das kann man mit Hilfe der Addition so erklären: Für $m, n \in \mathbb{N}$ gilt

$$m \leq n \Leftrightarrow \text{es gibt ein } l \in \mathbb{N} \text{ mit } n = m + l.$$

Außerdem erklärt man

$$m < n \Leftrightarrow m \leq n \text{ und } m \neq n.$$

Eine oft benützte Eigenschaft der natürlichen Zahlen ist der

Satz vom kleinsten Element Ist $M \subset \mathbb{N}$ und $M \neq \emptyset$, so gibt es ein $n \in M$, so dass $n \leq m$ für jedes $m \in M$.

Diese Aussage ist offensichtlich für ganze oder auch positive rationale Zahlen falsch.

Beweis Man kann entweder bei 0 beginnen und so lange Nachfolger bilden, bis man zum ersten Mal in M anstößt, oder in M beginnend so lange Vorgänger betrachten, bis man M verlassen hat. Die zweite Methode ist formal einfacher.

Da $M \neq \emptyset$, können wir ein $m_0 \in M_0 := M$ wählen und die endliche Menge

$$M_1 := \{m \in M : m < m_0\} \subsetneq M$$

betrachten. Ist $M_1 = \emptyset$, so ist $n := m_0$ das kleinste Element. Andernfalls wähle man $m_1 \in M_1$ und betrachte

$$M_2 := \{m \in M : m < m_1\} \subsetneq M_1.$$

Ist $M_2 = \emptyset$, so kann man $n := m_1$ setzen. Da M_1 endlich ist und in jedem Schritt eine echt kleinere Menge auftritt, gibt es ein $k \in \mathbb{N}$ so, dass

$$\emptyset = M_{k+1} := \{m \in M : m < m_k\} \subsetneq M_k \neq \emptyset,$$

und $n := m_k$ ist das kleinste Element von M . ■

Zum Schluss dieses Abschnitts noch eine Aussage über die Mächtigkeit endlicher Mengen.

Lemma *Ist M eine endliche Menge mit $\#M = n$, so gilt für die Potenzmenge*

$$\#\mathcal{P}(M) = 2^n.$$

Beweis durch Induktion über n . Für $n = 0$ ist $M = \emptyset$ und $\mathcal{P}(M) = \{\emptyset\}$, also ist $\#\mathcal{P}(M) = 1 = 2^0$.

Angenommen $\#\mathcal{P}(M) = 2^n$ sei schon für alle M mit $\#(M) = n$ bewiesen. Ist nun

$$\overline{M} := \{m_1, \dots, m_{n+1}\}$$

mit paarweise verschiedenen m_i gegeben, so sei $M := \{m_1, \dots, m_n\}$. Wir betrachten die disjunkte Zerlegung

$$\mathcal{P}(\overline{M}) = \mathcal{P}_1 \cup \mathcal{P}_2 \quad \text{mit} \quad \mathcal{P}_1 := \{N \subset \overline{M} : m_{n+1} \notin N\} \quad \text{und} \quad \mathcal{P}_2 := \{N \subset \overline{M} : m_{n+1} \in N\}.$$

Offensichtlich ist $\mathcal{P}_1 = \mathcal{P}(M)$, also $\#\mathcal{P}(M) = 2^n$. Weiterhin hat die Abbildung

$$\mathcal{P}_1 \rightarrow \mathcal{P}_2, \quad N \mapsto N \cup \{m_{n+1}\},$$

eine Umkehrung $\mathcal{P}_2 \rightarrow \mathcal{P}_1$, $N \mapsto N \cap M$, damit ist sie nach Bemerkung aus 1.1.3 bijektiv, also folgt

$$\#\mathcal{P}_2 = \#\mathcal{P}_1 = 2^n \quad \text{und} \quad \#\mathcal{P}(\overline{M}) = 2^n + 2^n = 2^{n+1}.$$
■

1.2.2 Verknüpfungen und Halbgruppen

Addition und Multiplikation natürlicher Zahlen kann man auffassen als Abbildungen

$$+ : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}, (m, n) \mapsto m + n, \text{ und } \cdot : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}, (m, n) \mapsto m \cdot n.$$

Das sind Beispiele für *innere Verknüpfungen* in einer Menge M , die ganz allgemein durch eine Abbildung

$$* : M \times M \rightarrow M, (a, b) \mapsto a * b,$$

beschrieben werden. Solche Verknüpfungen können von völlig verschiedener Art sein. Wir geben zuerst einige Beispiele:

- a) $M = \mathbb{N}, m * n = m + n$ oder $m * n = m \cdot n$
- b) $M = \mathbb{Z}, m * n = m + n$
- c) $M = \mathbb{Q}, a * b = a + b$
- d) $M = \mathbb{Q}, a * b = a \cdot b$
- e) $M = \mathbb{Q}^*, a * b = a \cdot b$
- f) $M = \mathbb{R}^n, v * w = v + w$
- g) $M = \mathbb{N}, m * n = m^n$
- h) $M = \mathbb{Q}, a * b = \frac{1}{2}(a + b)$
- i) X beliebige Menge, $M = \text{Abb}(X, X) = \{f : X \rightarrow X\}, f * g := f \circ g$
- j) $M = \mathcal{S}(X) := \{f \in \text{Abb}(X, X) : f \text{ bijektiv}\}, f * g = f \circ g$

Für besondere Eigenschaften von Verknüpfungen gibt es Namen:

Definition Sei $* : M \times M \rightarrow M$ eine Verknüpfung auf einer beliebigen Menge M .

1. $*$ heißt **assoziativ**, wenn $(a * b) * c = a * (b * c)$ für alle $a, b, c \in M$.
2. $*$ heißt **kommutativ**, wenn $a * b = b * a$ für alle $a, b \in M$.
3. $e \in M$ heißt **neutrales Element**, wenn $e * a = a = a * e$ für alle $a \in M$.
4. Ein $a' \in M$ heißt **inverses Element** zu $a \in M$, wenn $a' * a = a * a' = e$, wobei e ein neutrales Element ist.
5. Es gilt die **Kürzungsregel**, wenn für alle $a, x, y \in M$

$$a * x = a * y \Rightarrow x = y \quad \text{und} \quad x * a = y * a \Rightarrow x = y.$$

Prüft man diese Regeln in den obigen Beispielen nach, so erhält man folgendes Ergebnis, wobei $+ = ja$ und $- = nein$ bedeutet:

Beispiel	a	b	c	d	e	f	g	h	i	j
assoziativ	+	+	+	+	+	+	-	-	+	+
kommutativ	+	+	+	+	+	+	-	+	-	-
es gibt ein neutrales Element	+	+	+	+	+	+	-	-	+	+
es gibt ein neutrales und inverse Elemente	-	+	+	-	+	+	-	-	-	+
es gilt die Kürzungsregel	+	+	+	-	+	+	-	+	-	+

Bei Beispiel a) wurden die in 1.2.1 beschriebenen Eigenschaften der natürlichen Zahlen benutzt. Beispiele b) bis f) wurden schon kurz in Kapitel 0 behandelt; mehr dazu folgt in 1.3. Die Beispiele g) und h) seien dem Leser überlassen. Man beachte dabei die üblichen Regeln für Potenzen:

$$2^{3^2} := 2^{(3^2)} = 2^9 = 512, \quad \text{aber} \quad (2^3)^2 = 8^2 = 64.$$

Im Beispiel i) ist die Assoziativität wichtig. Zwei Abbildungen sind genau dann gleich, wenn sie für alle Argumente die gleichen Werte besitzen. Nach Definition der Hintereinanderschaltung von Abbildungen gilt für alle $x \in X$

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

Daraus folgt $(f \circ g) \circ h = f \circ (g \circ h)$.

Dass die Hintereinanderschaltung nicht kommutativ ist, kann man schon mit $X = \{1, 2\}$ sehen. Ist

$$f(x) = 1 \quad \text{und} \quad g(x) = 2 \quad \text{für alle } x \in X,$$

so ist $(f \circ g)(x) = 1$ und $(g \circ f)(x) = 2$ für alle $x \in X$.

Setzt man auch $h(x) = 1$ für alle $x \in X$, so ist

$$h \circ f = h \circ g, \quad \text{aber} \quad f \neq g.$$

Also gilt keine Kürzungsregel. Die identische Abbildung id_X ist ein neutrales Element.

Im Beispiel j) bleibt die Assoziativität und das neutrale Element aus Beispiel c) erhalten. Die Kommutativität ist verletzt, wenn X mindestens drei Elemente enthält. Man findet leicht Beispiele in $X = \{1, 2, 3\}$.

Die Kürzungsregeln sind klar, wir zeigen die erste. Seien $f, g, h \in M'$ gegeben, und angenommen es wäre $f \neq g$. Dann gibt es mindestens ein $x \in X$ mit $f(x) \neq g(x)$. Da h insbesondere injektiv ist, folgt

$$(h \circ f)(x) = h(f(x)) \neq h(g(x)) = (h \circ g)(x).$$

Also ist $h \circ f \neq h \circ g$. ■

Für Verknüpfungen mit guten Eigenschaften gibt es einige Namen. Wir beginnen mit folgender

Definition Eine Menge M zusammen mit einer assoziativen Verknüpfung $*$: $M \times M \rightarrow M$ heißt **Halbgruppe**.

In dieser Terminologie haben wir in den obigen Beispielen a) bis f), sowie i) und j) Halbgruppen gefunden.

Es sei noch vermerkt, dass man als Folgerung aus dem Assoziativgesetz auch bei einem Produkt von mehr als drei Faktoren alle möglichen Klammern weglassen und einfach $a_1 \cdot \dots \cdot a_n$ schreiben kann.

1.2.3 Gruppen

Wie wir gesehen haben, ist die Menge \mathbb{N} der natürlichen Zahlen zusammen mit der Addition ein Beispiel für eine Halbgruppe; naheliegend ist die Frage nach der „anderen Hälfte“. Es wird sich zeigen, dass dies die negativen Zahlen sind. Zunächst eine grundlegende allgemeine

Definition Eine Menge G zusammen mit einer Verknüpfung $* : G \times G \rightarrow G$ heißt **Gruppe**, wenn Folgendes gilt:

G1 Die Verknüpfung $*$ ist assoziativ, d.h. G zusammen mit $*$ ist eine Halbgruppe.

G2 Es gibt ein eindeutig bestimmtes $e \in G$, so dass

a) $a * e = e * a = a$ für alle $a \in G$ (e heißt **neutrales Element**).

b) Zu jedem $a \in G$ gibt es ein eindeutig bestimmtes $a' \in G$, so dass

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

(a' heißt zu a **inverses Element**).

G mit $*$ heißt **kommutativ** (oder **abelsch**), wenn $a * b = b * a$ für alle $a, b \in G$.

Genau genommen ist eine Gruppe ein Paar $(G, *)$. Ist klar, welche Verknüpfung $*$ gemeint ist, kann man auch von der Gruppe G sprechen.

Noch ein Hinweis auf übliche Bezeichnungen. Besonders wichtige Verknüpfungen sind Addition und Multiplikation, dann schreibt man $* = +$ und $* = \cdot$.

Im Fall der Addition setzt man immer voraus, dass sie kommutativ ist. Das neutrale Element wird mit $0 = \text{Null}$, das Inverse a' von a wird mit $-a$ als **Negatives** bezeichnet. Zusammengefasst gilt

$$a + b = b + a, \quad a + 0 = a, \quad a + (-a) = 0.$$

Statt $*$ schreibt man für eine beliebige Verknüpfung in einer Gruppe meist den Malpunkt \cdot , und statt $a \cdot b$ kann man ab schreiben. Das Inverse a' wird in der multiplikativen Schreibweise mit a^{-1} bezeichnet.

Beispiel 1 Von der Serie a) bis j) von Beispielen aus 1.2.2 erfüllen die folgenden die Gruppenaxiome:

$$(\mathbb{Z}, +), \quad (\mathbb{Q}, +), \quad (\mathbb{Q}^*, \cdot), \quad (\mathbb{R}^n, +), \quad (\mathcal{S}(X), \circ).$$

Diese Gruppen sind abelsch, mit Ausnahme von $\mathcal{S}(X)$ für $\#X \geq 3$. Man nennt $\mathcal{S}(X)$ die *symmetrische Gruppe von X* .

Für die Menge $X = \{1, \dots, n\}$ nennt man $\mathcal{S}_n := \mathcal{S}(X)$ auch *Permutationsgruppe*. Diese Gruppen werden in Kapitel 3 beim Studium von Determinanten eine wichtige Rolle spielen.

Die Anzahl der Elemente einer Menge hatten wir als Mächtigkeit bezeichnet, bei Gruppen spricht man üblicherweise von der *Ordnung*, in Zeichen

$$\text{ord}(G).$$

Über die symmetrische Gruppe halten wir schon einmal Folgendes fest:

Bemerkung Für $n \in \mathbb{N}^*$ ist $\text{ord}(\mathcal{S}_n) = n!$.

Dabei nennt man $n! := n \cdot (n-1) \cdot \dots \cdot 2 \cdot 1$ für $n \in \mathbb{N}^*$ die *Fakultät* von n . Statt der Definition mit drei Punkten kann man korrekter auch eine rekursive Definition geben:

$$1! := 1 \quad \text{und} \quad (n+1)! = (n+1) \cdot n! .$$

Beweis der Bemerkung. Eine bijektive Abbildung f von $\{1, \dots, n\}$ auf sich ist bestimmt durch die Bilder $f(1), \dots, f(n)$. Man muss also abzählen, in wie vielen verschiedenen Reihenfolgen man die Zahlen von 1 bis n aufschreiben kann.

Für den ersten Platz hat man n Möglichkeiten; beim zweiten Platz ist schon eine Zahl vergeben, es bleiben nur noch $n-1$ Möglichkeiten. Das macht man so weiter bis zum letzten Platz, da ist nur noch eine Zahl übrig. Also hat man insgesamt

$$n \cdot (n-1) \cdot \dots \cdot 2 \cdot 1 = n!$$

Möglichkeiten.

Formal etwas korrekter kann man die Aussage auch durch Induktion beweisen. Offensichtlich ist $\text{ord} \mathcal{S}_1 = 1$. Sei $\text{ord} \mathcal{S}_n = n!$ schon bewiesen. Für $f(n+1)$ gibt es $n+1$ mögliche Werte; dann verbleiben für $f(1), \dots, f(n)$ noch n mögliche Werte, das sind nach Induktionsannahme $n!$ Möglichkeiten. Also hat man insgesamt

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

Möglichkeiten. ■

Für spätere Verwendung notieren wir noch elementare

Rechenregeln für Gruppen *Ist (G, \cdot) eine Gruppe, so gilt für alle $a, b, x, y \in G$:*

- 1) $(a^{-1})^{-1} = a, \quad (a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$
- 2) $a \cdot x = a \cdot y \Rightarrow x = y$ und $x \cdot a = y \cdot a \Rightarrow x = y.$
- 3) Die Gleichungen $a \cdot x = b$ und $y \cdot a = b$ sind eindeutig lösbar durch

$$x = a^{-1} \cdot b \quad \text{und} \quad y = b \cdot a^{-1}.$$

Beweis Ad 1). Die Beziehung $a \cdot a^{-1} = e = a^{-1} \cdot a$ bedeutet zunächst, dass a^{-1} invers ist zu a ; anders herum gelesen besagt sie, dass a invers ist zu a^{-1} . Weiter gilt

$$\begin{aligned} (a \cdot b) \cdot (b^{-1} \cdot a^{-1}) &= a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot a^{-1} = e \quad \text{und} \\ (b^{-1} \cdot a^{-1}) \cdot (a \cdot b) &= b^{-1} \cdot (a^{-1} \cdot a) \cdot b = b^{-1} \cdot b = e. \end{aligned}$$

Ad 2). Zum Beweis der Kürzungsregeln genügt es, mit a^{-1} zu multiplizieren:

$$a \cdot x = a \cdot y \Rightarrow a^{-1} \cdot (a \cdot x) = a^{-1} \cdot (a \cdot y) \Rightarrow (a^{-1} \cdot a) \cdot x = (a^{-1} \cdot a) \cdot y \Rightarrow x = y.$$

Die zweite Regel folgt analog.

Ad 3). Die angegebenen Werte von x und y sind offensichtlich Lösungen der gegebenen linearen Gleichungen; die Eindeutigkeit folgt aus 2). ■

Ist in einer Menge M eine Verknüpfung $*$ gegeben, so hat man für jedes $a \in M$ Abbildungen

$$\begin{aligned} l_a : M &\rightarrow M, & x &\mapsto a * x, & \text{(Linkstranslation)} & \text{ und} \\ r_a : M &\rightarrow M, & x &\mapsto x * a, & \text{(Rechtstranslation)}. \end{aligned}$$

Als Folgerung aus den obigen Rechenregeln erhält man als

Korollar *Ist G eine Gruppe und $a \in G$ beliebig, so sind die Translationen l_a und r_a bijektive Abbildungen.*

Diese Eigenschaft kann man ausnützen bei dem Versuch, eine endliche Menge mit der Struktur einer Gruppe zu versehen. Ist $G = \{a_1, \dots, a_n\}$, so gibt man eine **Verknüpfungstafel** an, die so aussieht:

*	a_1	...	a_j	...	a_n
a_1					
\vdots					
a_i			$a_i * a_j$		
\vdots					
a_n					

In der Zeile i und der Spalte j steht $a_i * a_j$. Den Axiomen entsprechend ist so eine Tafel zahlreichen Einschränkungen unterworfen. Da es ein neutrales Element geben muss, kann man $a_1 = e$ annehmen, dadurch ist die erste Zeile und die erste Spalte festgelegt. Dem obigen Korollar entsprechend muss in jeder Zeile und in jeder Spalte jedes Element genau einmal vorkommen. Für $n = 2$ gibt es eine einzige Möglichkeit

*	e	a
e	e	a
a	a	e

Die Tafel ist symmetrisch, also ist $*$ kommutativ. Da es nur ein von e verschiedenes Element a gibt, genügt es für das Assoziativgesetz die eine Gleichung

$$a * (a * a) = (a * a) * a$$

zu prüfen. Als Ergebnis erhält man, dass $G = \{e, a\}$ zusammen mit $*$ eine Gruppe ist.

Für $G = \{e, a, b\}$ gibt es wegen der Kürzungsregel wieder nur eine mögliche Gruppentafel:

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Das einzige Problem ist die Assoziativität. Da jede Bedingung der Form

$$a_1 * (a_2 * a_3) = (a_1 * a_2) * a_3$$

drei Faktoren enthält, kann man das nicht aus der Gruppentafel erkennen. Zunächst gibt es $3^3 = 27$ verschiedene Tripel (a_1, a_2, a_3) aus $a_i \in G$. Da die Assoziativität klar ist, wenn mindestens einer der drei Faktoren a_i gleich e ist, bleiben nur noch $2^3 = 8$ Gleichungen zu prüfen. Nehmen wir eine davon:

$$a * (b * a) = a * e = a, \quad (a * b) * a = e * a = a.$$

Die anderen Gleichungen sieht man analog. Aber klar ist, dass diese Methode sehr mühsam ist. Hat G insgesamt n Elemente, so muss man $(n - 1)^3$ Gleichungen prüfen!

1.2.4 Die ganzen Zahlen als additive Gruppe*

Wie wir gesehen haben, bilden die natürlichen Zahlen sowohl mit der Addition als auch mit der Multiplikation eine Halbgruppe. Wir betrachten zuerst die Addition und ergänzen sie bezüglich dieser Operation zu einer Gruppe.

Von einem weniger abstrakten Standpunkt betrachten wir für $m, n \in \mathbb{N}$ die Gleichung

$$m + x = n.$$

Sie hat offenbar genau dann eine Lösung $x \in \mathbb{N}$, wenn $n \geq m$ ist, d.h. wenn n im Sinn der PEANO-Axiome zu den Nachfolgern von m gehört. In diesem Fall hat die Bezeichnung

$$x = n - m \in \mathbb{N}$$

einen Sinn als natürliche Zahl. Die Zahl $n - m$ ist dadurch charakterisiert, dass

$$m + (n - m) = n.$$

Für den Übergang zu negativen Zahlen gibt es viele Gründe, einer stammt aus dem täglichen Leben. Man hat n € und will für m € einkaufen. Ist $m \leq n$, so verbleibt als Rest ein Guthaben von $(n - m)$ €. Im Fall $m > n$ entstehen Schulden, die man als abstrakten negativen Rest bezeichnen kann. In jedem Fall kann der verbliebene Rest auch in einer anderen Kombination n' und m' der Gleiche sein, nämlich dann, wenn

$$n - m = n' - m'. \quad (*)$$

Aber Bedingung $(*)$ ist für beliebige m, n und $m', n' \in \mathbb{N}$ noch nicht zulässig, da negative Zahlen erst erklärt werden sollen. Der Trick ist nun, Bedingung $(*)$ so zu schreiben, dass sie in \mathbb{N} kontrolliert werden kann:

$$n + m' = m + n'. \quad (*')$$

Damit ist der Weg frei für eine formale Konstruktion. Statt der noch nicht erlaubten Differenzen $n - m$ betrachten wir geordnete Paare, also

$$\mathbb{N} \times \mathbb{N} := \{(n, m) : n, m \in \mathbb{N}\}$$

und in $\mathbb{N} \times \mathbb{N}$ definieren wir entsprechend der obigen Vorbereitung eine Äquivalenz

$$(n, m) \sim (n', m') \quad :\Leftrightarrow \quad n + m' = m + n'.$$

Ziel ist es, die ganzen Zahlen als Äquivalenzklassen solcher Paare zu erklären. Das ist ganz elementar, aber leider etwas langwierig.

Zunächst ist zu zeigen, dass durch \sim tatsächlich eine Äquivalenzrelation gegeben ist.

$$(n, m) \sim (n, m), \text{ denn } n + m = m + n$$

$$(n, m) \sim (n', m') \Rightarrow n + m' = m + n' \Rightarrow n' + m = m' + n \Rightarrow (n', m') \sim (n, m).$$

$$(n, m) \sim (n', m') \sim (n'', m'') \Rightarrow n + m' = m + n' \text{ und } n' + m' = m' + n''.$$

Zählt man diese beiden Gleichungen zusammen, so erhält man

$$(n + m'') + (m' + n') = (m + n'') + (n' + m'),$$

also $n + m'' = m + n''$, d.h. $(n, m) \sim (n'', m'')$.

Man beachte, dass wir die Assoziativität und Kommutativität der Addition sowie die Kürzungsregel benutzt haben.

Nun bezeichnen wir die Äquivalenzklasse von (n, m) mit $n - m$. Das ist zunächst nur eine Bezeichnung, eine „formale Differenz“. Nach den Regeln für Äquivalenzklassen gilt

$$n - m = n' - m' \Leftrightarrow (n, m) \sim (n', m') \Leftrightarrow n + m' = m + n'.$$

Damit kann die Gleichheit formaler Differenzen durch eine Rechnung in den natürlichen Zahlen überprüft werden.

Als Ergebnis der ersten Etappe notieren wir folgende

Definition Die Menge \mathbb{Z} der **ganzen Zahlen** ist erklärt als Menge der Äquivalenzklassen von $\mathbb{N} \times \mathbb{N}$ nach der Äquivalenzrelation

$$(n, m) \sim (n', m') \Leftrightarrow n + m' = m + n'.$$

Die Äquivalenzklasse von (n, m) wird mit $n - m$ bezeichnet.

Die ganzen Zahlen sollen die natürlichen Zahlen erweitern. Daher soll zunächst geklärt werden, wie man \mathbb{N} als Teilmenge von \mathbb{Z} wiederfinden kann.

Lemma Die Abbildung

$$\varphi: \mathbb{N} \rightarrow \mathbb{Z}, \quad n \mapsto n - 0,$$

ist injektiv.

Beweis Man beachte zunächst, dass die formale Differenz $n - 0$ die Äquivalenzklasse von $(n, 0)$ bedeutet. die naheliegende Rechnung $n - 0 = n$ ist noch nicht erlaubt, da noch nicht erklärt ist, wie man mit den Restklassen rechnen darf. Schön nach den gegebenen Regeln geht es so:

Sei $\varphi(n) = \varphi(n')$ für $n, n' \in \mathbb{N}$. Nun bedeutet

$$n - 0 = n' - 0, \text{ dass } (n, 0) \sim (n', 0), \text{ d.h. } n + 0 = 0 + n'.$$

Die letzte Gleichung gilt in \mathbb{N} , also folgt $n = n'$. ■

Nun folgt ein Schritt, der bei der Erweiterung von Zahlbereichen zur Vereinfachung immer wieder auftritt. Man „identifiziert“ \mathbb{N} mit seinem Bild $\varphi(\mathbb{N}) \subset \mathbb{Z}$ unter der injektiven Abbildung φ , d.h. man setzt

$$n = n - 0.$$

Links steht $n \in \mathbb{N}$, rechts die Äquivalenzklasse von $(n, 0)$, sie ist gleich der Äquivalenzklasse $(n + k, k)$ für jedes $k \in \mathbb{N}$.

Die neu hinzugekommenen nicht natürlichen Zahlen sind die ganzen negativen Zahlen; das sind die formalen Differenzen $n - m$ mit $m > n$. Auch hier können wir die Bezeichnungen vereinfachen und

$$-m := 0 - m$$

setzen. Das ist die Äquivalenzklasse von $(0, m)$, es ist $(0, m) = (k, m + k)$ für alle $k \in \mathbb{N}$. Damit sind wir endlich bei der üblichen Darstellung

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

angekommen und haben sie durch einen präzisen Formalismus untermauert.

Jetzt beginnt der zweite Teil der Arbeit, nämlich Addition und Multiplikation von \mathbb{N} nach \mathbb{Z} auszudehnen. Wir beginnen mit der Addition und machen den naheliegenden Versuch einer Definition für die Summe formaler Differenzen:

$$(n - m) + (l - k) := (n + l) - (m + k). \quad (+)$$

Hinter dieser „Definition“ ist ein Problem versteckt. Die Paare (m, n) und (k, l) sind Repräsentanten der Äquivalenzklassen und es muss nachgewiesen werden, dass das Ergebnis auf der rechten Seite von (+) von der Auswahl der Repräsentanten unabhängig ist. Ist das der Fall, so sagt man, die Addition ist durch (+) *wohldefiniert*.

Sei also $(m, n) \sim (m', n')$ und $(k, l) \sim (k', l')$ Aus

$$m + n' = n + m' \text{ und } k + l' = l + k' \text{ folgt } n + l + m' + k' = m + k + n' + l',$$

also ist $(n + l, m + k) \sim (n' + l', m' + k')$.

Beschränkt auf \mathbb{N} ist diese neue Addition gleich der alten, denn für $n, l \in \mathbb{N}$ gilt

$$(n - 0) + (l - 0) = (n + l) - (0 + 0) = (n + l) - 0 = n + l.$$

Wie man sich leicht mit Hilfe der entsprechenden Regeln für die natürlichen Zahlen aus 1.2.1 überzeugt, ist die so definierte Addition in \mathbb{Z} assoziativ und kommutativ. Neutrales Element ist die Null in den verschiedenen Darstellungen

$$0 = 0 - 0 = n - n \in \mathbb{N},$$

und das eindeutig bestimmte negative Element zu $n - m \in \mathbb{Z}$ ist $m - n \in \mathbb{Z}$, denn

$$(n - m) + (m - n) = (n + m) - (m + n) = 0 - 0 = 0.$$

Insgesamt haben wir gezeigt:

Satz Die Menge \mathbb{Z} der ganzen Zahlen mit der aus der Halbgruppe $\mathbb{N} \subset \mathbb{Z}$ fortgesetzten Addition ist eine abelsche Gruppe. ■

Da die Addition $+$ in \mathbb{Z} eine Fortsetzung der Addition $+$ in \mathbb{N} ist und da wir \mathbb{N} als Teilmenge von \mathbb{Z} ansehen, ist die Unterscheidung von $+$ und $+$ überflüssig geworden; man bezeichnet auch die Addition in \mathbb{Z} mit $+$.

Statt $n + (-m)$ schreibt man $n - m$.

Zum Schluss dieses Abschnitts ein **Fazit**: Die Definition ganzer Zahlen und der Nachweis der gewohnten Rechenregeln hat gezeigt, dass sie streng formal und ohne Mystik aus den natürlichen Zahlen gewonnen werden können. Ein Lehrer sollte das wissen, aber seine Schüler mehr intuitiv (etwa über den Begriff von Schulden) an die negativen Zahlen heranführen.

1.2.5 Untergruppen und Homomorphismen

Bei vielen algebraischen Strukturen treten immer wieder folgende Probleme auf:

- 1) Wann vererbt sich eine Struktur auf eine Teilmenge?
- 2) Wann sind zwei verschiedene Strukturen verträglich?

Das ist besonders einfach im Fall von Gruppen zu beschreiben. Zu Problem 1) geben wir folgende

Definition Sei $(G, *)$ eine Gruppe und $G' \subset G$ eine nichtleere Teilmenge. G' heißt **Untergruppe** von G , wenn Folgendes gilt:

- 1) $a, b \in G' \Rightarrow a * b \in G'$.
- 2) $a \in G' \Rightarrow a^{-1} \in G'$.

Die beiden Bedingungen kann man zusammenfassen zu $a, b \in G' \Rightarrow a * b^{-1} \in G'$.

In diesem Fall vererbt sich die Gruppenstruktur von G zu einer Gruppenstruktur auf G' . Nach Bedingung 1) hat man eine Verknüpfung

$$* : G' \times G' \rightarrow G', \quad (a, b) \mapsto a * b.$$

Diese ist assoziativ, da sie aus G stammt. Da $G \neq \emptyset$ gibt es ein $a \in G'$. Nach 2) ist $a^{-1} \in G'$, nach 1) ist auch $a * a^{-1} = e \in G'$. Wieder folgt mit Hilfe von 2), dass es in G' auch inverse Elemente gibt. Damit haben wir Folgendes gezeigt:

Bemerkung Eine Untergruppe wird in kanonischer Weise selbst zu einer Gruppe.

Beispiel 1 Für jedes $m \in \mathbb{N}$ ist

$$m \cdot \mathbb{Z} = \{m \cdot x : x \in \mathbb{Z}\} \subset \mathbb{Z}$$

Untergruppe, wobei $*$ = $+$ in \mathbb{Z} . Analog ist auch $\mathbb{Z} \subset \mathbb{Q}$ eine additive Untergruppe.

Für $n \geq 2$ ist $S' := \{\sigma \in S_n : \sigma(n) = n\} \subset S_n$ eine Untergruppe mit $\text{ord } S' = (n-1)!$.

Weitere Beispiele werden uns später begegnen.

Bemerkenswert ist, dass es in der Gruppe \mathbb{Z} keine anderen als die in Beispiel 1 angegebenen Untergruppen gibt:

Lemma *Ist $G \subset \mathbb{Z}$ eine Untergruppe, so gibt es ein eindeutig bestimmtes $m \in \mathbb{N}$ derart, dass $G = m\mathbb{Z}$.*

Beweis Ist $G = \{0\}$, so $m = 0$. Da G Untergruppe ist, ist für jedes $n \in G$ auch $-n \in G$. Im Fall $G \neq \{0\}$ gibt es daher nach dem Satz vom kleinsten Element aus 1.2.1 ein kleinstes positives $m \in G$. Offensichtlich ist dann $m\mathbb{Z} \subset G$. Dass auch $G \subset m\mathbb{Z}$ gilt, zeigen wir mit der anschließend in 1.3.1 bewiesenen Division mit Rest. Ist $n \in G$, so gibt es eine eindeutige Darstellung

$$n = q \cdot m + r \quad \text{mit } q, r \in \mathbb{Z} \quad \text{und } 0 \leq r < m.$$

Dann ist auch $r = n - q \cdot m \in G$, und da m minimal gewählt war, muss $r = 0$ sein; also folgt $n = q \cdot m \in m\mathbb{Z}$. ■

Nun zur Verträglichkeit einer Abbildung mit Strukturen.

Definition *Sind $(G, *)$ und $(H, *')$ Gruppen, so heißt eine Abbildung $\varphi : G \rightarrow H$ **Homomorphismus** von Gruppen, wenn*

$$\varphi(a * b) = \varphi(a) *' \varphi(b) \quad \text{für alle } a, b \in G.$$

*Ein Homomorphismus heißt **Isomorphismus**, wenn er bijektiv ist.*

Beispiel 2 Die für jedes $m \in \mathbb{N}$ erklärte Abbildung

$$\varphi_m : \mathbb{Z} \rightarrow \mathbb{Z}, \quad x \mapsto m \cdot x,$$

ist ein Homomorphismus, $\varphi_m(\mathbb{Z}) = m\mathbb{Z}$.

Zwischen den Gruppen $(\mathbb{R}, +)$ und (\mathbb{R}_+^*, \cdot) ist die Abbildung

$$\varphi : \mathbb{R} \rightarrow \mathbb{R}_+^*, \quad x \mapsto e^x,$$

ein Isomorphismus, denn $e^{x+y} = e^x \cdot e^y$.

1.3 Ringe und Körper

1.3.1 Die ganzen Zahlen als Ring*

Für die natürlichen Zahlen ist neben der Addition auch eine Multiplikation erklärt, die auf die Addition zurückgeführt ist. Sie kann ebenso wie die Addition auf die ganzen Zahlen ausgedehnt werden.

Eine ganze Zahl war in 1.2.4 erklärt worden als die Äquivalenzklasse eines Paares $(n, m) \in \mathbb{N} \times \mathbb{N}$, die mit $n - m$ als formale Differenz bezeichnet wurde. Um eine Idee zu bekommen, wie man solche Äquivalenzklassen in sinnvoller Weise multiplizieren sollte, machen wir die informelle naive Rechnung

$$(n - m) \cdot (l - k) = (n \cdot l + m \cdot k) - (m \cdot l + n \cdot k).$$

Will man daraus die formale Definition

$$(n - m) \bullet (l - k) := (n \cdot l + m \cdot k) - (m \cdot l + n \cdot k) \quad (\bullet)$$

machen, so ist zu zeigen, dass diese Multiplikation wohldefiniert ist, d.h. dass das Ergebnis nicht von der Auswahl der Repräsentanten abhängt. Sei also

$$\begin{aligned} (n, m) \sim (n', m'), \quad \text{d.h.} \quad n + m' = m + n' \quad \text{und} \\ (l, k) \sim (l', k'), \quad \text{d.h.} \quad l + k' = k + l'. \end{aligned} \quad (\sim)$$

Zu zeigen ist, dass daraus

$$nl + mk + m'l' + n'k' = ml + nk + n'l' + m'k' \quad (*)$$

folgt. Die dazu nötige Rechnung kann man vereinfachen durch einen kleinen Kniff: Man addiert zur einen Seite von $(*)$ die Zahl

$$r := (l + k) \cdot (n' + m') = ln' + lm' + kn' + km' \in \mathbb{N}.$$

Indem man die Gleichungen aus (\sim) benutzt, erhält man durch die Rechnung in \mathbb{N}

$$\begin{aligned} nl + mk + m'l' + n'k' + r &= l(n + m') + k(m + n') + n'(l + k') + m'(k + l') \\ &= l(m + n') + k(n + m') + n'(k + l') + m'(l + k') \\ &= ml + nk + n'l' + m'k' + r. \end{aligned}$$

Da man r in \mathbb{N} kürzen kann, folgt $(*)$.

Beschränkt auf \mathbb{N} ist diese neue Multiplikation in \mathbb{Z} gleich der alten, denn für $n, l \in \mathbb{N}$ gilt

$$(n - 0) \bullet (l - 0) = (n \cdot l + 0) - (0 + 0) = n \cdot l - 0 = n \cdot l.$$

Also kann man die Unterscheidung von \bullet und \cdot aufgeben.

Die in \mathbb{Z} üblichen **Vorzeichenregeln** kann man nun beweisen. Für $m, n \in \mathbb{N}$ gilt

$$m \cdot (-n) = (-m) \cdot n = -(m \cdot n) \quad \text{und} \quad (-m) \cdot (-n) = m \cdot n.$$

Wir zeigen die letzte dieser Regeln:

$$(-m) \cdot (-n) = (0 - m) \cdot (0 - n) = (0 \cdot 0 + m \cdot n) - (m \cdot 0 + 0 \cdot n) = m \cdot n.$$

Damit ist die Regel „minus \cdot minus = plus“ formal nachgewiesen. Die anderen Regeln beweist man analog.

Weiter kann man unter Benutzung der entsprechenden Regeln für \mathbb{N} aus 1.2.1 zeigen, dass die Multiplikation in \mathbb{Z} assoziativ und kommutativ ist, und dass ein Distributivgesetz gilt. Um all die so erhaltenen Eigenschaften von \mathbb{Z} zusammenzufassen, führen wir einen neuen Namen ein.

Definition Eine Menge R zusammen mit zwei Verknüpfungen

$$+ : R \times R \rightarrow R \quad \text{und} \quad \cdot : R \times R \rightarrow R$$

heißt **Ring**, wenn Folgendes gilt:

R1 R zusammen mit der Addition $+$ ist eine abelsche Gruppe.

R2 R zusammen mit der Multiplikation \cdot ist eine Halbgruppe.

R3 Es gelten die Distributivgesetze, d.h. für $a, b, c \in R$ ist

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{und} \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Ein Ring R heißt **kommutativ**, wenn die Multiplikation kommutativ ist, d.h. für $a, b \in R$ gilt $a \cdot b = b \cdot a$.

Ein Element $1 \in R$ heißt **Einselement**, wenn für alle $a \in R$ gilt, dass $1 \cdot a = a \cdot 1 = a$.

Die Ergebnisse der vorangegangenen Abschnitte können wir nun so zusammenfassen:

Satz Die Menge \mathbb{Z} der ganzen Zahlen zusammen mit Addition und Multiplikation ist ein kommutativer Ring mit Einselement. ■

Für die Praxis bedeutet das nur, dass man mit ganzen Zahlen so rechnen kann wie gewohnt; jetzt aber mit gutem Gewissen!

In einem Ring sind die Anforderungen an die Multiplikation weit schwächer als an die Addition. Zu jedem $a \in R$ gibt es ein Negatives $-a$, aber bezüglich der Multiplikation muss es kein Inverses a^{-1} geben. Das ist ganz klar, denn will man zwei ganze Zahlen dividieren, so ist das Ergebnis im Allgemeinen nicht mehr ganzzahlig. Ein in vielen Fällen nützlicher Ersatz ist die

Division mit Rest Zu je zwei Zahlen $n \in \mathbb{Z}$ und $m \in \mathbb{N}^*$ gibt es eindeutig bestimmte Zahlen $q \in \mathbb{Z}$ und $r \in \mathbb{N}$ so, dass

$$n = q \cdot m + r \quad \text{und} \quad 0 \leq r < m.$$

Der Buchstabe q steht für „Quotient“, r für „Rest“. Als Beziehung für rationale Zahlen kann man die obige Gleichung auch in der Form

$$\frac{n}{m} = q + \frac{r}{m}$$

schreiben. Dann ist q der ganzzahlige Anteil, $\frac{r}{m} \in \mathbb{Q}$ mit $0 \leq \frac{r}{m} < 1$ der kleinstmögliche gebrochene Rest.

Beweis Da $r = n - q \cdot m$ möglichst klein und nicht negativ sein soll, berechnet man für alle möglichen $k \in \mathbb{Z}$ die Differenz

$$\rho(k) := n - k \cdot m \in \mathbb{Z}.$$

Geometrisch kann man sich das so vorstellen, dass man die Lage von n relativ zur Menge $m \cdot \mathbb{Z}$ betrachtet. Auf diese Weise erhält man eine injektive Abbildung

$$\rho : \mathbb{Z} \rightarrow \mathbb{Z}, \quad k \mapsto \rho(k).$$

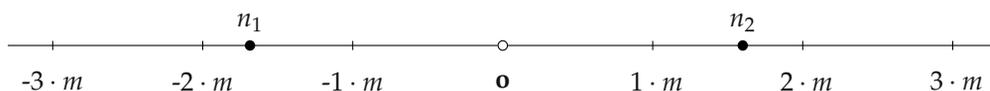
Die Werte von ρ können nicht alle negativ sein, in Zeichen

$$\rho(\mathbb{Z}) \cap \mathbb{N} \neq \emptyset.$$

Denn ist $n \geq 0$, so ist $\rho(0) = n \in \mathbb{N}$, für $n < 0$ ist

$$\rho(n) = n - n \cdot m = n(1 - m) \geq 0,$$

da $1 - m \leq 0$. Nach dem Satz vom kleinsten Element aus 1.2.1 gibt es einen kleinsten nicht negativen Rest $\rho(k_0) \in \mathbb{N}$; wir setzen $q := k_0$ und $r := \rho(k_0)$.



In unserer Skizze ist

$$q = 1 \text{ für } n = n_1 \quad \text{und} \quad q = -2 \text{ für } n = n_2.$$

Nach Definition von q und r gilt

$$n = q \cdot m + r.$$

Zum Nachweis der Existenz der gewünschten Darstellung ist nur noch $r < m$ zu zeigen. Wäre aber $r = \rho(k_0) \geq m$, so würde

$$0 \leq n - (k_0 + 1)m = \rho(k_0 + 1) < \rho(k_0) = n - k_0 m$$

folgen, im Widerspruch zur Wahl von k_0 .

Es bleibt die Eindeutigkeit der Darstellung zu zeigen. Angenommen

$$n = q \cdot m + r = q' \cdot m + r' \quad \text{mit} \quad 0 \leq r, r' < m.$$

Wir können $r \geq r'$, also $0 \leq r - r' < m$ annehmen. Indem man die beiden Darstellungen von n subtrahiert, erhält man

$$r - r' = (q' - q) \cdot m.$$

Also muss $q = q'$ und somit auch $r = r'$ sein. ■

Als Anwendung der Teilung mit Rest wollen wir die üblichen Darstellungen von natürlichen und damit auch ganzen Zahlen präzise begründen.

Nach dem naiven Vorgang des Zählens kann man eine natürliche Zahl n durch n Striche darstellen, damit gleichwertig ist die Darstellung

$$n = \underbrace{1 + 1 + \dots + 1}_{n\text{-mal}}.$$

Als Grundlage für effiziente Rechenverfahren war erst einmal die Entwicklung von handlicheren Darstellungen der natürlichen Zahlen nötig. Da der Mensch zehn Finger hat, war das Dezimalsystem besonders bevorzugt. Um zur üblichen *Dezimaldarstellung*

$$n = z_N z_{N-1} \dots z_1 z_0 \quad \text{mit} \quad z_i \in \{0, \dots, 9\} \quad \text{und} \quad z_N \neq 0$$

einer natürlichen Zahl $n \geq 1$ mit *Ziffern* z_i zu kommen, ist folgende Überlegung nötig.

Zunächst muss für das gegebene $n \geq 1$ die Position N ermittelt werden. Dazu betrachtet man die Menge

$$M := \{k \in \mathbb{N} : n < 10^k\} \subset \mathbb{N}.$$

Da ganz sicher $n < 10^n$, ist $M \neq \emptyset$. Nach dem Satz vom kleinsten Element aus 1.2.1 gibt es ein kleinstes $k_0 \in M$. Da $n \geq 1$, ist $k_0 \geq 1$, also $N := k_0 - 1 \in \mathbb{N}$.

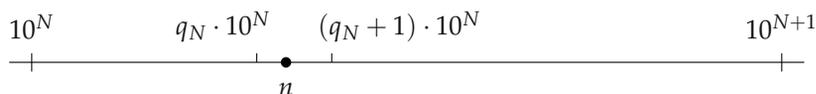
Die Position von n ist also eingeschränkt durch

$$10^N \leq n < 10^{N+1} = 10^{k_0}.$$

Nun wird n mit Rest durch 10^N geteilt:

$$n = q_N \cdot 10^N + r_N \quad \text{mit} \quad 0 \leq r_N < 10^N.$$

Zunächst weiß man nur, dass $q_N \in \mathbb{N}$. Nach der speziellen Wahl von N folgt aber $q \in \{1, \dots, 9\}$. Die genauere Position von n kann man so zeichnen:



Im zweiten Schritt wird der Rest r_N des ersten Schrittes mit Rest durch 10^{N-1} geteilt:

$$r_N = q_{N-1} 10^{N-1} + r_{N-1}, \quad \text{wobei} \quad q_{N-1} \in \{0, \dots, 9\} \quad \text{und} \quad 0 \leq r_{N-1} < 10^{N-1}.$$

Das führt man so lange weiter, bis man bei

$$r_1 = q_0 10^0 + r_0 \quad \text{mit} \quad q_0 \in \{0, \dots, 9\} \quad \text{und} \quad 0 \leq r_0 < 10^0 = 1,$$

also $r_0 = 0$ angekommen ist. Insgesamt erhält man die Summendarstellung

$$n = q_N \cdot 10^N + q_{N-1} \cdot 10^{N-1} + \dots + q_1 \cdot 10^1 + q_0 \cdot 10^0.$$

Wegen der Eindeutigkeit der Division mit Rest in jedem Schritt ist diese Darstellung insgesamt eindeutig.

Wie man an dem Verfahren sofort sieht, hätte man statt der Zahl 10 jede andere Zahl $g \in \mathbb{N}$ mit $g \geq 2$ verwenden können, da es stets ein kleinstes N mit $n < g^{N+1}$ gibt. In diesem Fall sind die Ziffern

$$q_i \in \{0, 1, \dots, g-1\}.$$

Wir fassen das Ergebnis zusammen:

Darstellungssatz Sei $g \in \mathbb{N}$ mit $g \geq 2$. Dann gibt es zu jeder Zahl $n \in \mathbb{N}$ eine eindeutige Darstellung

$$n = q_N \cdot g^N + q_{N-1} \cdot g^{N-1} + \dots + q_0 \cdot g^0 \quad (*)$$

mit $N \in \mathbb{N}$, $q_i \in \{0, \dots, g-1\}$ und $q_N \neq 0$.

Man nennt (*) die ***g-adische Darstellung*** von n . Im Fall $g = 10$ spricht man von der ***Dezimaldarstellung***, im Fall $g = 2$ von der ***binären Darstellung*** im ***Dualsystem***.

Als ganz einfaches Beispiel geben wir

$$37 = 3 \cdot 10^1 + 7 \cdot 10^0 = 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 100101.$$

1.3.2 Der Körper der rationalen Zahlen

Wie wir gesehen haben, hat man im Ring der ganzen Zahlen für jedes m ein Negatives $-m$, ein multiplikatives Inverses m^{-1} gibt es nur für $m = \pm 1$. Vom Standpunkt der Lösung von Gleichungen gibt es in \mathbb{Z} für

$$m + x = n \quad \text{die Lösung} \quad x = n - m,$$

für $m \cdot x = n$ mit $m \neq 0$ hat man nur dann eine Lösung $x = \frac{n}{m}$, wenn m ein Teiler von n ist. Die Aufgabe besteht nun darin, für einen beliebigen Bruch $\frac{n}{m}$ mit $m, n \in \mathbb{Z}$ und $m \neq 0$ eine präzise Erklärung zu geben und Rechenregeln dafür bereitzustellen.

Im Prinzip kann man ganz analog vorgehen wie bei der Erweiterung der additiven Halbgruppe \mathbb{N} zur Gruppe \mathbb{Z} . Den allgemeinen Rahmen für eine derartige Konstruktion findet man z.B. in $[\text{F1}_3]$.

Um dem Symbol $\frac{n}{m}$ eine formal präzise Erklärung zu geben, betrachtet man die Menge

$$\mathbb{Z} \times \mathbb{Z}^* = \{(n, m) : n, m \in \mathbb{Z}, m \neq 0\}.$$

Um die passende Äquivalenzrelation zu finden, bedenkt man, dass naiv gerechnet

$$\frac{n}{m} = \frac{n'}{m'} \quad \Leftrightarrow \quad n \cdot m' = m \cdot n'. \quad (=)$$

Entscheidend dabei ist, dass die Bedingung auf der rechten Seite in \mathbb{Z} geprüft werden kann. Nach dieser Vorüberlegung definieren wir auf $\mathbb{Z} \times \mathbb{Z}^*$ eine Relation durch

$$(n, m) \sim (n', m') : \Leftrightarrow n \cdot m' = m \cdot n'.$$

Ganz analog zu 1.2.4 prüft man nach, dass es sich um einen Äquivalenzrelation handelt. Dabei wird benutzt, dass die Multiplikation in \mathbb{Z} assoziativ und kommutativ ist, und dass die Kürzungsregel

$$m \cdot x = m \cdot y \Rightarrow x = y$$

gilt. Nun bezeichnen wir mit

$$\frac{n}{m} \text{ die Äquivalenzklasse von } (n, m);$$

nach dieser Definition ist die Beziehung $(=)$ präzise begründet. Eine solche Äquivalenzklasse $\frac{n}{m}$ heißt **rationale Zahl**, mit

$$\mathbb{Q} := \left\{ \frac{n}{m} : (n, m) \in \mathbb{Z} \times \mathbb{Z}^* \right\}$$

wird die Menge der rationalen Zahlen bezeichnet.

Die rationalen Zahlen sollen eine Erweiterung der ganzen Zahlen sein, das heißt $\mathbb{Z} \subset \mathbb{Q}$ soll eine Teilmenge sein. Das geht wie bei den meisten Erweiterungen nur durch eine „Identifikation“. Dabei betrachtet man die Abbildung

$$\mathbb{Z} \longrightarrow \mathbb{Q}, \quad n \mapsto \frac{n}{1}.$$

Sie ist offenbar injektiv, denn aus

$$\frac{n}{1} = \frac{n'}{1} \quad \text{folgt} \quad n \cdot 1 = 1 \cdot n', \quad \text{also} \quad n = n'.$$

Daher müssen wir zwischen n und dem Bruch $\frac{n}{1}$ nicht unterscheiden, wir können beide Elemente identifizieren (obwohl sie formal verschieden sind). Offensichtlich gilt dann auch

$$n = \frac{n \cdot k}{k} \quad \text{für alle } k \in \mathbb{Z}^*.$$

Ist nun $\mathbb{Z} \subset \mathbb{Q}$ als Teilmenge angesehen, so stellt sich die Frage, wie man die in \mathbb{Z} erklärten Operationen von Addition und Multiplikation nach \mathbb{Q} fortsetzen kann. Nahelegend ist folgender Versuch:

$$\frac{n}{m} + \frac{l}{k} := \frac{n \cdot k + l \cdot m}{m \cdot k} \quad \text{und} \quad \frac{n}{m} \cdot \frac{l}{k} := \frac{n \cdot l}{m \cdot k}.$$

Wie üblich muss man zeigen, dass dadurch die Operationen wohldefiniert sind, d.h. dass das Ergebnis nicht von der Wahl der Repräsentanten abhängt. Sei also

$$\frac{n}{m} = \frac{n'}{m'} \quad \text{und} \quad \frac{l}{k} = \frac{l'}{k'}, \quad \text{d.h.} \quad nm' = mn' \quad \text{und} \quad lk' = kl'.$$

Zur Wohldefiniertheit der Addition ist zu zeigen, dass

$$\frac{nk + lm}{mk} = \frac{n'k' + l'm'}{m'k'}, \quad \text{d.h.} \quad (nk + lm)m'k' = mk(n'k' + l'm').$$

Das folgt durch einfache Rechnung in \mathbb{Z} :

$$\begin{aligned} (nk + lm)m'k' &= nkm'k' + lmm'k' \\ &= nm'kk' + lk'mm' \\ &= mn'kk' + kl'mm' \\ &= mkn'k' + mkl'm'. \end{aligned}$$

Wir wollen nun zeigen, dass die Menge \mathbb{Q} der rationalen Zahlen zusammen mit der oben erklärten Addition und Multiplikation nicht nur ein Ring, sondern sogar ein „Körper“ ist. Dieser Begriff war zunächst von DEDEKIND unter dem Namen „Zahlkörper“ eingeführt worden, für ein System von Zahlen mit besonders guten Eigenschaften. Die allgemeine Definition geht auf WEBER [WEB] zurück.

Definition Ein Ring $(K, +, \cdot)$ heißt **Körper**, wenn $K^* = K \setminus \{0\}$ zusammen mit der Multiplikation eine abelsche Gruppe ist.

Das zu $a \in K^*$ eindeutig bestimmte multiplikative Inverse wird mit a^{-1} bezeichnet. Es gilt

$$a \cdot a^{-1} = a^{-1} \cdot a = 1.$$

Wer noch einmal ohne Benutzung der Begriffe Ring und Gruppe sehen möchte, welche Rechenregeln zu einem Körper gelten müssen, kann das in 0.1.1 nachlesen. Wir notieren zunächst noch einige Rechenregeln, die leicht aus den Axiomen folgen.

Bemerkung Ist K ein Körper, so gilt:

- a) $1 \neq 0$
- b) $0 \cdot a = a \cdot 0 = 0$ für alle $a \in K$.
- c) $a \cdot b = 0 \Rightarrow a = 0$ oder $b = 0$ für $a, b \in K$.
- d) $a \cdot (-b) = -(a \cdot b)$ und $(-a) \cdot (-b) = a \cdot b$ für $a, b \in K$.
- e) $x \cdot a = y \cdot a \Rightarrow x = y$ für $a \in K^*$ und $x, y \in K$.

Beweis a) ist klar, denn $1 \in K^* = K \setminus \{0\}$. Ein Körper enthält also mindestens zwei Elemente, nämlich 0 und 1.

b) folgt aus $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$.

c) folgt aus der Bedingung, dass K^* mit der Multiplikation eine Gruppe ist. Danach muss für $a, b \in K^*$ auch $a \cdot b \in K^*$ gelten.

d) folgt aus

$$ab + (-a)b = (a + (-a))b = 0 \cdot b = 0 \quad \text{und} \\ (-a)(-b) = -((-a)b) = -(-(ab)) = ab,$$

wobei für die ersten beiden Gleichungen die gerade bewiesene erste Regel verwendet wurde, für die dritte Gleichung die Rechenregel 1) für Gruppen aus 1.2.3.

e) folgt aus der Rechenregel 2) für Gruppen aus 1.2.3. ■

Nun kommen wir zum Ergebnis dieses Abschnitts.

Satz Die Menge \mathbb{Q} der **rationalen Zahlen** zusammen mit der oben erklärten Addition und Multiplikation ist ein Körper.

Beweis Im Prinzip sind all die in 0.1.1 zusammengestellten Regeln nachzuweisen. Das ist Routinearbeit; um den Leser (und auch den Schreiber) nicht zu langweilen führen wir nur einige Regeln aus. Was dabei verwendet wird, sind die Rechenregeln aus 1.3.1 im Ring \mathbb{Z} .

Zum Assoziativgesetz für die Addition:

$$\left(\frac{n}{m} + \frac{l}{k}\right) + \frac{s}{r} = \frac{nk + lm}{mk} + \frac{s}{r} = \frac{(nk + lm)r + smk}{mkr}, \\ \frac{n}{m} + \left(\frac{l}{k} + \frac{s}{r}\right) = \frac{n}{m} + \frac{lr + sk}{kr} = \frac{nkr + (lr + sk)m}{mkr}.$$

Da die Zähler der beiden Brüche ganz rechts gleich sind, folgt die Behauptung. Die Kommutativität der Addition folgt sofort aus der Definition. Nullelement ist $\frac{0}{1}$, Negatives von $\frac{n}{m}$ ist $\frac{-n}{m}$.

Dass $\frac{n}{m}$ und $\frac{l}{k}$ in \mathbb{Q}^* liegen, bedeutet $n \neq 0$ und $l \neq 0$. Dann ist auch

$$\frac{n}{m} \cdot \frac{l}{k} = \frac{n \cdot l}{m \cdot k} \in \mathbb{Q}^*, \quad \text{denn in } \mathbb{Z} \text{ gilt } m \cdot k \neq 0 \quad \text{und} \quad n \cdot l \neq 0.$$

Die Assoziativität und die Kommutativität der Multiplikation sind leicht zu prüfen. Ein multiplikatives Inverses $\frac{l}{k}$ von $\frac{n}{m}$ mit $n \neq 0$ und $m \neq 0$ muss die Bedingung

$$\frac{n}{m} \cdot \frac{l}{k} = \frac{n \cdot l}{m \cdot k} = \frac{1}{1}, \quad \text{also } nl = mk, \quad \text{also } \frac{l}{k} = \frac{m}{n}$$

erfüllen. Damit ist das Inverse

$$\left(\frac{n}{m}\right)^{-1} = \frac{m}{n}$$

eindeutig bestimmt. Auch das Distributivgesetz erfordert nur einfache Rechnung. ■

Wie wir gesehen haben, kann man die natürlichen Zahlen als Teil der ganzen Zahlen ansehen, und diese als Teil der rationalen Zahlen, in Zeichen

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}.$$

An dieser Stelle scheint es angebracht, grundlegende Begriffe für die Beziehungen zwischen Ringen zu erwähnen.

Definition Sei $(R, +, \cdot)$ ein Ring und $R' \subset R$ eine Teilmenge. R' heißt **Unterring** von R , wenn für alle $a, b \in R'$ gilt

$$1) \quad a - b \in R'. \quad 2) \quad a \cdot b \in R'.$$

Bedingung 1) bedeutet nach 1.2.5, dass R' eine Untergruppe von $(R, +)$ ist. Bedingung 2) kann man auch so ausdrücken: R' ist abgeschlossen gegenüber der Multiplikation in R .

Ist $R' \subset R$ ein Unterring, so wird die Ringstruktur von R auf R' vererbt, so wie das schon im Fall von Untergruppen bei nur einer Verknüpfung erklärt worden war. Ein ganz einfaches Beispiel ist

$$R' = m\mathbb{Z} \subset \mathbb{Z} = R,$$

wobei $m \in \mathbb{N}$ beliebig gewählt werden kann. Da es nach dem Lemma aus 1.2.5 keine anderen Untergruppen von $(\mathbb{Z}, +)$ gibt, sind das auch die einzigen möglichen Unterringe von \mathbb{Z} .

Außerdem ist $\mathbb{Z} \subset \mathbb{Q}$ ein Unterring, wenn man die ganze Zahl n mit dem Bruch $\frac{n}{1}$ „identifiziert“, was wir zuvor schon getan hatten. Das kann man noch etwas genauer – aber auch umständlicher – beschreiben. Dazu benötigen wir die

Definition Seien R und S Ringe, wobei wir zur Vereinfachung Addition und Multiplikation in beiden Ringen mit dem gleichen Symbol $+$ und \cdot bezeichnen. Eine Abbildung

$$\varphi : R \rightarrow S$$

heißt **Homomorphismus** von Ringen, wenn für alle $a, b \in R$ gilt:

$$\mathbf{1)} \quad \varphi(a + b) = \varphi(a) + \varphi(b). \quad \mathbf{2)} \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

Ein Homomorphismus heißt **Isomorphismus**, wenn er bijektiv ist.

Ein ganz einfaches Beispiel für einen Homomorphismus von Ringen ist die für jedes $m \in \mathbb{N}$ erklärte Abbildung

$$\varphi_m : \mathbb{Z} \rightarrow \mathbb{Z}, \quad x \mapsto m \cdot x.$$

Das Bild $\varphi_m(\mathbb{Z})$ ist der Unterring $m\mathbb{Z}$.

Nun – wie versprochen – zu einer präziseren Beschreibung der ganzen Zahlen als Teil der rationalen Zahlen. Wir betrachten die Abbildung

$$\varphi : \mathbb{Z} \rightarrow \mathbb{Q}, \quad n \mapsto \frac{n}{1}.$$

Nach den Rechenregeln für Brüche in \mathbb{Q} ist φ ein Homomorphismus von Ringen:

$$\varphi(m + n) = \frac{m + n}{1} = \frac{m}{1} + \frac{n}{1} = \varphi(m) + \varphi(n), \quad \varphi(m \cdot n) = \frac{m \cdot n}{1} = \frac{m}{1} \cdot \frac{n}{1} = \varphi(m) \cdot \varphi(n).$$

Das Bild $\varphi(\mathbb{Z}) \subset \mathbb{Q}$ besteht aus den Brüchen, die eine Darstellung mit dem Nenner 1 besitzen, und die Einschränkung von φ

$$\varphi' : \mathbb{Z} \rightarrow \varphi(\mathbb{Z})$$

ist bijektiv, also ein Isomorphismus. All das kann man wie zuvor wieder einfacher ausdrücken: Wir identifizieren \mathbb{Z} mit seinem isomorphen Bild $\varphi(\mathbb{Z})$, dann kann man $\mathbb{Z} \subset \mathbb{Q}$ als Teilmenge ansehen.

Analog werden wir solche Identifikationen bei Körpern durchführen. Dabei heißt eine Teilmenge $K' \subset K$ eines Körpers $(K, +, \cdot)$ Unterkörper, wenn $K' \subset K$ Unterring ist und wenn außerdem

$$a^{-1} \in K' \quad \text{für alle } a \in K' \quad \text{mit } a \neq 0.$$

In diesem Fall erbt K' von K die Struktur eines Körpers. Beispiele dafür werden folgen:

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Schließlich erscheint es nützlich, die abstrakten Hintergründe des Rechnens mit Ungleichungen zu beleuchten.

Man nennt eine ganze Zahl $n \in \mathbb{Z}$ **positiv**, in Zeichen $n > 0$, wenn $n \in \mathbb{N}^*$, d.h. $n \in \mathbb{N}$ und $n \neq 0$.

Diese übliche Bezeichnung kann man zum Begriff der „Anordnung“ in einem beliebigen kommutativen und nullteilerfreien Ring R verallgemeinern.

Eine **Anordnung** in R ist erklärt durch eine Teilmenge $P \subset R$ von Elementen, die **positiv** genannt werden, in Zeichen

$$x > 0 \quad :\Leftrightarrow \quad x \in P,$$

so dass folgende Axiome erfüllt sind:

O1 Für jedes $x \in R$ gilt genau eine der folgenden Eigenschaften:

$$x > 0 \quad \text{oder} \quad x = 0 \quad \text{oder} \quad -x > 0.$$

O2 $x, y > 0 \Rightarrow x + y > 0$ und $x \cdot y > 0$.

In diesem Sinne ist also durch $P := \mathbb{N}^*$ eine Anordnung in \mathbb{Z} erklärt.

Durch eine Anordnung in einem Ring R kann man auch „größer“- und „kleiner“-Beziehungen zwischen beliebigen Elementen erklären:

Für $x, y \in R$ sei

$$x > y \quad :\Leftrightarrow \quad x - y > 0 \quad \text{und} \quad x \geq y \quad :\Leftrightarrow \quad (x > y \quad \text{oder} \quad x = y).$$

$$x < y \quad :\Leftrightarrow \quad y > x \quad \text{und} \quad x \leq y \quad :\Leftrightarrow \quad (x < y \quad \text{oder} \quad x = y).$$

Aus den Axiomen kann man die üblichen Rechenregeln für Ungleichungen in Ringen und Körpern ableiten (vgl. etwa [FO₁, §3]).

Besonders wichtig sind die Regeln

$$x \neq 0 \quad \Rightarrow \quad x^2 > 0 \quad \text{für alle} \quad x \in R, \quad \text{insbesondere gilt} \quad 1 > 0.$$

Beispiele für Ringe, die keine Anordnung zulassen, werden wir in 1.3.6 und 1.3.7 antreffen.

In einem Ring R kann man für $x \in R$ und $n \in \mathbb{N}$ stets das „Produkt“

$$n \cdot x := \underbrace{x + \dots + x}_{n\text{-mal}} \in R.$$

erklären. Eine Anordnung in R heißt nun **archimedisch**, wenn es für beliebige $x, y \in R$ mit $x > 0$ ein $n \in \mathbb{N}$ gibt, so dass $n \cdot x > y$. Wesentlich dabei ist, dass y beliebig groß und x beliebig klein sein darf.

Ganz einfach erhält man die

Bemerkung 1 Die durch \mathbb{N}^* erklärte Anordnung auf \mathbb{Z} ist archimedisch.

Beweis Für $x, y \in \mathbb{N}^*$ setzen wir $n := y + 1$. Dann ist

$$n \cdot x = (y + 1) \cdot x = y \cdot x + x \geq y + 1 > y.$$

■

Die betrachtete Anordnung im Ring \mathbb{Z} kann man nun fortsetzen zu einer Anordnung im Körper \mathbb{Q} , die erklärt ist durch

$$x = \frac{n}{m} > 0 : \Leftrightarrow \begin{cases} m > 0 & \text{und } n > 0 \\ m < 0 & \text{und } n < 0 \end{cases} \text{ oder}$$

Nun prüft man ganz leicht nach, dass diese Definition die Axiome einer Anordnung erfüllt. Mit Hilfe von Bemerkung 1 erhält man

Bemerkung 2 Die oben erklärte Anordnung des Körpers \mathbb{Q} der rationalen Zahlen ist archimedisch.

Beweis Sind $x, y \in \mathbb{Q}$ mit $x > 0$ und $y > 0$, so gibt es Darstellungen

$$x = \frac{k}{l} \quad \text{und} \quad y = \frac{r}{s} \quad \text{mit} \quad k, l, r, s \in \mathbb{N}^*.$$

Für ein beliebiges $n \in \mathbb{N}$ ist

$$n \cdot x - y = \frac{nks - rl}{ls}.$$

Nach Bemerkung 1 kann man n so wählen, dass $n(ks) > rl$, dann ist auch $n \cdot x > y$. ■

Schließlich kann man in einem Ring R mit Anordnung einen **Betrag** oder **Absolutbetrag** erklären, indem man für alle $x \in R$

$$|x| := \begin{cases} x & \text{für } x \geq 0, \\ -x & \text{für } x < 0 \end{cases}$$

setzt. Wie man leicht nachweist, gelten für $x, y \in R$ die Rechenregeln (vgl. [FO₁, §3])

$$|x \cdot y| = |x| \cdot |y| \quad \text{und} \quad |x + y| \leq |x| + |y|.$$

1.3.3 Dezimalbruchentwicklung rationaler Zahlen*

In 1.3.1 hatten wir eine ganze Zahl $n \in \mathbb{Z}$ durch wiederholte Teilung mit Rest g -adisch dargestellt, wobei $g \in \mathbb{N}$ mit $g \geq 2$ war. Für $g = 10$ ergab sich die Dezimaldarstellung

$$n = \pm z_N z_{N-1} \dots z_0 = \sum_{i=0}^N z_i \cdot 10^i \quad (*)$$

mit $N \in \mathbb{N}$ und Ziffern $z_i \in \{0, \dots, 9\}$. In diesem Abschnitt wollen wir uns mit der üblichen Darstellung einer rationalen Zahl als Dezimalbruch beschäftigen, etwa

$$\frac{4}{3} = 1.333\dots$$

Hier sind die unendlich vielen Positionen nach dem Punkt $.$ mit der Ziffer 3 besetzt. Zunächst einmal muss präzise geklärt werden, was ein derartiger Ausdruck bedeuten soll. Allgemein schreiben wir einen **Dezimalbruch** als einen zunächst nur formalen Ausdruck

$$z = \pm z_{-N} \dots z_0 . z_1 z_2 \dots = \pm \left(\sum_{i=-N}^0 z_i \cdot 10^{-i} + \sum_{i=1}^{\infty} z_i \cdot 10^{-i} \right) = \pm \sum_{i=-N}^{\infty} z_i \cdot 10^{-i} \quad (**)$$

mit $N \in \mathbb{N}$ und Ziffern $z_i \in \{0, \dots, 9\}$. Man beachte die veränderte Reihenfolge der Summation im Vergleich zu (*): In (**) steigt die Summe von einer negativen Zahl $-N$ über 0 und 1 auf nach ∞ . Der erste Teil der Summe ist endlich und stellt wie in (*) eine ganze Zahl dar, dem zweiten unendlichen Teil muss erst eine mehr als formale Bedeutung gegeben werden. Zunächst kann man für jedes $n \in \mathbb{N}$ eine endliche **Partialsomme**

$$s_n(z) := \pm \sum_{i=-N}^n z_i \cdot 10^{-i}$$

erklären; offensichtlich ist $s_n(z) \in \mathbb{Q}$. Die Betrachtung der Folge $(s_n(z))$ von rationalen Zahlen ist ein grundlegendes Problem der elementaren reellen Analysis. In diesem Abschnitt wollen wir erst einmal spezielle Dezimalbrüche untersuchen.

Definition Ein Dezimalbruch $z = \pm z_{-N} \dots z_0 . z_1 z_2 \dots$ heißt **periodisch**, wenn er von der Form

$$z_{-N} \dots z_0 . z_1 \dots z_k \overline{z_{k+1} \dots z_{k+l}}$$

mit $k \in \mathbb{N}$ und $l \in \mathbb{N}^*$ ist, wobei der Querstrich bedeutet, dass sich die Ziffernfolge $z_{k+1} \dots z_{k+l}$ anschließend unendlich oft wiederholt. Formaler aufgeschrieben bedeutet das, dass

$$z_{i+l} = z_i \quad \text{für} \quad i \geq k+1.$$

Ist die Zahl $l \geq 1$ minimal gewählt, so heißt sie die **Periodenlänge**. Ist $k \geq 0$ minimal gewählt, so heißt die Ziffernfolge $z_1 \dots z_k$ die **Vorperiode**. Im Fall $k = 0$ heißt der Dezimalbruch **rein periodisch**. Ist $l = 1$ und $z_{k+1} = 0$, so heißt der Dezimalbruch **abbrechend**.

Im Fall eines abbrechenden Dezimalbruchs kann man

$$z = \pm z_{-N} \dots z_0 \cdot z_1 \dots z_k \bar{0} = \pm z_{-N} \dots z_0 \cdot z_1 \dots z_k.$$

schreiben.

Nun zeigen wir, dass die periodischen Dezimalbrüche den rationalen Zahlen entsprechen. Genauer gilt:

Satz a) Bei einem periodischen Dezimalbruch konvergieren die Partialsummen gegen eine rationale Zahl.

b) Jede rationale Zahl $\frac{n}{m}$ lässt sich durch einen periodischen Dezimalbruch darstellen. Für die Periodenlänge l gilt $l \leq m - 1$.

Beweis Für Teil a) genügt es, einen Dezimalbruch der Form

$$z = 0 \cdot z_1 \dots z_k \overline{z_{k+1} \dots z_{k+l}} \quad (*)$$

zu betrachten. Aus der Analysis benötigen wir die Summenformel für die *geometrische Reihe*. Es genügt dabei der Spezialfall rationaler Zahlen:

$$\sum_{i=0}^{\infty} x^i = \frac{1}{1-x} \quad \text{für } x \in \mathbb{Q} \quad \text{mit } |x| < 1.$$

Daraus folgt für $l \in \mathbb{N}^*$ die Formel

$$\sum_{i=0}^{\infty} \left(\frac{1}{10^l} \right)^i = \frac{10^l}{10^l - 1}.$$

Für $l = 1$ bedeutet das $1.111\dots = 1.\bar{1} = \frac{10}{9}$.

Nun zerlegen wir den gegebenen Dezimalbruch (*) entsprechend seiner Vorperiode und seiner Periode: Ist

$$v := z_1 \cdot 10^{-1} + \dots + z_k \cdot 10^{-k} \quad \text{und} \quad p := z_{k+1} \cdot 10^{-(k+1)} + \dots + z_{k+l} \cdot 10^{-(k+l)},$$

so gilt $v, p \in \mathbb{Q}$. Die Folge der Partialsummen von z entspricht der unendlichen Summe

$$v + p \cdot \sum_{i=0}^{\infty} \left(\frac{1}{10^l} \right)^i = v + \frac{p \cdot 10^l}{10^l - 1},$$

und das ist eine rationale Zahl.

Ein ganz einfaches Beispiel ist $z = 0.\bar{3}$. Hier ist

$$v = 0 \quad \text{und} \quad p = 3 \cdot 10^{-1}, \quad \text{also} \quad z = \frac{3 \cdot 10^{-1} \cdot 10}{10 - 1} = \frac{3}{9} = \frac{1}{3}.$$

Ein weiteres wichtiges Beispiel ist $z = 0.\bar{9}$. Hier ist

$$v = 0 \quad \text{und} \quad p = 9 \cdot 10^{-1}, \quad \text{also} \quad z = \frac{9 \cdot 10^{-1} \cdot 10}{10 - 1} = \frac{9}{9} = 1.$$

Die Gleichung $0.\bar{9} = 1$ hat schon viele Diskussionen ausgelöst. Natürlich ist jeder endliche Abschnitt des Dezimalbruchs $0.\bar{9}$ noch kleiner als 1, aber der Unterschied wird mit wachsender Länge des Abschnitts immer geringer. Die Gleichung $0.\bar{9} = 1$ ist eine Aussage über den Grenzwert der Folge von Partialsummen. Außerdem zeigt die Gleichung $0.\bar{9} = 1.\bar{0}$, dass die Dezimalbruchentwicklung einer rationalen Zahl nicht eindeutig sein muss. Auf diese Frage kommen wir in 1.3.5 zurück.

Allgemeiner erhält man mit der oben bewiesenen Summenformel

$$0.\bar{z}_1 = \frac{z_1}{9}, \quad 0.\overline{z_1 z_2} = \frac{10 \cdot z_1 + z_2}{99}, \quad 0.\overline{z_1 z_2 z_3} = \frac{100 \cdot z_1 + 10 \cdot z_2 + z_3}{999}, \quad \text{usw.}$$

Man beachte, dass dagegen $0.z_1 z_2 z_3 = \frac{100 \cdot z_1 + 10 \cdot z_2 + z_3}{1000}$.

Zum Nachweis von Teil b) können wir $m > 0$ annehmen und durch Division mit Rest nach 1.3.1

$$\frac{n}{m} = q + \frac{r}{m} \quad \text{mit} \quad q, r \in \mathbb{Z} \quad \text{und} \quad 0 \leq r < m$$

darstellen. Es genügt also die Dezimalbruchentwicklung von $\frac{r}{m}$ anzugeben, d.h. wir können $0 \leq n < m$ annehmen. Um eine Darstellung $0.z_1 z_2 \dots$ von $\frac{r}{m}$ zu erhalten, rechnet man nach dem aus der Schule bekannten Verfahren:

Im ersten Schritt dividiert man $10n$ mit Rest durch m . Setzt man $r_0 := n$, so ergibt das

$$\frac{10n}{m} = \frac{10r_0}{m} = z_1 + \frac{r_1}{m} \quad \text{mit} \quad z_1, r_1 \in \mathbb{N}, 0 \leq r_1 < m.$$

Wegen $n < m$ ist $z_1 < 10$, also $z_1 \in \{0, \dots, 9\}$. Im zweiten Schritt dividiert man $10r_1$ mit Rest durch m , das ergibt

$$\frac{10r_1}{m} = z_2 + \frac{r_2}{m}, \quad \text{und allgemeiner}$$

$$\frac{10r_i}{m} = z_{i+1} + \frac{r_{i+1}}{m} \quad \text{mit} \quad z_{i+1} \in \{0, \dots, 9\}, r_{i+1} \in \mathbb{N} \quad \text{und} \quad 0 \leq r_{i+1} < m.$$

Wir notieren die Ergebnisse in einigen Beispielen:

$$\frac{1}{4} : \begin{array}{|c|c|c|c|c|} \hline i & 0 & 1 & 2 & 3 \\ \hline z_i & & 2 & 5 & \mathbf{0} \\ \hline r_i & 1 & 2 & \mathbf{0} & \mathbf{0} \\ \hline \end{array} \dots,$$

$$\text{also} \quad \frac{1}{4} = 0.25\bar{0}.$$

$$\frac{7}{9} : \begin{array}{|c|c|c|c|c|} \hline i & 0 & 1 & 2 & 3 \\ \hline z_i & & \mathbf{7} & \mathbf{7} & \mathbf{7} \\ \hline r_i & \mathbf{7} & \mathbf{7} & \mathbf{7} & \mathbf{7} \\ \hline \end{array} \dots,$$

$$\text{also} \quad \frac{7}{9} = 0.777\dots = 0.\bar{7}.$$

$$\frac{1}{7} : \begin{array}{c|cccccccc} i & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline z_i & & \mathbf{1} & \mathbf{4} & \mathbf{2} & \mathbf{8} & \mathbf{5} & \mathbf{7} & \mathbf{1} & \mathbf{4} \\ \hline r_i & \mathbf{1} & \mathbf{3} & \mathbf{2} & \mathbf{6} & \mathbf{4} & \mathbf{5} & \mathbf{1} & \mathbf{3} & \mathbf{2} \end{array} \dots, \quad \text{also } \frac{1}{7} = 0.\overline{142857}.$$

$$\frac{5}{6} : \begin{array}{c|cccc} i & 0 & 1 & 2 & 3 \\ \hline z_i & & \mathbf{8} & \mathbf{3} & \mathbf{3} \\ \hline r_i & \mathbf{5} & \mathbf{2} & \mathbf{2} & \mathbf{2} \end{array} \dots, \quad \text{also } \frac{5}{6} = 0.8\overline{3}.$$

Im Fall $\frac{1}{4}$ bricht der Dezimalbruch ab.

Im Fall $\frac{7}{9}$ wären Reste $0 \leq r_i \leq 8$ möglich, es bleibt immer nur die 7; also verlaufen alle Schritte gleich, es gibt keine Vorperiode und die Periodenlänge ist $l = 1$.

Im Fall $\frac{1}{7}$ treten bei den ersten 6 Schritten alle möglichen Reste $1 \leq r_i \leq 6$ auf, dann ist $r_6 = r_0$ und für die Periodenlänge erhält man $l = 6$.

Im Fall $\frac{5}{6}$ hat man eine Vorperiode der Länge $k = 1$ und $l = 1$.

Mit Hilfe der Dezimalbruchentwicklung von $\frac{1}{7}$ erhält man

$$\frac{22}{7} = 3\frac{1}{7} = 3.\overline{142857}.$$

Das ist eine für viele Zwecke brauchbare rationale Approximation der Kreiszahl

$$\pi = 3.141\,592\,653\,589\,793\,238\,462\,643\,383\,279\,502\,884\,197\,169\,399\,375\,105\,820\,974\,944\dots$$

deren Dezimalbruchentwicklung keine Periode und eine Ziffernfolge hat, die von einer zufällig entstandenen Folge nicht zu unterscheiden ist. Ein Rekord im auswendigen Aufsagen der Stellen von π liegt bei 22 514 (vgl. [ZI, p. 49]).

Eine bessere rationale Approximation von π ist

$$\frac{355}{113} = 3.\overline{141\,592\,920\,353\dots7168}.$$

Dieser Dezimalbruch hat keine Vorperiode und die maximale Periodenlänge von 112.

Nach den obigen Beispielen ist klar, wie man die Periodenlänge l abschätzen kann. Man betrachtet die Folge (r_i) der Reste. Dabei müssen unendlich viele Positionen mit Zahlen aus $\{0, \dots, m - 1\}$ besetzt werden. Betrachten wir die ersten m Reste

$$r_0, r_1, \dots, r_{m-1}.$$

Entweder es gibt ein $k \in \{0, \dots, m - 1\}$ mit $r_k = 0$. Dann ist $z_i = 0$ für $i \geq k + 1$, und der Dezimalbruch bricht ab. Andernfalls treten nur die $m - 1$ von 0 verschiedenen Reste auf, es muss also ein Rest mehrmals auftreten. Sind k und $k + l$ mit $0 \leq k < k + l \leq m - 1$ die kleinsten auftretenden Positionen gleicher Reste, so ergibt sich daraus eine Periodizität

$$0.z_1 \dots z_k \overline{z_{k+1} \dots z_{k+l}}$$

des iterativ aus $\frac{n}{m}$ berechneten Dezimalbruchs. Um zu zeigen, dass dieser Dezimalbruch gegen $\frac{n}{m}$ konvergiert, genügt es, die Partialsummen s_N auszurechnen. Setzt man die in der Iteration erhaltenen Werte von z_i ein, so erhält man

$$\begin{aligned}\frac{n}{m} &= z_1 \cdot 10^{-1} + \frac{r_1}{m} \cdot 10^{-1} = z_1 \cdot 10^{-1} + z_2 \cdot 10^{-2} + \dots + z_N \cdot 10^{-N} + \frac{r_N}{m} \cdot 10^{-N} \\ &= s_N + \frac{r_N}{m} \cdot 10^{-N}.\end{aligned}$$

Da $0 \leq r_N < m$, folgt $|\frac{n}{m} - s_N| \leq 10^{-N}$, das ergibt die Konvergenz. ■

1.3.4 Konstruktion der reellen Zahlen*

Vorsicht! So wie im Vorspann eines jugendgefährdenden Filmes sei hier vorsorglich gewarnt, dass die beiden folgenden Abschnitte nur für Leser mit genügender mathematischer Reife geeignet sind.

Will man den Gipfel eines hohen Berges erreichen, so hat man zwei wesentlich verschiedene Möglichkeiten: Man kann den Rucksack packen und mit einigen Zwischenstationen an Berghütten zu Fuß hinaufsteigen. Oder aber man fliegt mit einem Hubschrauber über das Gebirge und sucht einen Landeplatz in der Umgebung des Gipfels. Bei der ersten mühsamen Methode sieht man auf dem Weg viele Einzelheiten, bei der zweiten hat man aus der Höhe einen weit besseren Überblick.

Ähnlich ist es bei der Einführung der reellen Zahlen. Man kann die Axiome dafür angeben, es ist ein *vollständig archimedisch angeordneter Körper*, und damit weiter arbeiten (vgl. etwa [FO₁]). Das entspricht der Landung mit dem Hubschrauber. Von dort oben kann man dann die natürlichen Zahlen unten im Tal als Vielfache der reellen Zahl 1 ansehen, die rationalen Zahlen sind dann ein Teilkörper des Körpers der reellen Zahlen.

Wir haben in den vorhergehenden Abschnitten den Fußweg angetreten und ausgehend von den natürlichen Zahlen die ganzen und die rationalen Zahlen formal präzise eingeführt. Das war etwas langwierig, aber doch recht elementar gewesen. Nun aber steht die schwierigste Etappe bevor: In Geometrie und Analysis benötigt man viele nicht rationale Zahlen, wie etwa $\sqrt{2}$, π oder e . Mit solchen irrationalen oder „inkommensurablen“ Größen hat man sich schon im Altertum beschäftigt, Vieles davon findet sich schon bei EUKLID ([EU]). Geometrisch gesehen ist es nun die Aufgabe, die rationalen Zahlen zu vervollständigen zu einer „lückenlosen“ reellen Zahlengeraden. Dieses Projekt wurde in formal präziser Weise erst um 1860 in Angriff genommen, ein Klassiker ist das Buchlein von DEDEKIND [DED₁].

Ein naheliegender Einstieg in die Konstruktion der reellen Zahlen ergibt sich aus der schon in 0.1.1 gemachten Erfahrung, dass bei der rationalen Approximation von $\sqrt{2}$ die Perioden der Dezimalbrüche immer länger werden. Außerdem ist in der Praxis eine

reelle Zahl immer nur durch einen endlichen Dezimalbruch gegeben. Es liegt also nahe, eine reelle Zahl als einen Dezimalbruch mit beliebiger Ziffernfolge darzustellen, d.h.

$$z = \pm z_{-N} \dots z_{-1} z_0 \cdot z_1 z_2 \dots = \pm \sum_{i=-N}^{\infty} z_i \cdot 10^{-i} \text{ mit } z_i \in \{0, \dots, 9\}.$$

Für jedes $n \in \mathbb{N}$ bezeichnen wir mit

$$s_n(z) := \pm \sum_{i=-N}^n z_i \cdot 10^{-i} = z_{-N} \dots z_0 \cdot z_1 \dots z_n$$

die n -te Partialsumme von z . Offensichtlich ist $s_0(z) \in \mathbb{Z}$ und $s_n(z) \in \mathbb{Q}$ für $n \in \mathbb{N}^*$.

Es treten sofort gravierende *Probleme* auf:

- 1) Ist die Folge $(s_n(z))$ der Partialsummen konvergent?
- 2) Wie addiert und multipliziert man unendliche Dezimalbrüche?
- 3) Wie viele verschiedene Darstellungen einer reellen Zahl als Dezimalbruch gibt es?

Zu *Problem 1*) kann man zunächst nur sagen, dass die Folge (s_n) nicht gegen eine rationale Zahl konvergieren muss. Etwa der Dezimalbruch

$$0.101\ 001\ 000\ 1\dots$$

mit Blöcken von Nullen zunehmender Länge ist nicht periodisch, also kann er nach dem Satz aus 1.3.3 keine rationale Zahl darstellen.

Zu *Problem 2*) betrachten wir zwei Dezimalbrüche

$$z = 0.z_1 z_2 z_3 \dots \quad \text{und} \quad w = 0.w_1 w_2 w_3 \dots \quad \text{mit} \quad z_i, w_i \in \{0, \dots, 9\}.$$

Die Summen $z_i + w_i$ der Ziffern können größer als 9 werden, das ergibt Überträge in die vorhergehenden Stellen. Ist etwa

$$z = 0.99\dots 99\bar{0} \quad \text{und} \\ w = 0.00\dots 01\bar{0},$$

wobei die letzte Ziffer 9 von z und die Ziffer 1 von w an beliebig hoher Position n stehen können, so ist stets

$$z + w = 1.\bar{0}.$$

Daran sieht man, dass eine Ziffer im Dezimalbruch von $z + w$ im Allgemeinen erst dann feststeht, wenn alle Stellen von z und w berücksichtigt worden sind. Bei abbrechenden Dezimalbrüchen kann man mit der Addition hinten anfangen, bei unendlichen Dezimalbrüchen gibt es kein „ganz hinten“. Noch komplizierter sind die Probleme mit der Multiplikation von unendlichen Dezimalbrüchen.

Problem 3) wird sich als relativ harmlos erweisen: Man kann die Dezimalbruchdarstellungen eindeutig machen, indem man in der Menge aller Dezimalbrüche nur die Teilmenge derjenigen betrachtet, die keine unendlichen Neunerperioden haben.

Ziel dieses Abschnitts ist es, eine Konstruktion des Körpers \mathbb{R} der reellen Zahlen zu skizzieren. Dabei ist es von Vorteil, sich zunächst von den vor allem wegen Problem 2) sehr tückischen Dezimalbrüchen zu lösen. Nach dem Ende eines relativ langen Umwegs werden wir in 1.3.5 wieder auf die Dezimalbrüche zurückkommen.

Von den zahlreichen Möglichkeiten der Konstruktion reeller Zahlen erwähnen wir drei:

- Mit den sogenannten **DEDEKINDSchen Schritten**, die in $[\text{DED}_1]$ beschrieben werden.
- Mit **Intervallschachtelungen**, d.h. Folgen von Intervallen $I_n = [a_n, b_n]$ mit $a_n, b_n \in \mathbb{Q}$, so dass $I_0 \supset I_1 \supset I_2 \supset \dots$ und $\lim_{n \rightarrow \infty} (b_n - a_n) = 0$. Dieser von WEIERSTRASS angegebene Zugang ist besonders anschaulich.
- Mit CAUCHY-Folgen rationaler Zahlen.

Wir folgen hier dem von CANTOR $[\text{CA}_1]$ vorgeschlagenen Weg c), der auch bei anderen Problemen der „Vervollständigung“ in der Analysis gangbar ist. Dazu muss zunächst an einige Eigenschaften von Folgen erinnert werden.

Definition Gegeben sei eine Folge (a_n) rationaler Zahlen.

Diese Folge heißt **konvergent** gegen $a \in \mathbb{Q}$, in Zeichen $a = \lim_{n \rightarrow \infty} a_n$, wenn es zu jedem rationalen $\varepsilon > 0$ ein $N \in \mathbb{N}$ gibt, so dass

$$|a - a_n| < \varepsilon \quad \text{für } n \geq N.$$

Die Folge (a_n) heißt **CAUCHY-Folge**, wenn es zu jedem rationalen $\varepsilon > 0$ ein $N \in \mathbb{N}$ gibt, so dass

$$|a_n - a_m| < \varepsilon \quad \text{für } n, m \geq N.$$

Die Folge (a_n) heißt **Nullfolge**, wenn $\lim_{n \rightarrow \infty} a_n = 0$.

Wie man in der Analysis lernt, ist jede konvergente Folge eine CAUCHY-Folge $[\text{Fo}_1, \S 5]$. Dass nicht jede CAUCHY-Folge rationaler Zahlen gegen eine rationale Zahl konvergiert, folgt mit Hilfe eines nicht periodischen Dezimalbruchs aus der folgenden

Bemerkung Für jeden Dezimalbruch ist die Folge (s_n) der Partialsummen eine rationale CAUCHY-Folge. Genauer gilt $|s_n - s_m| < 10^{-m}$ für $n, m \in \mathbb{N}$ und $n > m$.

Beweis Da $z_i \leq 9$ für alle i , erhält man mit Hilfe einer geometrischen Reihe

$$\begin{aligned} |s_n - s_m| &= \sum_{i=m+1}^n z_i \cdot 10^{-i} < 9 \cdot \sum_{i=m+1}^{\infty} 10^{-i} = 9 \cdot 10^{-(m+1)} \cdot \sum_{i=0}^{\infty} \left(\frac{1}{10}\right)^i \\ &= 9 \cdot 10^{-(m+1)} \cdot \frac{1}{1 - \frac{1}{10}} = 10^{-m}. \end{aligned}$$

Also genügt es, N so zu wählen, dass $10^{-N} < \varepsilon$. ■

Im Gegensatz zu den starren Dezimalbrüchen kann man mit beliebigen Folgen rationaler Zahlen bequem rechnen. Sind (a_n) und (b_n) Folgen rationaler Zahlen, so hat man eine

$$\begin{aligned} \text{Summenfolge} \quad (a_n) + (b_n) &:= (a_n + b_n) \quad \text{und eine} \\ \text{Produktfolge} \quad (a_n) \cdot (b_n) &:= (a_n \cdot b_n). \end{aligned}$$

Wir benutzen folgende in der Analysis bewiesenen

Konvergenzeigenschaften Für Folgen (a_n) und (b_n) rationaler Zahlen gilt:

a) Sind (a_n) und (b_n) konvergent, so sind auch $(a_n + b_n)$ und $(a_n \cdot b_n)$ konvergent, und es gilt

$$\lim_{n \rightarrow \infty} (a_n + b_n) = \lim_{n \rightarrow \infty} a_n + \lim_{n \rightarrow \infty} b_n, \quad \lim_{n \rightarrow \infty} (a_n \cdot b_n) = \left(\lim_{n \rightarrow \infty} a_n \right) \cdot \left(\lim_{n \rightarrow \infty} b_n \right).$$

b) Sind (a_n) und (b_n) CAUCHY-Folgen, so sind auch $(a_n + b_n)$ und $(a_n \cdot b_n)$ CAUCHY-Folgen.

c) Ist $a_n \neq 0$ für alle n und gibt es ein rationales $c > 0$ und ein $N \in \mathbb{N}$ so dass $|a_n| \geq c$ für $n \geq N$, so ist auch (a_n^{-1}) eine CAUCHY-Folge.

Folglich hat man auf der Menge \mathcal{C} aller rationalen CAUCHY-Folgen eine Addition und eine Multiplikation. Reine Routine ist der Beweis von folgendem

Lemma 1 Die Menge \mathcal{C} aller rationalen CAUCHY-Folgen zusammen mit der oben erklärten Addition und Multiplikation ist ein kommutativer Ring mit Einselement.

Nullelement in \mathcal{C} ist die konstante Folge (0) , Einselement die konstante Folge (1) . Gibt es in einer Folge (a_n) mindestens ein n mit $a_n = 0$, so gibt es zu (a_n) keine multiplikativ inverse Folge. Also ist der Ring \mathcal{C} kein Körper.

Es gibt eine naheliegende injektive Abbildung

$$\mathbb{Q} \rightarrow \mathcal{C}, a \mapsto (a),$$

die jeder rationalen Zahl a die konstante Folge (a) zuordnet, aber es gibt sehr viele rationale Folgen (a_n) die gegen a konvergieren. Um aus dem Ring \mathcal{C} einen Körper zu machen, muss man eine geeignete Äquivalenz von Folgen erklären. Dazu sei

$$\mathcal{N} := \{(c_n) \in \mathcal{C} : (c_n) \text{ ist Nullfolge}\}$$

und für $(a_n), (b_n) \in \mathcal{C}$ wird die Äquivalenz erklärt durch

$$(a_n) \sim (b_n) :\Leftrightarrow (a_n - b_n) \in \mathcal{N},$$

d.h. wenn die Differenzfolge eine Nullfolge ist.

Um zu zeigen, dass dadurch eine Äquivalenzrelation erklärt ist, und um eine Standardkonstruktion der Ringtheorie ausführen zu können, benötigen wir

Lemma 2 Die Menge $\mathcal{N} \subset \mathcal{C}$ der rationalen Nullfolgen im Ring der rationalen CAUCHY-Folgen ist ein **Ideal**, d.h. es gilt

- 1) $(a_n), (b_n) \in \mathcal{N} \Rightarrow (a_n - b_n) \in \mathcal{N}$,
- 2) $(a_n) \in \mathcal{C}, (b_n) \in \mathcal{N} \Rightarrow (a_n \cdot b_n) \in \mathcal{N}$.

Beweis Zu 1): Sei $\varepsilon > 0$ vorgegeben. Zu $\frac{\varepsilon}{2}$ können wir für die beiden Folgen ein gemeinsames N finden, so dass

$$|a_n| < \frac{\varepsilon}{2} \quad \text{und} \quad |b_n| < \frac{\varepsilon}{2} \quad \text{für} \quad n \geq N.$$

Nach der Dreiecksungleichung folgt

$$|a_n - b_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon \quad \text{für} \quad n \geq N.$$

Zu 2): Wir benutzen, dass die Folge (a_n) beschränkt ist, was man leicht mit $\varepsilon = 1$ sehen kann. Es gibt also ein $0 < c \in \mathbb{Q}$, so dass $|a_n| \leq c$ für alle n . Zu $\varepsilon > 0$ wählen wir für (b_n) ein N , so dass für $n \geq N$

$$|b_n| < \frac{\varepsilon}{c}, \quad \text{also folgt} \quad |a_n \cdot b_n| < c \cdot \frac{\varepsilon}{c} = \varepsilon.$$

■

Als Folgerung aus Lemma 2 ergibt sich sofort, dass durch die obige Definition eine Äquivalenzrelation erklärt ist, und dass die Äquivalenzklasse einer Folge (a_n) aus \mathcal{C} gegeben ist durch

$$\{(b_n) \in \mathcal{C} : (b_n) \sim (a_n)\} = (a_n) + \mathcal{N} = \{(a_n + c_n) : (c_n) \in \mathcal{N}\}.$$

Anders ausgedrückt ist \mathcal{N} die Menge der Differenzen aus einer Äquivalenzklasse:

$$(c_n) = (b_n - a_n).$$

Nun folgt eine Definition, die auf den ersten Blick vom Himmel zu fallen scheint:

Eine **reelle Zahl** α ist erklärt als eine Äquivalenzklasse rationaler CAUCHY-Folgen, in Zeichen

$$\alpha = (a_n) + \mathcal{N}.$$

Mit \mathbb{R} wird die Menge aller reellen Zahlen bezeichnet.

Die Erwartung an die reellen Zahlen ist, dass sie die rationalen Zahlen zu einer lückenlosen Zahlengeraden vervollständigen. Daher wollen wir zunächst zeigen, wie man \mathbb{Q} in \mathbb{R} wiederfinden kann. Zu jedem $a \in \mathbb{Q}$ kann man die konstante Folge (a) betrachten, das ergibt eine Abbildung

$$\iota : \mathbb{Q} \longrightarrow \mathbb{R}, a \mapsto \iota(a) := (a) + \mathcal{N}.$$

Diese Abbildung ι ist offenbar injektiv, denn für $a, b \in \mathbb{Q}$ mit $a \neq b$ ist $(a - b)$ als konstante Folge keine Nullfolge. Im nächsten Schritt wird \mathbb{R} so zu einem Körper gemacht, dass die Körperstruktur von \mathbb{Q} auf \mathbb{R} ausgedehnt wird.

Theorem Auf der Menge \mathbb{R} der reellen Zahlen ist durch

$$\begin{aligned} ((a_n) + \mathcal{N}) + ((b_n) + \mathcal{N}) &:= (a_n + b_n) + \mathcal{N} \quad \text{und} \\ ((a_n) + \mathcal{N}) \cdot ((b_n) + \mathcal{N}) &:= (a_n \cdot b_n) + \mathcal{N} \end{aligned}$$

eine Addition und Multiplikation wohldefiniert; \mathbb{R} wird damit zu einem Körper. Die injektive Abbildung $\iota : \mathbb{Q} \rightarrow \mathbb{R}$ ist ein Homomorphismus von Ringen; daher kann man $\iota(\mathbb{Q})$ mit \mathbb{Q} identifizieren, somit wird $\mathbb{Q} \subset \mathbb{R}$ ein Unterkörper.

In der Sprache der Ringtheorie ist \mathbb{R} der **Restklassenring** \mathcal{C}/\mathcal{N} .

Beweis Sei $(a_n) \sim (a'_n)$ und $(b_n) \sim (b'_n)$. Dann ist

$$\begin{aligned} (a_n + b_n) - (a'_n + b'_n) &= (a_n - a'_n) + (b_n - b'_n) \in \mathcal{N} \quad \text{und} \\ (a_n \cdot b_n) - (a'_n \cdot b'_n) &= (a_n \cdot b_n - a'_n \cdot b'_n) = (b'_n) \cdot (a_n - a'_n) + (a_n) \cdot (b_n - b'_n) \in \mathcal{N}, \end{aligned}$$

denn \mathcal{N} ist ein Ideal. Also sind Addition und Multiplikation wohldefiniert.

Die Ringeigenschaften von \mathcal{C} übertragen sich mühelos auf \mathbb{R} . Entscheidend ist nun, dass es zu jedem

$$\alpha = (a_n) + \mathcal{N} \quad \text{mit} \quad (a_n) \notin \mathcal{N}$$

ein Inverses $\alpha^{-1} = (b_n) + \mathcal{N}$ gibt. Bedingung dafür ist

$$((a_n) + \mathcal{N}) \cdot ((b_n) + \mathcal{N}) = (1) + \mathcal{N}, \text{ d.h. } (a_n \cdot b_n - 1) \in \mathcal{N}.$$

Wir müssen also eine geeignete Folge (b_n) konstruieren. Da $(a_n) \notin \mathcal{N}$, gibt es ein $N \in \mathbb{N}$ und ein $0 < c \in \mathbb{Q}$, so dass $|a_n| \geq c$ für alle $n \geq N$. Wir definieren

$$b_n := \begin{cases} 1 & \text{für } n < N, \\ a_n^{-1} & \text{für } n \geq N. \end{cases}$$

Nach Teil c) der oben angegebenen Konvergenzeigenschaften ist (b_n) wieder eine rationale CAUCHY-Folge, für $n \geq N$ ist $(a_n \cdot b_n)$ die konstante Folge (1) . Also gilt $(a_n \cdot b_n - 1) \in \mathcal{N}$.

Zu rationalen Zahlen a, b gehören die reellen Zahlen $\iota(a) = (a) + \mathcal{N}$, $\iota(b) = (b) + \mathcal{N}$. Nach der Definition von Addition und Multiplikation gilt

$$\begin{aligned}\iota(a + b) &= (a + b) + \mathcal{N} = ((a) + \mathcal{N}) + ((b) + \mathcal{N}) = \iota(a) + \iota(b) \quad \text{und} \\ \iota(a \cdot b) &= (a \cdot b) + \mathcal{N} = ((a) + \mathcal{N}) \cdot ((b) + \mathcal{N}) = \iota(a) \cdot \iota(b).\end{aligned}$$

Also ist $\iota : \mathbb{Q} \rightarrow \mathbb{R}$ ein injektiver Homomorphismus von Ringen. ■

Wir wollen noch kurz skizzieren, wie man die weiteren in den Axiomen der reellen Zahlen geforderten Eigenschaften in dem so konstruierten Körper \mathbb{R} nachweisen kann. Dabei wollen wir zur Vereinfachung der Bezeichnungen nicht mehr zwischen einer rationalen Zahl $a \in \mathbb{Q}$ und der durch die konstante Folge (a) repräsentierten reellen Zahl $\iota(a) + \mathcal{N} \in \mathbb{R}$ unterscheiden.

Zunächst erklären wir in \mathbb{R} eine **Anordnung**. Dazu genügt es zu erklären, wann eine reelle Zahl **positiv** ist (vgl. 1.3.2).

Zusatz 1 *Im Körper \mathbb{R} der reellen Zahlen ist durch*

$$\alpha = (a_n) + \mathcal{N} > 0 \quad :\Leftrightarrow \quad \text{Es gibt ein } a \in \mathbb{Q} \text{ mit } a > 0 \text{ und ein } N \in \mathbb{N} \\ \text{so dass } a_n \geq a \text{ für alle } n \geq N$$

eine archimedische Anordnung erklärt.

Man beachte bei dieser Definition, dass die Ungleichungen $a > 0$ und $a_n \geq a$ für rationale Zahlen gelten müssen, dafür sind sie schon in 1.3.2 erklärt.

Beweisskizze Zunächst sieht man, dass die Eigenschaft $\alpha > 0$ wohldefiniert, d.h. unabhängig vom Repräsentanten (a_n) ist. Zu zeigen sind dann die folgenden Eigenschaften für alle $\alpha, \beta \in \mathbb{R}$:

- a) Für jedes α gilt entweder $\alpha > 0$ oder $\alpha = 0$ oder $-\alpha > 0$.
- b) $\alpha > 0$ und $\beta > 0 \Rightarrow \alpha + \beta > 0$ und $\alpha \cdot \beta > 0$.
- c) Zu $\alpha > 0$ und $\beta > 0$ gibt es ein $n \in \mathbb{N}$ so dass $n \cdot \alpha > \beta$, d.h. $n \cdot \alpha - \beta > 0$.

1) und 2) überlassen wir dem Leser zur Übung. Zu 3) setzen wir

$$\alpha = (a_n) + \mathcal{N} \quad \text{und} \quad \beta = (b_n) + \mathcal{N}.$$

Aus der Definition von $\alpha > 0$ folgt, dass es ein $a \in \mathbb{Q}$ gibt, mit $\alpha \geq a > 0$. Da jede CAUCHY-Folge beschränkt ist, gibt es ein $b \in \mathbb{Q}$ mit $b \geq \beta > 0$. Da \mathbb{Q} archimedisch angeordnet ist, gibt es ein $n \in \mathbb{N}$ mit $n \cdot a > b$, also folgt $n \cdot \alpha \geq n \cdot a > b \geq \beta$. ■

Mit Hilfe der Anordnung kann man nun für eine reelle Zahl α den **Absolutbetrag** erklären durch

$$|\alpha| := \begin{cases} \alpha & \text{für } \alpha \geq 0, \\ -\alpha & \text{für } \alpha < 0. \end{cases}$$

Nun beginnt das entscheidende Finale. Mit Hilfe des Absolutbetrages in \mathbb{R} kann man ganz analog zu \mathbb{Q} für eine Folge (a_n) reeller Zahlen erklären, wann sie gegen eine reelle Zahl α konvergiert, und wann sie eine CAUCHY-Folge ist. Für die dabei nötigen Abschätzungen reeller Zahlen eine kleine

Vorbemerkung Sei $\alpha = (a_n) + \mathcal{N} \in \mathbb{R}$. Wenn es zu einem rationalen $\varepsilon > 0$ ein $N \in \mathbb{N}$ gibt, so dass $|a_n| \leq \frac{\varepsilon}{2}$ für alle $n \geq N$, so folgt $|\alpha| < \varepsilon$.

Beweis Zunächst ist klar, dass $|\alpha| = (|a_n|) + \mathcal{N}$. Für $n \geq N$ ist

$$|a_n| \leq \frac{\varepsilon}{2} \Rightarrow \varepsilon - |a_n| \geq \frac{\varepsilon}{2} \Rightarrow \varepsilon - |\alpha| > 0 \Rightarrow |\alpha| < \varepsilon. \quad \blacksquare$$

Nach der Definition einer reellen Zahl α gehört dazu eine Klasse äquivalenter CAUCHY-Folgen rationaler Zahlen. Es ist mehr als plausibel, dass jede dieser Folgen rationaler Zahlen gegen die neu eingeführte Zahl α konvergiert. Präzise formuliert ist das die

Bemerkung Ist $\alpha = (a_n) + \mathcal{N} \in \mathbb{R}$, so folgt $\alpha = \lim_{n \rightarrow \infty} a_n$.
Anders ausgedrückt: Die rationalen Zahlen liegen **dicht** in den reellen Zahlen.

Beweis Da es zu jedem reellen $\varepsilon > 0$ ein rationales ε' mit $0 < \varepsilon' < \varepsilon$ gibt, genügt es zu zeigen, dass für jedes rationale $\varepsilon > 0$ ein $N \in \mathbb{N}$ existiert, so dass

$$|\alpha - a_n| < \varepsilon \quad \text{für } n \geq N. \quad (*)$$

Da (a_n) eine rationale CAUCHY-Folge ist, gibt es zu $0 < \varepsilon \in \mathbb{Q}$ ein $N \in \mathbb{N}$ mit

$$|a_n - a_m| \leq \frac{\varepsilon}{2} \quad \text{für } n, m \geq N.$$

Nach der Definition der Differenz reeller Zahlen ist

$$\alpha - a_n = (b_n) + \mathcal{N} \quad \text{mit } b_n = a_n - a_N.$$

Da $b_N = 0$, folgt $|b_n| = |b_n - b_N| = |a_n - a_N| \leq \frac{\varepsilon}{2}$ für $n \geq N$. Somit folgt (*) aus der Vorbemerkung. ■

Nun stehen alle Hilfsmittel bereit zum Beweis der wichtigsten Eigenschaft der reellen Zahlen.

Zusatz 2 Der Körper \mathbb{R} ist **vollständig**, d.h. jede CAUCHY-Folge (α_n) in \mathbb{R} konvergiert gegen ein $\alpha \in \mathbb{R}$, in Zeichen

$$\lim_{n \rightarrow \infty} \alpha_n = \alpha.$$

Beweis Jede reelle Zahl α_n ist durch eine Folge gegeben, wir haben also eine Folge von Folgen zu betrachten. Dazu ist etwas Sorgfalt in den Bezeichnungen erforderlich.

Jede der reellen Zahlen α_n ist Grenzwert einer Folge rationaler Zahlen. Zu jedem α_n gibt es also ein $a_n \in \mathbb{Q}$ mit

$$|\alpha_n - a_n| < \frac{1}{n} \quad \text{für } n \in \mathbb{N}^*.$$

Nun ist es naheliegend, die Folge (a_n) rationaler Zahlen zu betrachten, das ist eine Art von „Diagonalfolge“. Es sind zwei Beweisschritte nötig:

- (1) Die Folge (a_n) ist eine CAUCHY-Folge.
- (2) Setzt man $\alpha := (a_n) + \mathcal{N}$, so gilt $\alpha = \lim_{n \rightarrow \infty} \alpha_n$.

Zu (1) : Zu vorgegebenem rationalem $\varepsilon > 0$ können wir ein $N \in \mathbb{N}^*$ wählen, so dass

$$|\alpha_n - \alpha_m| \leq \frac{\varepsilon}{3} \quad \text{für } n, m \geq N, \quad \text{sowie } N \geq \frac{3}{\varepsilon}, \text{ also } \frac{1}{N} \leq \frac{\varepsilon}{3}.$$

Dann folgt nach der Dreiecksungleichung für $n, m \geq N$

$$|a_n - a_m| \leq |\alpha_n - a_n| + |\alpha_n - \alpha_m| + |\alpha_m - a_m| < \frac{1}{n} + \frac{\varepsilon}{3} + \frac{1}{m} \leq \varepsilon.$$

Zu (2) : Wieder zu vorgegebenem rationalem $\varepsilon > 0$ können wir ein $N \in \mathbb{N}^*$ wählen, so dass

$$|\alpha - a_n| \leq \frac{\varepsilon}{2} \quad \text{für } n \geq N, \quad \text{sowie } N \geq \frac{2}{\varepsilon}, \text{ also } \frac{1}{N} \leq \frac{\varepsilon}{2}.$$

Daraus folgt für $n \geq N$

$$|\alpha - \alpha_n| \leq |\alpha - a_n| + |\alpha_n - a_n| < \frac{\varepsilon}{2} + \frac{1}{n} \leq \varepsilon.$$

■

1.3.5 Reelle Zahlen als Dezimalbrüche*

Das entscheidende Problem mit den unendlichen Dezimalbrüchen ist, dass man nicht recht weiß, wie man sie addieren oder multiplizieren soll. Daher war es von Vorteil

gewesen, nicht nur die Folgen der Partialsummen von Dezimalbrüchen, sondern allgemein die Menge \mathcal{C} aller rationalen CAUCHY-Folgen zu betrachten; \mathcal{C} konnte ganz einfach zu einem Ring gemacht werden. Aus dieser Sicht kann man noch einmal die Menge \mathcal{D} aller Dezimalbrüche betrachten. Man hat nach der Bemerkung aus 1.3.4 eine Abbildung

$$s : \mathcal{D} \rightarrow \mathcal{C}, z \mapsto s(z) = (s_n(z)),$$

die jedem Dezimalbruch z die rationale Folge $(s_n(z))$ der Partialsummen zuordnet. Die Abbildung s ist offensichtlich injektiv, aber $s(\mathcal{D}) \subset \mathcal{C}$ ist kein Unterring. Um das zu sehen, genügt es, die Dezimalbrüche $z = 0.9$ und $w = 0.1$ zu betrachten. In diesem Fall ist

$$s_0(z) = s_0(w) = 0 \quad \text{und} \quad s_1(z) = 0.9, \quad s_1(w) = 0.1.$$

Die Summenfolge ist $(a_0, a_1, a_2, \dots) = (0, 1, 1, \dots)$ mit $a_1 - a_0 = 1$. Dies kann nicht die Folge der Partialsummen irgend eines Dezimalbruchs u sein, da stets

$$|s_1(u) - s_0(u)| \leq 0.9 < 1$$

sein muss. Damit ist der Mangel der Dezimalbrüche auch aus abstrakter Sicht beleuchtet. Die Abbildung $s : \mathcal{D} \rightarrow \mathcal{C}$ kann man fortsetzen zur Abbildung

$$\sigma : \mathcal{D} \rightarrow \mathbb{R}, z \mapsto \sigma(z) = (s_n(z)) + \mathcal{N},$$

die jedem *Dezimalbruch* z die dadurch dargestellte reelle Zahl $\sigma(z)$ zuordnet. Ist

$$z = \pm z_{-N} \dots z_{-1} z_0 \cdot z_1 z_2 \dots,$$

so ist nach den Ergebnissen von 1.3.4 die Schreibweise

$$\sigma(z) = \sum_{i=-N}^{\infty} z_i \cdot 10^{-i} \in \mathbb{R}$$

als unendliche Summe gerechtfertigt. Während die Abbildung $s : \mathcal{D} \rightarrow \mathcal{C}$ injektiv war, ist das bei σ nicht mehr der Fall. Die einfachsten Beispiele sind $z = 0.\bar{9}$ und $w = 1.\bar{0}$, allgemeiner

$$z = 0.z_1 \dots z_{k-1} z_k \bar{9} \quad \text{und} \\ w = 0.z_1 \dots z_{k-1} (z_k + 1) \bar{0},$$

wobei $z_k \in \{0, \dots, 8\}$ und $k \in \mathbb{N}^*$ beliebig ist. In beiden Fällen ist $z \neq w$ als Dezimalbrüche, aber $\sigma(z) = \sigma(w)$ als reelle Zahlen. Es ist nicht schwer zu zeigen, dass es keine anderen Beispiele gibt.

Lemma 1 *Angenommen, es gibt für ein $\alpha \in \mathbb{R}$ zwei verschiedene Darstellungen*

$$\alpha = \sum_{i=1}^{\infty} z_i \cdot 10^{-i} \quad \text{und} \tag{1}$$

$$\alpha = \sum_{i=1}^{\infty} w_i \cdot 10^{-i}, \tag{2}$$

wobei $z_i, w_i \in \{0, \dots, 9\}$, $z_i = w_i$ für $i = 1, \dots, k-1$ und $z_k < w_k$. Dann folgt

$$w_k = z_k + 1, \quad \text{und für } i \geq k+1 \text{ ist } z_i = 9, w_i = 0.$$

Beweis Für $\beta := \alpha - \sum_{i=1}^k z_i \cdot 10^{-i}$ erhält man aus (1) und (2) die Darstellungen

$$\beta = \sum_{i=k+1}^{\infty} z_i \cdot 10^{-i} \quad \text{und} \quad (1')$$

$$\beta = (w_k - z_k) \cdot 10^{-k} + \sum_{i=k+1}^{\infty} w_i \cdot 10^{-i}. \quad (2')$$

Das ergibt die Abschätzungen

$$\beta \leq \sum_{i=k+1}^{\infty} 9 \cdot 10^{-i} = 9 \cdot 10^{-(k+1)} \cdot \sum_{i=0}^{\infty} \left(\frac{1}{10}\right)^i = 10^{-k} \quad \text{und} \quad (1'')$$

$$\beta \geq (w_k - z_k) \cdot 10^{-k} \geq 10^{-k}. \quad (2'')$$

Also muss $\beta = 10^{-k}$ sein. Da dann die beiden Ungleichungen scharf sind, folgt $z_i = 9$ für $i \geq k+1$ aus (1'') und $w_k = z_k + 1$, sowie $w_i = 0$ für $i \geq k+1$ aus (2''). ■

Um eine einfache Sprechweise zu haben, nennen wir einen Dezimalbruch

$$\pm z_{-N} \dots z_0 \cdot z_1 z_2 \dots \in \mathcal{D}$$

echt, wenn er keine unendliche Neunerperiode hat. Mit

$$\mathcal{D}^* \subset \mathcal{D}$$

bezeichnen wir die Teilmenge der echten Dezimalbrüche. Da man jeden Dezimalbruch durch Multiplikation mit einem Faktor $\pm 10^{-N-1}$ auf die Form $0.w_1 w_2 \dots$ bringen kann, folgt aus dem obigen Lemma 1 das

Korollar Die Abbildung

$$\sigma^* : \mathcal{D}^* \rightarrow \mathbb{R}, \quad \pm z_{-N} \dots z_0 \cdot z_1 z_2 \dots \mapsto \pm \sum_{i=-N}^{\infty} z_i \cdot 10^{-i},$$

ist injektiv.

Um zu zeigen, dass die Abbildung $\sigma^* : \mathcal{D}^* \rightarrow \mathbb{R}$ sogar bijektiv ist, beweisen wir wie üblich durch iterierte Teilung mit Rest das folgende

Lemma 2 Jede reelle Zahl hat eine Darstellung als Dezimalbruch, d.h. zu $\alpha \in \mathbb{R}$ gibt es eine Darstellung

$$\alpha = \pm \sum_{i=-N}^{\infty} z_i \cdot 10^{-i} \quad \text{mit } N \in \mathbb{N} \quad \text{und } z_i \in \{0, \dots, 9\}.$$

Beweis Es genügt, den Fall $\alpha \geq 0$ zu betrachten. Nach dem Archimedischen Axiom gibt es eine eindeutig bestimmte Zahl $n \in \mathbb{N}$, so dass $n \leq \alpha < n + 1$. Für den ganzzahligen Anteil $n = \lfloor \alpha \rfloor$ hatten wir schon in 1.3.1 eine Dezimaldarstellung berechnet, die wir in der Form

$$n = \sum_{i=-N}^0 z_i \cdot 10^{-i} \quad \text{mit } N \in \mathbb{N} \quad \text{und } z_i \in \{0, \dots, 9\}$$

schreiben, damit der folgende Rest der Summe von 1 nach ∞ aufsteigen kann.

Jeder einzelne Schritt der Konstruktion beruht auf folgender Tatsache: Zu $\beta \in \mathbb{R}$ mit $0 \leq \beta < 10$ gibt es eine eindeutige Darstellung

$$\beta = z + \varrho \quad \text{mit } z \in \{0, \dots, 9\}, \varrho \in \mathbb{R} \quad \text{und } 0 \leq \varrho < 1.$$

Die Ziffer z ist der ganzzahlige Anteil von β , die reelle Zahl ϱ ist der Rest.

Zur Bestimmung von z_1 beginnen wir mit $\varrho_0 := \alpha - n$.

Da $0 \leq \varrho_0 < 1$, ist $0 \leq 10 \cdot \varrho_0 < 10$, also

$$10 \cdot \varrho_0 = z_1 + \varrho_1 \quad \text{mit } z_1 \in \{0, \dots, 9\} \quad \text{und } 0 \leq \varrho_1 < 1.$$

Daraus folgt $\alpha = n + \varrho_0 = n + z_1 \cdot 10^{-1} + \varrho_1 \cdot 10^{-1}$. Weiter ist analog

$$10 \cdot \varrho_1 = z_2 + \varrho_2, \quad \text{also } \alpha = n + z_1 \cdot 10^{-1} + z_2 \cdot 10^{-2} + \varrho_2 \cdot 10^{-2}.$$

Allgemeiner erhält man die Ziffer z_k aus der Zerlegung

$$10 \cdot \varrho_{k-1} = z_k + \varrho_k, \quad \text{es gilt } \alpha = n + \sum_{i=1}^k z_i \cdot 10^{-i} + \varrho_k \cdot 10^{-k}.$$

Für den in jedem Schritt verbleibenden Rest gilt $\varrho_k \cdot 10^{-k} < 10^{-k}$, also konvergiert die unendliche Summe. Natürlich kann man mit diesem Verfahren auch die schon in 1.3.1 bewiesene Dezimaldarstellung von n mit ableiten. ■

Nun ist das Endergebnis erreicht:

Satz Die Abbildung $\sigma^* : \mathcal{D}^* \rightarrow \mathbb{R}$, die jedem echten Dezimalbruch die dadurch dargestellte reelle Zahl zuordnet, ist bijektiv. Dadurch wird auch \mathcal{D}^* zu einem vollständig archimedisch angeordneten Körper. Eine Zahl $\sigma^*(z) \in \mathbb{R}$ ist genau dann rational, wenn der Dezimalbruch $z \in \mathcal{D}^*$ periodisch ist.

Beweis Nach Lemma 2 ist die Abbildung $\sigma : \mathcal{D} \rightarrow \mathbb{R}$ surjektiv, nach Lemma 1 ist auch σ^* surjektiv. Man kann sich auch davon überzeugen, dass der in Lemma 2 konstruierte Dezimalbruch schon selbst echt ist. Die Aussage über die Rationalität folgt aus 1.3.3. ■

Mit diesem abschließenden Satz ist gezeigt, dass die unendlichen Dezimalbrüche geeignet sind, die reellen Zahlen zu beschreiben. Für die *Praxis* gibt es kein Problem: Jede reelle Zahl kann nur durch einen endlichen Abschnitt des Dezimalbruchs approximiert werden, das aber mit beliebiger Genauigkeit. Die endlichen Abschnitte kann man addieren und multiplizieren, die Ergebnisse approximieren Summen und Produkte. Dabei rechnet man in Wirklichkeit nur mit rationalen Zahlen.

Für die *Theorie* kann man Summen und Produkte unendlicher Dezimalbrüche immerhin über den in den letzten Abschnitten beschriebenen Umweg berechnen. Das geht so: Gegeben

$$\alpha = \sum_{i=-N}^{\infty} z_i \cdot 10^{-i} \quad \text{und} \quad \beta = \sum_{i=-N}^{\infty} w_i \cdot 10^{-i}.$$

Dann bilden wir für $n \geq 0$ die Partialsummen

$$s_n(\alpha) = \sum_{i=-N}^n z_i \cdot 10^{-i} \quad \text{und} \quad s_n(\beta) = \sum_{i=-N}^n w_i \cdot 10^{-i}.$$

Aus den CAUCHY-Folgen $(s_n(\alpha))$ und $(s_n(\beta))$ berechnet man die CAUCHY-Folgen $(s_n(\alpha) + s_n(\beta))$ und $(s_n(\alpha) \cdot s_n(\beta))$. Wie schon bemerkt sind das im Allgemeinen keine Folgen von Partialsummen eines Dezimalbruchs. Aber ihre Äquivalenzklassen sind die reellen Zahlen $\alpha + \beta$ und $\alpha \cdot \beta$. Deren Dezimalbruchentwicklung kann man nach Lemma 2 berechnen. Das ist fürwahr ein Umweg!

Auf jeden Fall sollte man sich daran erinnern, wie tückisch die zunächst so verführerisch aussehenden Dezimalbrüche sein können.

Noch ein paar Worte zur Gesamtheit \mathbb{R} aller reellen Zahlen. Man kann sie nach den bewiesenen Eigenschaften ersetzen durch die relativ übersichtliche Menge der echten Dezimalbrüche. Aber um deren Gesamtheit präzise anzugeben, müsste man alle möglichen Folgen von Ziffern beschreiben. Das ist kaum möglich, und auch gar nicht nötig. Die Situation ist im Prinzip nicht anders als bei der Gesamtheit aller natürlichen Zahlen: Für die Arbeit damit ist es gar nicht erforderlich, sie allesamt irgendwo abgelegt zu haben. Es genügt, dass man in allen auftretenden Fällen zu jeder Zahl $n \in \mathbb{N}$ noch eins drauflegen kann zu $n + 1$ und damit gegebene natürliche Zahlen n, m auch uneingeschränkt addieren und multiplizieren kann.

Analog ist es bei den reellen Zahlen. Wann immer eine CAUCHY-Folge oder ein Dezimalbruch (etwa durch eine rekursive Konstruktion wie bei den Wurzeln) auftritt: man weiß, dass dadurch eine wohlbestimmte reelle Zahl erklärt ist.

1.3.6 Komplexe Zahlen

Die komplexen Zahlen kann man als die bedeutendste Erfindung in der Mathematik ansehen. Ansporn dafür war das Problem gewesen, Polynomgleichungen vom Grad zwei und höher zu lösen. Das einfachste Beispiel ist die Gleichung

$$x^2 = -1.$$

Da Quadrate reeller Zahlen nie negativ sein können, gibt es keine reelle Lösung dieser Gleichung. Als Ersatz hat man schon lange mit einer „imaginären Größe“ i gerechnet, von der man nur vorausgesetzt hat, dass $i^2 = -1$ gilt. Mehr zu der langen Geschichte hierzu findet man in [EB, Kap. 3]. Erst um 1800 war es gelungen, die komplexen Zahlen auf ein solides Fundament zu stellen. Nachdem schon 1797 der norwegische Landvermesser C. WESSEL eine **Zahlenebene** betrachtet hatte, veröffentlichte GAUSS 1831 in [GA₃] eine Konstruktion als die Menge von Summen der Form $a + bi$, zunächst für die Zahlentheorie nur mit ganzen Zahlen a, b :

quando campus arithmeticae ad quantitates *imaginarias* extenditur, ita ut absque restrictione ipsius obiectum constituent numeri formae $a + bi$, denotantibus i , pro more quantitatem imaginariam $\sqrt{-1}$, atque a, b indefinite omnes numeros reales integros inter $-\infty$ et $+\infty$. Tales numeros vocabimus *numeros integros complexos*, ita quidem, ut reales complexis non opponantur, sed tamquam species sub his contineri censeantur.

„... also stehen die reellen den komplexen Größen nicht entgegen, sondern sie enthalten diese als einen speziellen Fall unter sich.“

Betrachtet man solche Summen $a + bi$ (der Buchstabe i bleibt für einen Index reserviert) allgemeiner mit reellen a, b , so werden Addition und Multiplikation nahegelegt durch die folgenden naiven Rechnungen unter Benutzung der Beziehung $i^2 = -1$:

$$\begin{aligned}(a + bi) + (a' + b'i) &= (a + a') + (b + b')i \\ (a + bi) \cdot (a' + b'i) &= aa' + (ab' + ba')i + (bb')i^2 \\ &= (aa' - bb') + (ab' + ba')i.\end{aligned}$$

Präziser wird daraus die folgende Beschreibung mit Hilfe der Ebene

$$\mathbb{R}^2 = \{(a, b) : a, b \in \mathbb{R}\}.$$

Neben der Addition von Vektoren

$$(a, b) + (a', b') := (a + a', b + b') \quad (+)$$

führt man eine Multiplikation ein durch die Definition

$$(a, b) \cdot (a', b') := (aa' - bb', ab' + ba'). \quad (\cdot)$$

Dass diese Operationen viele Wünsche erfüllen, zeigt der

Satz Die Menge $\mathbb{C} := \mathbb{R}^2$ mit der oben erklärten Addition und Multiplikation ist ein Körper. Einselement ist $(1,0)$ und das multiplikative Inverse von $(a,b) \neq (0,0)$ ist gegeben durch

$$(a,b)^{-1} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right). \quad (*)$$

Identifiziert man ein $a \in \mathbb{R}$ mit $(a,0) \in \mathbb{C}$, so wird $\mathbb{R} \subset \mathbb{C}$ ein Unterkörper. Erklärt man weiter die **imaginäre Einheit** als

$$\mathbf{i} := (0,1),$$

so hat jede komplexe Zahl (a,b) eine eindeutige Darstellung

$$(a,b) = a + b\mathbf{i} \quad \text{mit} \quad a, b \in \mathbb{R}$$

und $\mathbf{i}^2 = (-1,0) = -1 \in \mathbb{R}$.

Beweis Der Vektorraum \mathbb{R}^2 ist mit seiner Addition (+) eine abelsche Gruppe. Dass die durch (\cdot) erklärte Multiplikation assoziativ wird, ist gar nicht offensichtlich. Man muss dazu etwas rechnen:

$$\begin{aligned} ((a,b) \cdot (a',b')) \cdot (a'',b'') &= (aa' - bb', ab' + ba') \cdot (a'',b'') \\ &= ((aa' - bb')a'' - (ab' + ba')b'', (aa' - bb')b'' + (ab' + ba')a'') \\ &= (aa'a'' - bb'a'' - ab'b'' - ba'b'', aa'b'' - bb'b'' + ab'a'' + ba'a''). \end{aligned}$$

Das gleiche Ergebnis erhält man aus $(a,b) \cdot ((a',b') \cdot (a'',b''))$.

Dass die Multiplikation kommutativ ist, sieht man sofort:

$$(a',b') \cdot (a,b) = (a'a - b'b, a'b + b'a) = (aa' - bb', ab' + ba').$$

Einselement ist $(1,0)$, denn

$$(1,0) \cdot (a,b) = (1 \cdot a - 0 \cdot b, 1 \cdot b + 0 \cdot a) = (a,b) = (a,b) \cdot (1,0).$$

Um die Formel für $(a,b)^{-1}$ zu finden, kann man zunächst etwas informell rechnen:

$$\frac{1}{a + b\mathbf{i}} = \frac{a - b\mathbf{i}}{(a + b\mathbf{i})(a - b\mathbf{i})} = \frac{a - b\mathbf{i}}{a^2 + b^2} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}\mathbf{i}.$$

Dadurch ist die Formel (*) motiviert, und man rechnet korrekt nach, dass

$$(a,b) \cdot \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right) = \left(\frac{a^2 + b^2}{a^2 + b^2}, \frac{-ab + ba}{a^2 + b^2} \right) = (1,0).$$

Zum Nachweis des Distributivgesetzes stellt man fest, dass

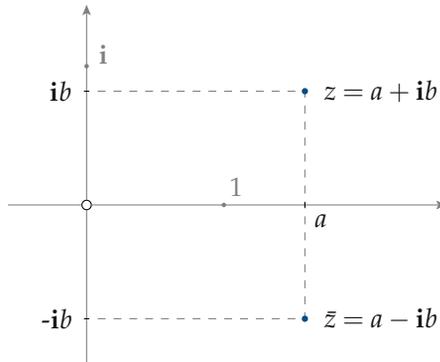
$$\begin{aligned} (a,b) \cdot ((a',b') + (a'',b'')) &= (aa' + aa'' - bb' - bb'', ab' + ab'' + ba' + ba'') \\ &= (a,b) \cdot (a',b') + (a,b) \cdot (a'',b''). \end{aligned}$$

Man beachte, dass bei all diesen Rechnungen die Körperaxiome für reelle Zahlen benutzt wurden. ■

Da die Multiplikation in \mathbb{C} kommutativ ist, gilt $bi = ib$. Also kann man eine komplexe Zahl auch in der Form $z = a + ib$ schreiben. Zum besseren Verständnis und zur Vereinfachung von Rechnungen ist es nützlich, die Multiplikation in der Zahlenebene auch geometrisch zu beschreiben. Dazu erklären wir zunächst für $z = a + bi \in \mathbb{C}$ die Zahlen

$$\begin{aligned} \operatorname{re} z &:= a \in \mathbb{R} && \text{als } \mathbf{Realteil} \text{ von } z, \\ \operatorname{im} z &:= b \in \mathbb{R} && \text{als } \mathbf{Imaginärteil} \text{ von } z \text{ und} \\ \bar{z} &:= a - bi \in \mathbb{C} && \text{als die zu } z \text{ } \mathbf{konjugiert komplexe Zahl}. \end{aligned}$$

Also ist $z = (\operatorname{re} z) \cdot 1 + (\operatorname{im} z) \cdot i = \operatorname{re} z + i \operatorname{im} z$.



Die Abbildung $\mathbb{C} \rightarrow \mathbb{C}$, $z \mapsto \bar{z}$, heißt **komplexe Konjugation**.

Wie man leicht nachrechnet, gelten die folgenden

Rechenregeln Für $z, w \in \mathbb{C}$ gilt:

$$a) \bar{\bar{z}} = z, \quad b) \overline{z + w} = \bar{z} + \bar{w}, \quad c) \overline{z \cdot w} = \bar{z} \cdot \bar{w}.$$

Für $z = a + bi \in \mathbb{C}$ ist $z \cdot \bar{z} = a^2 + b^2 \in \mathbb{R}_+$, also kann man

$$|z| := \sqrt{z \cdot \bar{z}} \in \mathbb{R}_+$$

als **Betrag** (oder **Norm**) von z erklären. Das stimmt überein mit der in 0.3.1 erklärten Norm im Vektorraum \mathbb{R}^2 , denn für

$$z = a + bi \quad \text{ist} \quad |z| = \|(a, b)\| = \sqrt{a^2 + b^2}.$$

Rechenregeln für den Betrag Für alle $z, w \in \mathbb{C}$ gilt:

- $$\begin{aligned} a) \quad & |z| \geq 0 \text{ und } |z| = 0 \Leftrightarrow z = 0, \\ b) \quad & |z + w| \leq |z| + |w|, && \text{(Dreiecksungleichung)} \\ c) \quad & |z \cdot w| = |z| \cdot |w|. && \text{(Law of Moduli)} \end{aligned}$$

Aus Regel c) folgt noch einmal, dass es in \mathbb{C} keine Nullteiler gibt, also

$$z, w \neq 0 \quad \Rightarrow \quad z \cdot w \neq 0.$$

Beweis Die Regeln a) und b) folgen aus den entsprechenden Regeln für die Norm in \mathbb{R}^2 aus 0.3.1 und 0.3.3. Regel c) beweist man einfacher in der quadrierten Form:

$$|z \cdot w|^2 = (z \cdot w) \cdot (\overline{z \cdot w}) = z \cdot w \cdot \bar{z} \cdot \bar{w} = (z \cdot \bar{z}) \cdot (w \cdot \bar{w}) = |z|^2 \cdot |w|^2.$$

■

Vorsicht! Die in 1.3.4 erklärte Anordnung von \mathbb{R} lässt sich nicht auf \mathbb{C} fortsetzen. Genauer gesagt gibt es auf \mathbb{C} gar keine Anordnung, denn

$$1 > 0, \quad \text{also} \quad -1 < 0 \quad \text{und} \quad -1 = i^2.$$

Das widerspricht der Eigenschaft einer Anordnung, dass Quadrate nicht negativ sein können (vgl. 1.3.2).

Für komplexe Zahlen $z, w \in \mathbb{C}$ kann man mit Ungleichungen nur die Beträge vergleichen. Es gilt lediglich

$$|z| \leq |w| \quad \text{oder} \quad |z| \geq |w|.$$

Insbesondere kann man alle $z = a + bi \in \mathbb{C}$ mit

$$|z| = \sqrt{a^2 + b^2} = 1, \quad \text{d.h.} \quad a^2 + b^2 = 1$$

betrachten. Sie entsprechen den Punkten eines Kreises um den Ursprung im \mathbb{R}^2 mit dem Radius 1. Das ist der Schlüssel für die Darstellung komplexer Zahlen in Polarkoordinaten. Dazu verwenden wir aus der Analysis die komplexe *Exponentialreihe*, die gegeben ist durch

$$e^z = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \dots = \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

und für alle $z \in \mathbb{C}$ konvergiert. Für die dadurch erklärte Funktion

$$\exp : \mathbb{C} \rightarrow \mathbb{C}, \quad z \mapsto e^z,$$

gelten die folgenden

Rechenregeln Für alle $z, w \in \mathbb{C}$ gilt:

- 1) $\exp(z + w) = \exp(z) \cdot \exp(w)$
- 2) $\exp(z) \neq 0$
- 3) $\exp \bar{z} = \overline{\exp z}$

Setzt man $z = e^{it}$ mit $t \in \mathbb{R}$, so ist

$$\exp(it) \cdot \overline{\exp(it)} = \exp(it) \cdot \exp(\overline{it}) = \exp(it) \cdot \exp(-it) = \exp(0) = 1.$$

Also folgt $|\exp(it)| = 1$ für alle $t \in \mathbb{R}$. Geometrisch gesehen bedeutet das, dass die reelle Zahlengerade durch

$$\varphi: \mathbb{R} \longrightarrow S = \{z \in \mathbb{C} : |z| = 1\}, \quad t \mapsto \exp(it),$$

auf die Kreislinie $S \subset \mathbb{C}$ abgebildet wird.

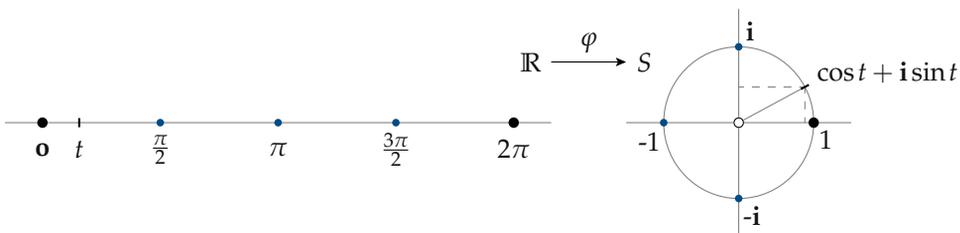
Setzt man in der Exponentialreihe $z = it$ ein und berechnet man die Potenzen von i , so erhält man

$$\begin{aligned} \exp(it) &= \sum_{n=0}^{\infty} \frac{(it)^n}{n!} = 1 + it + \frac{i^2 t^2}{2!} + \frac{i^3 t^3}{3!} + \frac{i^4 t^4}{4!} + \frac{i^5 t^5}{5!} + \dots \\ &= 1 + it - \frac{t^2}{2!} - i \frac{t^3}{3!} + i \frac{t^4}{4!} + i \frac{t^5}{5!} - \dots \\ &= \left(1 - \frac{t^2}{2!} + \frac{t^4}{4!} - \dots\right) + i \left(t - \frac{t^3}{3!} + \frac{t^5}{5!} - \dots\right) \\ &= \sum_{k=0}^{\infty} (-1)^k \frac{t^{2k}}{(2k)!} + i \cdot \left(\sum_{k=0}^{\infty} (-1)^k \frac{t^{2k+1}}{(2k+1)!}\right) \\ &= \cos t + i \cdot \sin t. \end{aligned}$$

Das Ergebnis ist die klassische

Formel von EULER Für alle $t \in \mathbb{R}$ gilt $\exp(it) = \cos t + i \cdot \sin t$.

Verwendet man die in der Analysis bewiesenen Aussagen über den Verlauf der Werte und die Periodizität von Cosinus und Sinus, so erhält man folgendes Bild:



$$\exp(0) = 1, \quad \exp\left(\frac{\pi i}{2}\right) = i, \quad \exp(\pi i) = -1, \quad \exp\left(\frac{3\pi i}{2}\right) = -i, \quad \exp(2\pi i) = 1.$$

Außerdem ist die Abbildung $\varphi: \mathbb{R} \rightarrow S$ periodisch mit der Periode 2π , d.h.

$$\exp(\mathbf{i}(t + 2\pi)) = \exp(\mathbf{i}t) \quad \text{für alle } t \in \mathbb{R},$$

und die Einschränkung $\varphi : [0, 2\pi[\rightarrow S$ ist bijektiv.

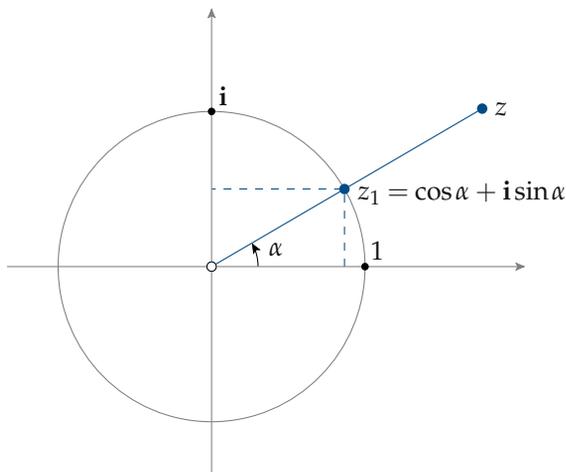
Ist nun $z \in \mathbb{C}$ mit $z \neq 0$ gegeben, so erklärt man dazu

$$z_1 := \frac{1}{|z|} \cdot z; \quad \text{es ist } |z_1| = \frac{1}{|z|} \cdot |z| = 1 \quad \text{und} \quad z = |z| \cdot z_1.$$

Also gibt es genau ein $\alpha \in [0, 2\pi[$ mit $z_1 = \exp(\mathbf{i}\alpha)$. Dieses α nennt man *Argument* von z , in Zeichen

$$\arg z := \alpha, \quad \text{also} \quad z = |z| \cdot \exp(\mathbf{i} \arg z).$$

Die Zahlen $|z| \in \mathbb{R}_+$ und $\alpha \in [0, 2\pi[$ sind die *Polarkoordinaten* von $z \in \mathbb{C}^*$.



Mit Hilfe der Polarkoordinaten erhält man eine schöne geometrische Beschreibung der Multiplikation komplexer Zahlen. Seien $z, w \in \mathbb{C}^*$ und

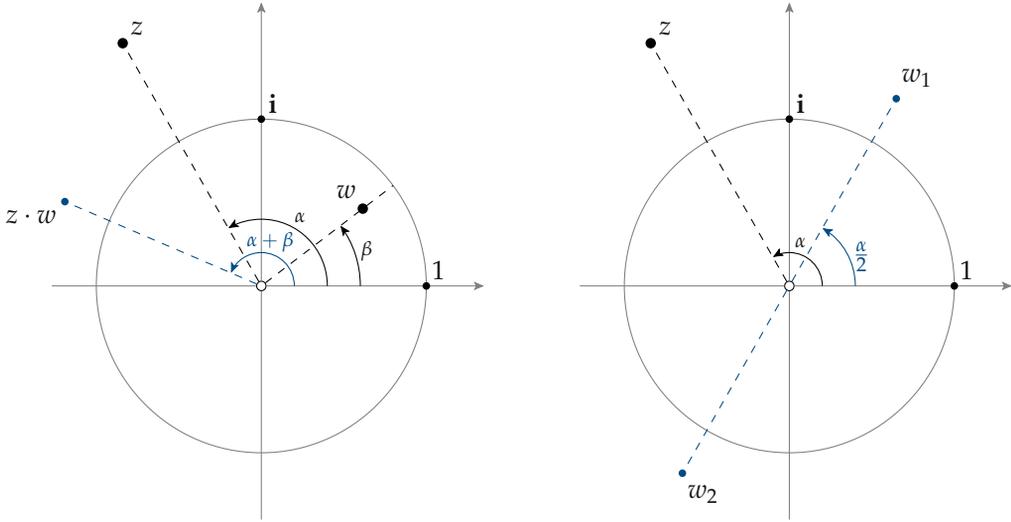
$$z = |z| \cdot \exp(\mathbf{i} \arg z) \quad \text{und} \quad w = |w| \cdot \exp(\mathbf{i} \arg w),$$

folgt

$$z \cdot w = |z| \cdot |w| \cdot \exp(\mathbf{i} \arg z) \cdot \exp(\mathbf{i} \arg w) = |z| \cdot |w| \cdot \exp(\mathbf{i}(\arg z + \arg w)).$$

Bei der Multiplikation komplexer Zahlen werden also die Beträge multipliziert und die Argumente addiert. Bei der Summe der Argumente ist zu bedenken, dass man modulo 2π rechnen muss. Um Quadratwurzeln w_1, w_2 aus einer Zahl $z \in \mathbb{C}^*$ zu ziehen, zieht man die positive Quadratwurzel $\sqrt{|z|}$, dann ist

$$w_1 = \sqrt{|z|} \cdot \exp(\frac{1}{2} \arg z), \quad w_2 = -w_1.$$



Bei der Konstruktion der komplexen Zahlen hat man den Vektorraum \mathbb{R}^2 so zu einem Körper gemacht, dass der Körper \mathbb{R} als Unterkörper darin enthalten ist. Es liegt nahe, zu fragen, ob das auch mit Vektorräumen \mathbb{R}^n für $n \geq 3$ möglich ist. In der Algebra beweist man, dass dies als Folgerung aus dem Fundamentalsatz für \mathbb{C} unmöglich ist. Nach langen Versuchen ist es HAMILTON gelungen, im \mathbb{R}^4 wenigstens eine assoziative, aber nicht kommutative Multiplikation zu finden, und daraus den *Schiefkörper* \mathbb{H} der *Quaternionen* zu machen. Darin ist $\mathbb{C} \subset \mathbb{H}$ als Unterkörper enthalten.

Für $n > 4$ gibt es nur noch im \mathbb{R}^8 eine nicht-assoziative Multiplikation, die eine Erweiterung der Multiplikationen in \mathbb{C} und \mathbb{H} darstellt. Das führt zu den *Oktaven* von CAYLEY. Mehr darüber findet man in [EB, Kap. 9].

1.3.7 Endliche Körper*

Im 19. Jahrhundert hat man beim systematischen Aufbau des Systems von Zahlen die Mengen \mathbb{Q} , \mathbb{R} und \mathbb{C} der rationalen, reellen und komplexen Zahlen als *Zahlkörper* bezeichnet. Im Jahr 1893 wies H. WEBER in einer grundlegenden Arbeit [WEB] darauf hin, dass man auch allgemeinere, etwa *endliche Körper* betrachten kann. Dabei benutzt er den knapp hundert Jahre zuvor von GAUSS eingeführten Begriff der Kongruenz.

Zunächst einmal folgt aus der Definition eines Körpers, dass er mindestens zwei verschiedene Elemente 0 und 1 enthalten muss, das sind die neutralen Elemente der Addition und Multiplikation. Als Verknüpfungstafeln für die Menge $\mathbb{F}_2 := \{0, 1\}$ kommen nach den Axiomen nur

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	1	1

in Frage. Die verschiedenen Regeln prüft man leicht nach, \mathbb{F}_2 ist ein Körper mit zwei Elementen. Er ist eine mathematische Grundlage für alle elektronischen Rechner.

Merkwürdig erscheint nur die Regel $1 + 1 = 0$, wobei 0 und 1 nicht die natürlichen Zahlen, sondern die Elemente von \mathbb{F}_2 bezeichnen. Diese und auch die anderen Einträge der Tafeln werden ganz plausibel, wenn man folgenden Zusammenhang mit den ganzen Zahlen betrachtet:

0 steht für „gerade“, 1 steht für „ungerade“.

Dann hat man die bekannten Regeln

gerade + gerade = ungerade + ungerade = gerade,
gerade + ungerade = ungerade,

gerade · gerade = gerade · ungerade = gerade,
ungerade · ungerade = ungerade.

An diesem Zusammenhang erkennt man auch, wie die Konstruktion von \mathbb{F}_2 verallgemeinert werden kann, denn für $x \in \mathbb{Z}$ gilt

$$x \text{ gerade} \Leftrightarrow x \equiv 0 \pmod{2}, \quad x \text{ ungerade} \Leftrightarrow x \equiv 1 \pmod{2}.$$

Für einen beliebigen Modul $m \in \mathbb{N}$ kann man nun die schon in 1.1.5 eingeführten Restklassen $x + m\mathbb{Z} \subset \mathbb{Z}$ und die kanonische Abbildung

$$\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}, \quad x \mapsto x + m\mathbb{Z},$$

betrachten. Dabei gilt

$$x + m\mathbb{Z} = x' + m\mathbb{Z} \Leftrightarrow x' - x \in m\mathbb{Z} \Leftrightarrow x \equiv x' \pmod{m}.$$

Für $m = 0$ ist $\mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$. Für $m \geq 1$ hat man eine Darstellung durch spezielle Repräsentanten, nämlich

$$\mathbb{Z}/m\mathbb{Z} = \{0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \dots, (m-1) + m\mathbb{Z}\}.$$

Nun kann man in $\mathbb{Z}/m\mathbb{Z}$ eine Addition und Multiplikation erklären. Naheliegend ist der Versuch

$$(k + m\mathbb{Z}) + (l + m\mathbb{Z}) := (k + l) + m\mathbb{Z} \quad \text{und} \\ (k + m\mathbb{Z}) \cdot (l + m\mathbb{Z}) := (k \cdot l) + m\mathbb{Z}.$$

Es bleibt zu zeigen, dass diese Definitionen unabhängig sind von der Auswahl der Repräsentanten k und l . Dazu benutzt man die folgenden Rechenregeln für Kongruenzen:

$$k \equiv k' \pmod{m} \quad \text{und} \quad l \equiv l' \pmod{m} \Rightarrow \begin{cases} k + l \equiv (k' + l') \pmod{m}, & (+) \\ k \cdot l \equiv (k' \cdot l') \pmod{m}. & (\cdot) \end{cases}$$

Der Nachweis von (+) ist ganz klar:

$$(k' + l') - (k + l) = (k' - k) + (l' - l) \in m\mathbb{Z}.$$

Für (·) verwendet man, dass

$$k' \cdot l' - k \cdot l = (k' - k) \cdot l' + k(l' - l) \in m\mathbb{Z}.$$

Ergebnis dieser Konstruktion ist der

Satz Für jedes $m \in \mathbb{N}$ ist die Menge $\mathbb{Z}/m\mathbb{Z}$ der Restklassen von \mathbb{Z} modulo m mit der oben erklärten Addition und Multiplikation ein kommutativer Ring. Für $m = 0$ ist $\mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$, für $m = 1$ ist $\mathbb{Z}/1\mathbb{Z} = \{0\}$ und für $m \geq 2$ besteht $\mathbb{Z}/m\mathbb{Z}$ aus m Elementen; es gibt ein Einselement $1 + m\mathbb{Z} \neq 0 + m\mathbb{Z}$.

Man nennt $\mathbb{Z}/m\mathbb{Z}$ („ \mathbb{Z} modulo $m\mathbb{Z}$ “) den **Restklassenring** von \mathbb{Z} modulo m .

Beweis Die Assoziativität und Kommutativität von Addition und Multiplikation sowie die Distributivität folgen ganz einfach aus den entsprechenden Regeln in \mathbb{Z} ; man kann sagen, sie werden von \mathbb{Z} auf $\mathbb{Z}/m\mathbb{Z}$ vererbt.

Nullelement ist $0 + m\mathbb{Z}$, das Negative von $k + m\mathbb{Z}$ ist $(-k) + m\mathbb{Z}$. Neutrales Element der Multiplikation ist $1 + m\mathbb{Z}$. ■

Nun stellt sich die Frage, wann der Ring $\mathbb{Z}/m\mathbb{Z}$ ein Körper ist. Dazu betrachten wir zunächst als Beispiel die Multiplikation in $\mathbb{Z}/m\mathbb{Z}$ für $m = 2, 3, 4, 5$, wobei jeweils $\bar{k} := k + m\mathbb{Z}$ gesetzt ist:

$m = 2$	$m = 3$	$m = 4$	$m = 5$																																																																																																								
<table style="border-collapse: collapse; margin: auto;"> <tr><td style="padding: 2px 5px;">·</td><td style="padding: 2px 5px;"> </td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{1}$</td></tr> <tr><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;"> </td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{0}$</td></tr> <tr><td style="padding: 2px 5px;">$\bar{1}$</td><td style="padding: 2px 5px;"> </td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{1}$</td></tr> </table>	·		$\bar{0}$	$\bar{1}$	$\bar{0}$		$\bar{0}$	$\bar{0}$	$\bar{1}$		$\bar{0}$	$\bar{1}$	<table style="border-collapse: collapse; margin: auto;"> <tr><td style="padding: 2px 5px;">·</td><td style="padding: 2px 5px;"> </td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{1}$</td><td style="padding: 2px 5px;">$\bar{2}$</td></tr> <tr><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;"> </td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{0}$</td></tr> <tr><td style="padding: 2px 5px;">$\bar{1}$</td><td style="padding: 2px 5px;"> </td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{1}$</td><td style="padding: 2px 5px;">$\bar{2}$</td></tr> <tr><td style="padding: 2px 5px;">$\bar{2}$</td><td style="padding: 2px 5px;"> </td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{2}$</td><td style="padding: 2px 5px;">$\bar{1}$</td></tr> </table>	·		$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{0}$		$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{1}$		$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{2}$		$\bar{0}$	$\bar{2}$	$\bar{1}$	<table style="border-collapse: collapse; margin: auto;"> <tr><td style="padding: 2px 5px;">·</td><td style="padding: 2px 5px;"> </td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{1}$</td><td style="padding: 2px 5px;">$\bar{2}$</td><td style="padding: 2px 5px;">$\bar{3}$</td></tr> <tr><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;"> </td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{0}$</td></tr> <tr><td style="padding: 2px 5px;">$\bar{1}$</td><td style="padding: 2px 5px;"> </td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{1}$</td><td style="padding: 2px 5px;">$\bar{2}$</td><td style="padding: 2px 5px;">$\bar{3}$</td></tr> <tr><td style="padding: 2px 5px;">$\bar{2}$</td><td style="padding: 2px 5px;"> </td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{2}$</td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{2}$</td></tr> <tr><td style="padding: 2px 5px;">$\bar{3}$</td><td style="padding: 2px 5px;"> </td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{3}$</td><td style="padding: 2px 5px;">$\bar{2}$</td><td style="padding: 2px 5px;">$\bar{1}$</td></tr> </table>	·		$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$		$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{1}$		$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{2}$		$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{3}$		$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$	<table style="border-collapse: collapse; margin: auto;"> <tr><td style="padding: 2px 5px;">·</td><td style="padding: 2px 5px;"> </td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{1}$</td><td style="padding: 2px 5px;">$\bar{2}$</td><td style="padding: 2px 5px;">$\bar{3}$</td><td style="padding: 2px 5px;">$\bar{4}$</td></tr> <tr><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;"> </td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{0}$</td></tr> <tr><td style="padding: 2px 5px;">$\bar{1}$</td><td style="padding: 2px 5px;"> </td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{1}$</td><td style="padding: 2px 5px;">$\bar{2}$</td><td style="padding: 2px 5px;">$\bar{3}$</td><td style="padding: 2px 5px;">$\bar{4}$</td></tr> <tr><td style="padding: 2px 5px;">$\bar{2}$</td><td style="padding: 2px 5px;"> </td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{2}$</td><td style="padding: 2px 5px;">$\bar{4}$</td><td style="padding: 2px 5px;">$\bar{1}$</td><td style="padding: 2px 5px;">$\bar{3}$</td></tr> <tr><td style="padding: 2px 5px;">$\bar{3}$</td><td style="padding: 2px 5px;"> </td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{3}$</td><td style="padding: 2px 5px;">$\bar{1}$</td><td style="padding: 2px 5px;">$\bar{4}$</td><td style="padding: 2px 5px;">$\bar{2}$</td></tr> <tr><td style="padding: 2px 5px;">$\bar{4}$</td><td style="padding: 2px 5px;"> </td><td style="padding: 2px 5px;">$\bar{0}$</td><td style="padding: 2px 5px;">$\bar{4}$</td><td style="padding: 2px 5px;">$\bar{3}$</td><td style="padding: 2px 5px;">$\bar{2}$</td><td style="padding: 2px 5px;">$\bar{1}$</td></tr> </table>	·		$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$		$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{1}$		$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{2}$		$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$	$\bar{3}$		$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$	$\bar{4}$		$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
·		$\bar{0}$	$\bar{1}$																																																																																																								
$\bar{0}$		$\bar{0}$	$\bar{0}$																																																																																																								
$\bar{1}$		$\bar{0}$	$\bar{1}$																																																																																																								
·		$\bar{0}$	$\bar{1}$	$\bar{2}$																																																																																																							
$\bar{0}$		$\bar{0}$	$\bar{0}$	$\bar{0}$																																																																																																							
$\bar{1}$		$\bar{0}$	$\bar{1}$	$\bar{2}$																																																																																																							
$\bar{2}$		$\bar{0}$	$\bar{2}$	$\bar{1}$																																																																																																							
·		$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$																																																																																																						
$\bar{0}$		$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$																																																																																																						
$\bar{1}$		$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$																																																																																																						
$\bar{2}$		$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$																																																																																																						
$\bar{3}$		$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$																																																																																																						
·		$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$																																																																																																					
$\bar{0}$		$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$																																																																																																					
$\bar{1}$		$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$																																																																																																					
$\bar{2}$		$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$																																																																																																					
$\bar{3}$		$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$																																																																																																					
$\bar{4}$		$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$																																																																																																					

An den vier Multiplikationstabellen erkennt man einen deutlichen Unterschied:

Für $m = 2, 3, 5$ kann man die Multiplikation von $\mathbb{Z}/m\mathbb{Z}$ auf

$$(\mathbb{Z}/m\mathbb{Z})^* = (\mathbb{Z}/m\mathbb{Z}) \setminus \{0 + m\mathbb{Z}\}$$

einschränken. Für $m = 4$ geht das nicht, insbesondere weil in dem gestrichelt abgetrennten Teil $\bar{0}$ vorkommt; es gibt also den Nullteiler $\bar{2}$ mit $\bar{2} \cdot \bar{2} = \bar{0}$.

Bei einem allgemeinen Modul m betrachten wir die von Null verschiedenen Elemente $(\mathbb{Z}/m\mathbb{Z})^*$. Es gilt $k + m\mathbb{Z} \neq 0 + m\mathbb{Z}$ genau dann, wenn $k \notin m\mathbb{Z}$, d.h. m ist kein Teiler von k . Die Bedingung dafür, dass $(\mathbb{Z}/m\mathbb{Z})^*$ unter der Multiplikation abgeschlossen ist, bedeutet dann

$$k + m\mathbb{Z}, l + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^* \Rightarrow (k \cdot l) + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^*.$$

Das ist gleichwertig mit

$$m \text{ teilt } k \cdot l \Rightarrow m \text{ teilt } k \text{ oder } m \text{ teilt } l.$$

Nach einem Satz von EUKLID aus der elementaren Zahlentheorie (vgl. etwa [FI₃, II 3.4]) ist diese Eigenschaft charakteristisch dafür, dass der Modul m eine Primzahl ist. Das ist der Schlüssel zu folgendem

Korollar *Der Restklassenring $\mathbb{Z}/m\mathbb{Z}$ ist genau dann ein Körper, wenn m eine Primzahl ist.*

Ist p eine Primzahl, so nennt man

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$$

den *Primkörper* der *Charakteristik* p .

Beweis Ist m keine Primzahl, also $m = k \cdot l$ mit $k, l \in \mathbb{N}$, $1 < k, l < m$, so folgt

$$(k + m\mathbb{Z}) \cdot (l + m\mathbb{Z}) = m + m\mathbb{Z} = 0 + m\mathbb{Z},$$

also hat $\mathbb{Z}/m\mathbb{Z}$ Nullteiler.

Ist $m = p$ eine Primzahl, so ist zu zeigen, dass $(\mathbb{Z}/p\mathbb{Z})^*$ mit der Multiplikation eine Gruppe ist. Wie wir schon oben gezeigt haben, ist $(\mathbb{Z}/p\mathbb{Z})^*$ unter der Multiplikation abgeschlossen. Wie im Abschnitt 1.2.3 ausgeführt, bleibt zu zeigen, dass für jedes $\bar{k} = k + p\mathbb{Z}$ mit $k \notin p\mathbb{Z}$ die Linkstranslation

$$l_{\bar{k}}: (\mathbb{Z}/p\mathbb{Z})^* \rightarrow (\mathbb{Z}/p\mathbb{Z})^*, \quad x + p\mathbb{Z} \mapsto (k \cdot x) + p\mathbb{Z}$$

bijektiv ist. Da $(\mathbb{Z}/p\mathbb{Z})^*$ endlich ist, genügt es nach dem „Apfellemma“ aus 1.1.3 zu zeigen, dass $l_{\bar{k}}$ injektiv ist. Sei also

$$(k \cdot x) + p\mathbb{Z} = (k \cdot y) + p\mathbb{Z} \quad \text{für } k, x, y \in \mathbb{Z} \setminus p\mathbb{Z}.$$

Es folgt $k \cdot x - k \cdot y = k(x - y) \in p\mathbb{Z}$. Da p Primzahl, und p kein Teiler von k ist, muss p ein Teiler von $x - y$ sein. Also folgt

$$x + p\mathbb{Z} = y + p\mathbb{Z},$$

somit ist $l_{\bar{k}}$ injektiv. ■

In den Körpern der rationalen, reellen und komplexen Zahlen sind die natürlichen Zahlen als Teilmenge enthalten. In einem endlichen Körper K ist das unmöglich, denn \mathbb{N} ist unendlich. Daher ist es angebracht, in K die Summen

$$n \cdot 1 := \underbrace{1 + \dots + 1}_{n\text{-mal}} \in K \quad \text{mit } n \in \mathbb{N} \quad \text{und } 1 \in K$$

zu betrachten. In dem oben betrachteten Primkörper \mathbb{F}_p ist offensichtlich

$$p \cdot 1 = 0 \quad \text{und} \quad n \cdot 1 \neq 0 \quad \text{für } n = 1, \dots, p-1.$$

Auf der Suche nach endlichen Körpern, die von den Primkörpern verschieden sind, erklärt man zunächst für einen beliebigen Körper K die Charakteristik.

$$\text{char}(K) := \begin{cases} 0 & \text{falls } n \cdot 1 \neq 0 \text{ für alle } n \in \mathbb{N}^*, \\ \min\{n \in \mathbb{N}^* : n \cdot 1 = 0\} & \text{sonst.} \end{cases}$$

Im Fall $\text{char}(K) \neq 0$ spricht man auch von positiver Charakteristik.

Bemerkung 1 *Ist die Charakteristik eines Körpers positiv, so ist sie eine Primzahl.*

Beweis Nach dem Distributivgesetz in K gilt für $m, n \in \mathbb{N}$ und $1 \in K$

$$(m \cdot 1) \cdot (n \cdot 1) = \underbrace{(1 + \dots + 1)}_{m\text{-mal}} \cdot \underbrace{(1 + \dots + 1)}_{n\text{-mal}} = \underbrace{(1 + \dots + 1)}_{m \cdot n\text{-mal}} = (m \cdot n) \cdot 1.$$

Angenommen, $k = \text{char}(K) > 0$ sei nicht prim. Dann gibt es $m, n \in \mathbb{N}$ mit $2 \leq m, n \leq k-1$, so dass $k = m \cdot n$, also

$$0 = k \cdot 1 = (m \cdot n) \cdot 1 = (m \cdot 1) \cdot (n \cdot 1).$$

Da K keine Nullteiler besitzt, muss $m \cdot 1 = 0$ oder $n \cdot 1 = 0$ sein, im Widerspruch zur Minimalität von k . ■

Bemerkung 2 *Ist K ein Körper mit $\text{char}(K) = p > 0$, so ist die Teilmenge*

$$K' := \{0, 1, 2 \cdot 1, \dots, (p-1) \cdot 1\} \subset K$$

ein zum Primkörper \mathbb{F}_p isomorpher Unterkörper.

Beweis Die Abbildung

$$\chi: \mathbb{Z} \rightarrow K, \quad n \mapsto n \cdot 1,$$

ist ein Homomorphismus von Ringen mit $\text{Ker}(\chi) = p \cdot \mathbb{Z}$. Daher ist die Abbildung

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \rightarrow K', \quad k + p\mathbb{Z} \mapsto k \cdot 1, \quad \text{wobei } 1 \in K,$$

ein Isomorphismus. ■

Bemerkung 3 *In einem Körper der Charakteristik $p > 0$ gibt es keine Anordnung.*

Beweis Es genügt zu zeigen, dass der Primkörper \mathbb{F}_p nicht im Sinn der Definition von 1.3.2 angeordnet werden kann. Da $1 \in \mathbb{F}_p$ positiv sein muss, müsste auch jede Summe aus $k \cdot 1 = 1 + \dots + 1$ positiv sein; es ist aber $p \cdot 1 = 0$. ■

Mit etwas mehr algebraischen Hilfsmitteln kann man beweisen, dass die Anzahl der Elemente eines endlichen Körpers K mit $\text{char}(K) = p > 0$ gleich p^n mit einem $n \in \mathbb{N}^*$ ist, und dass es zu jeder Zahl $q = p^n$ bis auf Isomorphie genau einen Körper \mathbb{F}_q mit q Elementen gibt, dabei ist $\text{char}(\mathbb{F}_q) = p$.

Im ganz einfachen Fall $q = 2^2 = 4$ kann man das sehr elementar beschreiben. In der additiven Gruppe $(\mathbb{F}_4, +)$ muss $1 + 1 = 0$ gelten. Es gibt nur zwei wesentlich verschiedene Gruppen der Ordnung 4, die KLEINSche Vierergruppe - additiv geschrieben - passt. Die multiplikative Gruppe (\mathbb{F}_4^*, \cdot) hat drei Elemente, da gibt es nur eine Möglichkeit. Das ergibt für $\mathbb{F}_4 = \{0, 1, a, b\}$ die beiden folgenden Tabellen

+	0	1	a	b		·	0	1	a	b		\mathbb{F}_4
0	0	1	a	b		0	0	0	0	0		
1	1	0	b	a		1	0	1	a	b		
a	a	b	0	1		a	0	a	b	1		
b	b	a	1	0		b	0	b	1	a		

Die Regeln für Addition und Multiplikation für sich genommen sind erfüllt, weil bekannte Gruppen in die Tafeln eingesetzt wurden. Keineswegs selbstverständlich ist, dass auch das Distributivgesetz gilt. Dazu muss man im Prinzip alle möglichen Kombinationen einsetzen. Wir begnügen uns mit zwei davon

$$\begin{aligned} a \cdot (b + 1) &= a \cdot a = b, & a \cdot b + a \cdot 1 &= 1 + a = b, \\ a \cdot (a + b) &= a \cdot 1 = a, & a \cdot a + a \cdot b &= b + 1 = a. \end{aligned}$$

Also ist \mathbb{F}_4 mit den oben angegebenen Verknüpfungen ein Körper. Wie man sieht, ist $\mathbb{F}_2 = \{0, 1\}$ ein Unterkörper.

Vorsicht! Der gerade konstruierte Körper \mathbb{F}_4 ist zu unterscheiden vom Restklassenring $\mathbb{Z}/4\mathbb{Z}$. Zum Kontrast schreiben wir die Tafeln für Multiplikation und Addition, die wir zur Unterscheidung mit \oplus und \odot bezeichnen, noch einmal auf. Um den Unterschied zu \mathbb{F}_4 deutlich zu machen, setzen wir

$$0 = 0 + 4\mathbb{Z}, \quad 1 = 1 + 4\mathbb{Z}, \quad a = 2 + 4\mathbb{Z} \quad \text{und} \quad b = 3 + 4\mathbb{Z}.$$

\oplus	0	1	a	b
0	0	1	a	b
1	1	a	b	0
a	a	b	0	1
b	b	0	1	a

\odot	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	0	a
b	0	b	a	1

 $\mathbb{Z}/4\mathbb{Z}$

Daran sieht man, dass die Tafeln von \mathbb{F}_4 und $\mathbb{Z}/4\mathbb{Z}$ sowohl für Addition als auch für Multiplikation verschieden sind! Man könnte auch daran denken, die Multiplikation \cdot aus \mathbb{F}_4 mit der Addition \oplus aus $\mathbb{Z}/4\mathbb{Z}$ zu koppeln. Aber wie man sich leicht überzeugt, ist in dieser Kombination das Distributivgesetz verletzt. Schließlich sei noch erwähnt, dass es auch unendliche Körper mit positiver Charakteristik gibt.

1.3.8 Rückblick und Ausblick

In den vorausgehenden Abschnitten dieses Kapitels haben wir versucht, das Fundament des Gebäudes der Mathematik bestehend aus strukturierten Mengen von Zahlen einigermaßen systematisch zu beschreiben. Wie schon an mehreren Stellen bemerkt, entspricht dieser Aufbau ganz und gar nicht der historischen Entwicklung, die wir deshalb noch einmal kurz skizzieren wollen.

In den Büchern von EUKLID (um 300 v. Chr.) steht die Geometrie im Vordergrund, dabei sind Zahlen ein unentbehrliches Hilfsmittel. Den kommensurablen Größen entsprechen die rationalen Zahlen, die unvermeidlich auftretenden inkommensurablen Größen führen zu irrationalen Zahlen. Die dabei verwendeten Zahlen dienten vor allem der Messung geometrischer Größen. Das mag ein Grund dafür sein, dass negative Zahlen im Gegensatz zu rationalen Zahlen erst viel später (um 600 n. Chr.) verwendet wurden, obwohl formal Differenzen und Brüche durch ganz analoge Konstruktionen entstehen. Das mag auch an dem Missverständnis liegen, der Begriff „negativ“ sei als Wertung zu verstehen. Sogar KANT hat das 1763 zu einem Versuch bewogen, die Bedenken der Philosophen zu zerstreuen [KA].

Während der um 1700 beginnenden stürmischen Entwicklung der Infinitesimalrechnung blieben Fragen um die Struktur der reellen Zahlen als lückenlose Zahlengerade im Hintergrund. Auf den reellen Zahlen wurden komplexe Zahlen und in der Mitte des 19. Jahrhunderts Quaternionen und Oktaven aufgebaut. Ein Markstein auf dem Weg zur Festigung der Grundlagen waren die Erfahrungen von DEDEKIND bei einer Vorlesung am eidgenössischen Polytechnikum in Zürich aus dem Jahr 1858. Seine Überlegungen zur Charakterisierung reeller Zahlen wurden 1872 veröffentlicht [DED₁]. Daran anschließend ging er noch tiefer an das Fundament der Theorie der Zahlen. In seiner 1887 veröffentlichten Schrift ([DED₂]) führte er Mengen (unter dem Namen „Systeme“) und Abbildungen ein, damit charakterisierte er die natürlichen Zahlen und die algebraischen Operationen. Anschließend formulierte PEANO [PE₃] die Axiome der natürlichen Zahlen in streng formalisierter Weise und CANTOR baute die Mengenlehre weiter aus.

Im Jahr 1900 fand in Paris der 2. Internationale Mathematikerkongress statt. In seinem Vortrag formulierte D. HILBERT [HI₃] die Probleme, nicht nur die Mathematik, sondern auch die Physik auf unabhängige und widerspruchsfreie Axiome zu gründen. Das ist nicht so umfassend geglückt, wie es HILBERT erhofft hatte, aber seine Aufforderung hat die Mathematik des 20. Jahrhunderts geprägt. In der Nachfolge der Göttinger Schule verfasste eine stetig wechselnde Gruppe französischer Mathematiker unter dem Pseudonym NICOLAS BOURBAKI ab 1939 eine lange Serie von Büchern „*Eléments de mathématique*“, in der begonnen wurde, die Mathematik dem Programm von HILBERT entsprechend streng axiomatisch aufzubauen. Das erfordert einen Weg, der mit den allgemeinsten Strukturen beginnt und schrittweise zu spezielleren Strukturen fortschreitet. Dieses Vorgehen ist nicht unproblematisch. Ein bleibender Gewinn ist, dass verschiedene Teile der Mathematik dadurch eine ziemlich einheitliche Sprache gefunden haben. Aber eine Gefahr besteht darin, dass man beim Lehren und Lernen von Mathematik oft einen zu langen und umständlichen Weg gehen muss, und dass dabei die relevanten Anwendungen der Mathematik zu kurz kommen.

Als Fazit kann man festhalten, dass der systematische Aufbau der Mathematik keinesfalls der historischen Entwicklung entspricht. Das sollte man bei der Vermittlung der Mathematik bedenken. Es gibt wohl kein Patentrezept, aber eine gute Mischung von anschaulichem Zugang und strenger Methode scheint hilfreich zu sein. In der Schule sollte dabei die Anschauung im Vordergrund stehen, „beweisen“ sollte dabei „zeigen“ bedeuten. Aber ein zukünftiger Lehrer muss in seinem Studium auch die harten Methoden der Beweistechnik kennengelernt haben.

1.4 Polynome*

1.4.1 Polynome und Polynomfunktionen

In der linearen Algebra beschäftigt man sich in erster Linie mit linearen Funktionen von der Art

$$f: \mathbb{R}^n \rightarrow \mathbb{R}, \quad x = (x_1, \dots, x_n) \mapsto f(x) = a_1x_1 + \dots + a_nx_n.$$

„Linear“ bedeutet dabei, dass die x_i in $f(x)$ nur mit der ersten Potenz vorkommen. Im Fall $n = 1$ kann man auch allgemeinere Funktionen

$$f: \mathbb{R} \rightarrow \mathbb{R}, \quad x \mapsto f(x) = a_0 + a_1x + \dots + a_nx^n, \quad \text{mit } a_0, \dots, a_n \in \mathbb{R},$$

betrachten, wobei x in $f(x)$ mit endlich vielen beliebigen Potenzen auftreten kann. Solche „Polynome“ treten auch in der linearen Algebra auf, etwa bei der Suche nach Eigenwerten im Kapitel 4. Zur Vorbereitung darauf stellen wir hier schon das Wichtigste zusammen.

Wir starten mit einem beliebigen Körper K . Ein *Polynom* mit *Koeffizienten* aus (oder kürzer Polynom über) K ist ein formaler Ausdruck der Form

$$f = a_0 + a_1X + \dots + a_nX^n,$$

wobei $n \in \mathbb{N}$ und $a_0, \dots, a_n \in K$. Das Symbol X ist eine sogenannte *Unbestimmte*, für die man beliebige Elemente aus K (und eventuell noch allgemeinere Größen) einsetzen kann. Mit $K[X]$ bezeichnen wir die Menge aller Polynome über K . Das *Nullpolynom* $\mathbf{o} \in K[X]$ hat nur die Koeffizienten 0. Für die Unbestimmte X kann man beliebige Elemente $x \in K$ einsetzen. Auf diese Weise erhält man eine Abbildung

$$K[X] \rightarrow \text{Abb}(K, K), \quad f \mapsto \tilde{f}, \quad \text{wobei}$$

$$\tilde{f}(x) := a_0 + a_1x + \dots + a_nx^n, \quad \text{wenn } f = a_0 + a_1X + \dots + a_nX^n.$$

Man nennt \tilde{f} die zu f gehörige *Polynomfunktion*. Diese pedantisch erscheinende Unterscheidung zwischen f und \tilde{f} ist leider nicht überflüssig.

Beispiel Sei $K = \mathbb{F}_2 = \{0, 1\}$ und $f = X^2 + X$. Dann ist

$$\tilde{f}(0) = 0 + 0 = 0 \quad \text{und} \quad \tilde{f}(1) = 1 + 1 = 0,$$

also ist \tilde{f} die Nullabbildung, aber $f \neq \mathbf{o}$. Somit ist die Abbildung $K[X] \rightarrow \text{Abb}(K, K)$ nicht injektiv. Wir werden später in 1.4.4 sehen, dass es derartige Beispiele in jedem endlichen Körper gibt, nicht aber in unendlichen Körpern.

Für ein Polynom $f = a_0 + a_1X + \dots + a_nX^n$ erklärt man den *Grad* als

$$\deg f := \begin{cases} -\infty, & \text{falls } f = \mathbf{o}, \\ \max\{i : a_i \neq 0\} & \text{sonst.} \end{cases}$$

Dass man dem Nullpolynom den formalen Grad $-\infty$ zuordnet, ist motiviert durch die anschließend aufzustellenden Rechenregeln für den Grad. Ein Polynom f mit $\deg f \leq 0$ ist ein **konstantes Polynom** $f = a_0$. Schließlich nennt man ein Polynom f vom Grad n **normiert**, wenn $a_n = 1$, d.h.

$$f = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0.$$

1.4.2 Der Ring der Polynome

Zwei Polynomfunktionen kann man addieren und multiplizieren, indem man ihre Werte addiert und multipliziert. Ist etwa

$$\tilde{f}(x) = a_0 + a_1x \quad \text{und} \quad \tilde{g}(x) = b_0 + b_1x, \quad \text{so folgt}$$

$$\tilde{f}(x) + \tilde{g}(x) = (a_0 + b_0) + (a_1 + b_1)x \quad \text{und}$$

$$\tilde{f}(x) \cdot \tilde{g}(x) = a_0 \cdot b_0 + (a_0b_1 + a_1b_0)x + (a_1 \cdot b_1)x^2.$$

Allgemein betrachten wir formale Polynome $f, g \in K[X]$, wobei

$$f = a_0 + a_1X + \dots + a_nX^n \quad \text{und} \quad g = b_0 + b_1X + \dots + b_mX^m.$$

Für die Addition von f und g können wir $m = n$ voraussetzen, denn man kann immer höhere Koeffizienten Null hinzufügen. Dann ist

$$f + g := (a_0 + b_0) + (a_1 + b_1)X + \dots + (a_n + b_n)X^n.$$

Die Regel für die Multiplikation ist komplizierter. Durch formales Ausmultiplizieren erhält man

$$f \cdot g := c_0 + c_1X + \dots + c_{n+m}X^{n+m}, \quad \text{wobei} \quad c_k := \sum_{i+j=k} a_i b_j.$$

Etwas expliziter aufgeschrieben ist

$$\begin{aligned} c_0 &= a_0 b_0, \\ c_1 &= a_0 b_1 + a_1 b_0, \\ c_2 &= a_0 b_2 + a_1 b_1 + a_2 b_0, \\ &\vdots \\ c_{n+m} &= a_n b_m. \end{aligned}$$

Für die Grade der beteiligten Polynome hat man folgende

Bemerkung Sind $f, g \in K[X]$, so gilt

$$\deg(f + g) \leq \max\{\deg f, \deg g\} \quad \text{und} \quad \deg(f \cdot g) = \deg f + \deg g.$$

Dabei benutzt man die formalen Rechenregeln

$$n + (-\infty) = -\infty + m = -\infty + (-\infty) = -\infty.$$

Beweis Die erste Regel folgt sofort aus der Definition von $f + g$.

Ist $\deg f = n \geq 0$ und $\deg g = m \geq 0$, so folgt $a_n \neq 0$ und $b_m \neq 0$. Der höchste Koeffizient von $f \cdot g$ ist $c_{n+m} = a_n \cdot b_m \neq 0$. Ist $f = \mathbf{o}$ oder $g = \mathbf{o}$, so ist $f \cdot g = \mathbf{o}$, also $\deg(f \cdot g) = -\infty$. Daher gilt die zweite Regel auch in diesem Fall. ■

Satz Die Menge $K[X]$ der Polynome über einem Körper K zusammen mit der oben erklärten Addition und Multiplikation ist ein kommutativer Ring mit Einselement; er hat keine Nullteiler.

Beweis Der Nachweis der Ring-Axiome ist reine Routinearbeit. Einselement ist das konstante Polynom von 1.

Sind $f, g \in K[X]$ beide von \mathbf{o} verschieden, so ist $\deg f \geq 0$ und $\deg g \geq 0$, also nach der obigen Bemerkung auch $\deg(f \cdot g) \geq 0$ und somit $f \cdot g \neq \mathbf{o}$. ■

Korollar Im Polynomring gilt für $f, g, h \in K[X]$ mit $\deg f, \deg g$ und $\deg h \geq 0$ die Kürzungsregel

$$f \cdot g = f \cdot h \quad \Rightarrow \quad g = h.$$

Beweis Aus $f \cdot (g - h) = \mathbf{o}$ folgt $g - h = \mathbf{o}$, also $g = h$ wegen $f \neq \mathbf{o}$. ■

Vorsicht! Ein Polynom ist formal nichts anderes als eine Folge

$$f : \mathbb{N} \rightarrow K, \quad i \mapsto a_i,$$

mit der Eigenschaft, dass es ein $n \in \mathbb{N}$ gibt, so dass $a_i = 0$ für $i > n$. Der Faktor X^i in $a_i X^i$ dient dabei nur zur Markierung der Stelle, an der der Koeffizient a_i steht. In der Menge aller Folgen mit Werten in K ist neben der üblichen Addition auch eine andere Multiplikation oft üblich (vgl. 1.3.4):

$$f * g = (a_i) * (b_i) := (a_i \cdot b_i).$$

Auch damit wird die Menge dieser Folgen zu einem kommutativen Ring mit Einselement; allerdings wimmelt es da von Nullteilern. Außerdem ist die Multiplikation $*$ nicht verträglich mit der Multiplikation von Polynomen als Abbildungen.

1.4.3 Division mit Rest

Wie im Ring \mathbb{Z} der ganzen Zahlen kann man in einem Polynomring $K[X]$ nur sehr eingeschränkt dividieren. Ein Ersatz ist in beiden Ringen eine Division mit Rest, wobei nur die „Größe“ des Restes etwas unterschiedlich gemessen wird (vgl. dazu 1.3.1).

Satz Sei K ein Körper und seien $f, g \in K[X]$ mit $g \neq \mathbf{0}$. Dazu gibt es eindeutig bestimmte Polynome $q, r \in K[X]$ derart, dass

$$f = q \cdot g + r \quad \text{und} \quad \deg r < \deg g. \quad (*)$$

Dabei bedeutet q einen „Quotienten“, r einen „Rest“. Wie beim Übergang von \mathbb{Z} nach \mathbb{Q} kann man auch formale Quotienten von Polynomen betrachten, dann lässt sich die Beziehung $(*)$ in der etwas suggestiveren Form

$$\frac{f}{g} = q + \frac{r}{g}$$

schreiben.

Beweis Wir zeigen zunächst die Eindeutigkeit. Ist

$$f = q \cdot g + r = q' \cdot g + r' \quad \text{mit} \quad \deg r, \deg r' < \deg g,$$

so folgt $(q - q')g = r' - r$. Ist $q = q'$, so folgt $r = r'$. Angenommen, es wäre $q \neq q'$. Dann ergibt sich mit Hilfe der Bemerkung aus 1.4.2 wegen

$$\deg(r' - r) \leq \max\{\deg r, \deg r'\} < \deg g \quad \text{und}$$

$$\deg(r' - r) = \deg(q' - q) + \deg g \geq \deg g$$

ein Widerspruch.

Zum Beweis der Existenz genügt es, das aus der Schule bekannte Rechenverfahren in allgemeiner Form aufzuschreiben. Seien also

$$f = a_n X^n + \dots + a_0 \quad \text{und} \quad g = b_m X^m + \dots + b_0 \quad \text{mit} \quad n = \deg f \quad \text{und} \quad m = \deg g \geq 0.$$

Ist $n < m$, so kann man $q = 0$ und $r = f$ setzen: $f = 0 \cdot g + f$ ist eine Lösung.

Für $n \geq m$ konstruieren wir schrittweise $q_1, \dots, q_k \in K[X]$, so dass

$$q := q_1 + \dots + q_k$$

ein Quotient wird. Im ersten Schritt sei $f_0 := f$, und indem man die höchsten Terme von f_0 und g teilt, erhält man

$$q_1 := \frac{a_n}{b_m} X^{n-m}.$$

Nun setzen wir für den nächsten Schritt

$$f_1 := f_0 - q_1 g, \quad \text{offensichtlich ist } \deg f_1 < \deg f_0.$$

Ist $\deg f_1 < \deg g$, so ist $q = q_1$ und $r = f_1$ eine Lösung. Andernfalls setzen wir das Verfahren fort und berechnen wie oben mit f_0 und g aus f_1 und g ein q_2 . Dann betrachten wir

$$f_2 := f_1 - q_2 g \quad \text{mit} \quad \deg f_2 < \deg f_1 < \deg f_0 = \deg f.$$

Da die Grade der f_i bei jedem Schritt abnehmen, gibt es ein k derart, dass

$$f_k = f_{k-1} - q_k g \quad \text{und} \quad \deg f_k < \deg g.$$

Das ist spätestens bei $k = n - m + 1$ erreicht. Insgesamt ergibt sich

$$f = q_1 g + f_1 = (q_1 + q_2)g + f_2 = \dots = (q_1 + \dots + q_k)g + f_k,$$

also hat man mit $q := q_0 + \dots + q_k$ und $r := f_k$ eine Lösung. ■

Beispiel Ist $f = X^4 - 2$ und $g = X^2 + 1$, so verläuft die Rechnung wie folgt:

$$\begin{array}{r} (X^4 \quad -2) : (X^2 + 1) = (X^2 - 1) + (-1) : (X^2 + 1) \\ \hline -X^4 \quad -X^2 \\ \hline \quad -X^2 \quad -2 \\ \quad +X^2 \quad +1 \\ \hline \quad \quad -1 \end{array}$$

In diesem Fall ist also $k = 2$,

$$q_1 = X^2, \quad f_1 = -X^2 - 2 \quad \text{und} \quad q_2 = -1, \quad f_2 = -1 = r.$$

1.4.4 Nullstellen von Polynomen

Nach den Abschnitten mit den elementaren technischen Vorbereitungen kommen wir nun zur entscheidenden Frage nach der Existenz und der Berechnung von Nullstellen. Das ist so wichtig, weil sich viele Fragen in der Mathematik und ihren Anwendungen auf Nullstellen von Polynomen zurückführen lassen. In der linearen Algebra werden wir darauf in Kapitel 4 bei der Suche nach Eigenwerten zurückkommen.

Ist $f = a_0 + a_1 X + \dots + a_n X^n \in K[X]$, so heißt ein $x \in K$ **Nullstelle** von f , wenn

$$f(x) = a_0 + a_1 x + \dots + a_n x^n = 0 \in K.$$

Anders ausgedrückt: Die durch f bestimmte Abbildung $\tilde{f} : K \rightarrow K$ hat an der Stelle x den Wert 0.

Zur Frage nach der Existenz von Nullstellen gibt es gute und schlechte Nachrichten; die schlechten zuerst:

Beispiel 1 In $\mathbb{R}[X]$ haben die Polynome

$$f_n := X^{2n} + 1$$

für alle $n \in \mathbb{N}$ keine Nullstellen, da $f_n(x) \geq 1$ für alle $x \in \mathbb{R}$.

Beispiel 2 Ist K ein endlicher Körper, $K = \{x_1, \dots, x_n\}$, so sei

$$f := (X - x_1) \cdot \dots \cdot (X - x_n).$$

Dann ist $\deg f = n$ und $f(x) = 0$ für alle $x \in K$. Also ist $\tilde{f} \in \text{Abb}(K, K)$ die Nullabbildung.

Betrachtet man dagegen $g := f + 1$, so ist auch $\deg g = n$ und $g(x) = 1 \in K$ für alle $x \in K$. Somit hat g in K keine Nullstelle.

Nun zu den positiveren Aussagen:

Beispiel 3 Ist $f \in \mathbb{R}[X]$ und $\deg f$ ungerade, so hat f mindestens eine Nullstelle $x \in \mathbb{R}$. Das wird in der elementaren Analysis bewiesen, es benutzt die Vollständigkeit von \mathbb{R} (vgl. 1.3.4). Es gibt auch sehr gute Verfahren, den Wert von x beliebig genau zu approximieren (vgl. etwa [FO₁, §11]).

Beispiel 4 Ist $f \in \mathbb{R}[X]$ quadratisch, d.h. $\deg f = 2$ und

$$f = aX^2 + bX + c \quad \text{mit} \quad a \neq 0.$$

Dann hat man für die Nullstellen die klassische Formel

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \in \mathbb{C}.$$

Ob es reelle Lösungen gibt, hängt ab von der **Diskriminante** $D(f) := b^2 - 4ac \in \mathbb{R}$. Ist $D(f) > 0$, so gibt es zwei verschiedene Nullstellen. Für $D(f) = 0$ gibt es nur eine und für $D(f) < 0$ keine reelle Nullstelle.

Ähnliche, aber kompliziertere Formeln mit Wurzelausdrücken gibt es auch für Polynome vom Grad 3 und 4; ab Grad 5 sind solche Formeln unmöglich. Das ist ein klassisches Ergebnis der „höheren“ Algebra.

Hat man eine Nullstelle eines Polynoms gefunden, so kann man sich bei der Suche nach weiteren Nullstellen auf ein Polynom kleineren Grades beschränken. Das ergibt sich sofort aus dem

Lemma Ist $x \in K$ eine Nullstelle von $f \in K[X]$, so gestattet f eine eindeutige Zerlegung

$$f = g \cdot (X - x) \quad \text{mit} \quad g \in K[X] \quad \text{und} \quad \deg g = \deg f - 1.$$

Beweis Wir dividieren f mit Rest durch $(X - x)$:

$$f = g \cdot (X - x) + r, \quad \deg r < \deg(X - x) = 1.$$

Durch Einsetzen von x auf beiden Seiten folgt

$$0 = f(x) = g(x) \cdot (x - x) + r(x) = 0 + r(x).$$

Wäre $\deg r = 0$, so wäre $r = a \neq 0$. Also muss $\deg r = -\infty$ und $r = 0$ sein. ■

Wir notieren weitere einfache Folgerungen.

Korollar 1 Sie K ein beliebiger Körper und $f \in K[X]$ vom Nullpolynom verschieden. Für die Zahl k der Nullstellen von f in K gilt

$$k \leq \deg f.$$

Beweis Mit Hilfe des Lemmas kann man Schritt für Schritt Nullstellen herausteilen, dadurch verringert sich jeweils der Grad um 1. Damit ist die Behauptung klar. Das kann man auch etwas formaler durch Induktion über $n = \deg f$ beweisen.

Im Fall $n = 0$ ist $f = a_0 \neq 0$ ein konstantes Polynom, also ist $k = 0$.

Sei also $\deg f = n \geq 1$. Hat f keine Nullstelle, so ist $k = 0$. Ist $x \in K$ Nullstelle von f , so folgt aus dem Lemma

$$f = g \cdot (X - x) \quad \text{mit} \quad \deg g = n - 1.$$

Für jede von x verschiedene Nullstelle $y \in K$ von f gilt

$$0 = f(y) = (y - x) \cdot g(y),$$

also muss $g(y) = 0$ sein.

Ist l die Anzahl der Nullstellen von g in K , so gilt offensichtlich $k = l + 1$ und nach Induktionsannahme gilt

$$l \leq n - 1, \quad \text{also folgt} \quad k = l + 1 \leq n.$$

■

Man beachte, dass in diesem Beweis benutzt wurde, dass es in einem Körper keine Nullteiler gibt. Ist R ein kommutativer Ring mit Eins, so kann man analog auch den Polynomring $R[X]$ konstruieren. Dann ist aber die Aussage von Korollar 1 nicht mehr allgemein gültig.

Beispiel Sei $R = \mathbb{Z}/6\mathbb{Z}$ der Restklassenring aus 1.3.7 und

$$f := X^2 + X \in R[X] \quad \text{mit} \quad \deg f = 2.$$

In R hat f die folgenden Werte:

x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$f(x)$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{0}$	$\bar{2}$	$\bar{0}$

Also hat f vier Nullstellen $\bar{0}, \bar{2}, \bar{3}$ und $\bar{5}$. Das ergibt die verschiedenen Zerlegungen

$$f = (X - \bar{0}) \cdot (X - \bar{5}) = (X - \bar{2}) \cdot (X - \bar{3}).$$

Korollar 2 Ist der Körper K unendlich, so ist die Abbildung

$$K[X] \rightarrow \text{Abb}(K, K), \quad f \mapsto \tilde{f},$$

die jedem Polynom f die dadurch definierte Polynomfunktion $\tilde{f}: K \rightarrow K$ zuordnet, injektiv.

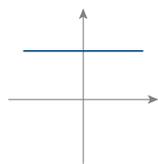
In diesem Fall muss man also nicht zwischen Polynomen und Polynomfunktionen unterscheiden. Wie wir in Beispiel 2 gesehen hatten, ist diese Unterscheidung aber in jedem endlichen Körper geboten.

Beweis Seien $f_1, f_2 \in K[X]$ mit $\tilde{f}_1 = \tilde{f}_2$. Für $g := f_2 - f_1$ gilt dann $\tilde{g} = \mathbf{o}$, d.h. $\tilde{g}(x) = 0$ für alle $x \in K$. Nach Korollar 1 muss $g = \mathbf{o}$, also $f_2 = f_1$ sein. ■

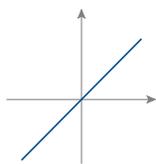
Bei der Zählung der Nullstellen eines Polynoms empfiehlt es sich, zu berücksichtigen, „wie oft“ eine Nullstelle vorkommt. Am deutlichsten sieht man das im Fall $K = \mathbb{R}$ an einem einfachen Beispiel. Das Polynom

$$f_n = X^n = \underbrace{(X - 0) \cdot \dots \cdot (X - 0)}_{n\text{-mal}}$$

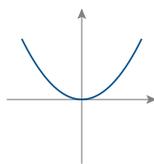
hat den Grad n , aber für $n \geq 1$ nur die eine Nullstelle $x = 0$.



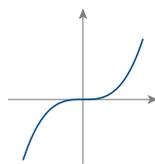
$n = 0$



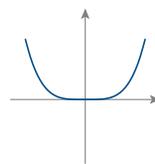
$n = 1$



$n = 2$



$n = 3$



$n = 4$

Geometrisch sieht man, dass der Graph von f_n mit der horizontalen Achse für steigendes n immer „höheren“ Kontakt hat; algebraisch sagt man, f_n hat an der Stelle $x = 0$ eine Nullstelle der „Ordnung“ (oder „Vielfachheit“) n .

Ganz allgemein kann man für ein $f \in K[X]$ und $x \in K$ eine **Vielfachheit der Nullstelle** x von f erklären durch

$$\mu(f; x) := \max\{r \in \mathbb{N} : f = (X - x)^r \cdot g \text{ mit } g \in K[X]\}.$$

Anders ausgedrückt: Man teilt den Faktor $(X - x)$ so lange aus f heraus, bis ein g mit $g(x) \neq 0$ übrig bleibt. Offensichtlich gilt:

$$0 \leq \mu(f; x) \leq \deg f \quad \text{und} \quad f(x) = 0 \quad \Leftrightarrow \quad \mu(f; x) \geq 1.$$

Sind $x_1, \dots, x_k \in K$ die paarweise verschiedenen Nullstellen eines Polynoms $f \in K[X]$, so erhält man schließlich durch wiederholte Anwendung des obigen Lemmas eine Darstellung

$$f = (X - x_1)^{r_1} \cdot \dots \cdot (X - x_k)^{r_k} \cdot g,$$

mit $r_i = \mu(f; x_i) \geq 1$ für $i = 1, \dots, k$ und einem verbleibenden Polynom $g \in K[X]$ ohne Nullstelle in K . Als Verschärfung von Korollar 1 ergibt sich

$$r_1 + \dots + r_k \leq \deg f.$$

In der Analysis lernt man, was im Fall $K = \mathbb{R}$ die Vielfachheit einer Nullstelle mit den Ableitungen zu tun hat:

$$\mu(f; x) = \max\{r \in \mathbb{N} : f(x) = f'(x) = \dots = f^{(r-1)}(x) = 0\}.$$

1.4.5 Eine Vorzeichenregel für reelle Polynome

Besonders erfreulich ist der Fall, wenn ein Polynom mit Vielfachheit gezählt so viele Nullstellen hat, wie sein Grad angibt. Das bedeutet, dass f in **Linearfaktoren** zerfällt, d.h.

$$f = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0 = (X - x_1) \cdot \dots \cdot (X - x_n),$$

mit $a_0, \dots, a_{n-1} \in K$ und $x_1, \dots, x_n \in K$. Dabei haben wir zur Vereinfachung $a_n = 1$ angenommen, das hat keinen Einfluß auf die Nullstellen. Es ist klar, dass sich die n Koeffizienten und die n Nullstellen gegenseitig festlegen. Wir schon erwähnt, ist es sehr schwierig, die Nullstellen aus den Koeffizienten zu berechnen. Die andere Richtung ist

ganz einfach, man muss nur die n Linearfaktoren $(X - x_i)$ ausmultiplizieren. Das Ergebnis ist

$$\begin{aligned} a_0 &= (-1)^n x_1 \cdot \dots \cdot x_n \\ a_1 &= (-1)^{n-1} (x_2 \cdot \dots \cdot x_n + x_1 \cdot x_3 \cdot \dots \cdot x_n + \dots + x_1 \cdot x_2 \cdot \dots \cdot x_{n-1}) \\ &\vdots \\ a_{n-2} &= x_1 \cdot x_2 + \dots + x_1 \cdot x_n + x_2 \cdot x_3 + \dots + x_2 \cdot x_n + \dots + x_{n-1} \cdot x_n \\ a_{n-1} &= -(x_1 + \dots + x_n). \end{aligned}$$

Das kann man formal etwas schöner aufschreiben, indem man die *elementarsymmetrischen Funktionen* s_k von x_1, \dots, x_n benutzt. Für $k = 1, \dots, n$ ist

$$s_k(x_1, \dots, x_n) := \sum_{1 \leq i_1 < \dots < i_k \leq n} x_{i_1} \cdot \dots \cdot x_{i_k}.$$

Die Summe hat $\binom{n}{k}$ Summanden, das ist die Anzahl der Möglichkeiten aus $\{1, \dots, n\}$ insgesamt k verschiedene Indizes i_1, \dots, i_k auszuwählen. Mit dieser Notation gilt für die Koeffizienten von f

$$a_k = (-1)^{n-k} \cdot s_{n-k}(x_1, \dots, x_n) \quad \text{für } k = 0, \dots, n-1.$$

Diese Formel nennt man den *Wurzelsatz* von VIETA.

In der Theorie der Eigenwerte werden wir reellen Polynomen begegnen, von denen man auf Grund ihrer Herkunft weiß, dass sie in Linearfaktoren zerfallen, aber deren Nullstellen unbekannt sind. Wenn es genügt zu wissen, ob alle Nullstellen positiv oder negativ sind, hilft die folgende klassische

Vorzeichenregel Angenommen, das reelle Polynom $f \in \mathbb{R}[X]$ zerfällt in Linearfaktoren, d.h.

$$f = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0 = (X - x_1) \cdot \dots \cdot (X - x_n)$$

mit $x_1, \dots, x_n \in \mathbb{R}$. Dann gilt:

- Genau dann sind alle Nullstellen x_i negativ, wenn alle Koeffizienten a_k positiv sind.
- Genau dann sind alle Nullstellen x_i positiv, wenn die Vorzeichen der Koeffizienten a_k alternierend sind, d.h. für $k = 0, \dots, n-1$ gilt

$$(-1)^{n-k} \cdot a_k > 0, \quad \text{d.h.} \quad \begin{cases} a_k > 0 & \text{für } n-k \text{ gerade,} \\ a_k < 0 & \text{für } n-k \text{ ungerade.} \end{cases}$$

Beweis Wir zeigen zunächst Teil a). Sind alle $a_k > 0$, so gilt für $x \geq 0$, dass

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \geq a_0 > 0.$$

Also müssen alle Nullstellen negativ sein. Sind umgekehrt alle $x_i < 0$, so gilt nach Definition der elementarsymmetrischen Funktionen

$$s_k(x_1, \dots, x_n) \begin{cases} > 0 & \text{für } k \text{ gerade,} \\ < 0 & \text{für } k \text{ ungerade.} \end{cases}$$

Daraus folgt $a_k = (-1)^{n-k} \cdot s_{n-k}(x_1, \dots, x_n) > 0$ für alle k .

Teil b) folgt aus Teil a), indem man von f zu f_- mit

$$f_-(X) := f(-X)$$

übergeht. Dabei werden aus negativen Nullstellen von f positive Nullstellen von f_- und wegen

$$a_k(-X)^k = (-1)^k \cdot a_k X^k$$

werden aus positiven Koeffizienten von f in f_- Koeffizienten mit alternierenden Vorzeichen. ■

1.4.6 Der Fundamentalsatz der Algebra

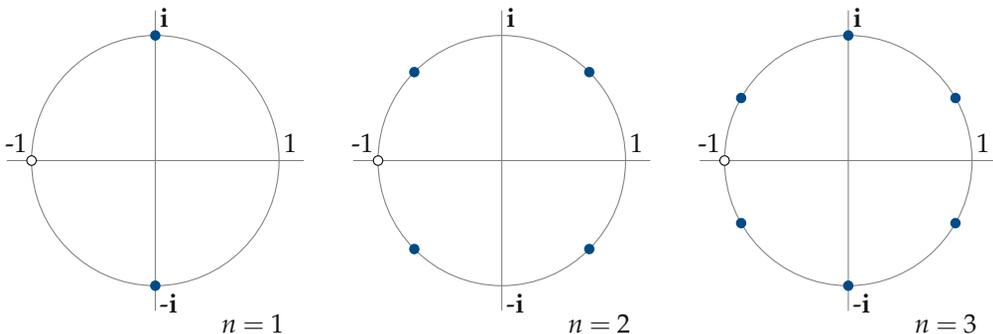
Die bisher beschriebenen Eigenschaften von Polynomen sind recht elementar und - bis auf die Vorzeichenregel für reelle Polynome - weitgehend unabhängig vom Körper K . Nun kommen wir zum entscheidenden Problem: Über vielen Körpern K gibt es Polynome beliebigen Grades ohne Nullstellen in K , etwa

$$f = X^n - 2 \text{ für } n \geq 2 \text{ in } K = \mathbb{Q}, \quad f = X^{2n} + 1 \text{ für } n \geq 2 \text{ in } K = \mathbb{R}.$$

Dass es für $n \geq 2$ keine n -te Wurzel aus 2 gibt, beweist man wie in 0.1.1 im Fall $n = 2$. Und für $x \in \mathbb{R}$ ist $x^{2n} + 1 > 0$.

In beiden Fällen gibt es einen Ausweg. Geht man vom Körper \mathbb{Q} der rationalen Zahlen zum größeren Körper \mathbb{R} der reellen Zahlen über, so gibt es für alle n zumindest eine reelle n -te Wurzel aus 2. Geht man von den reellen Zahlen über zu den komplexen Zahlen, so hat $X^{2n} + 1$ die $2n$ verschiedenen nicht reellen Nullstellen

$$\exp\left(\frac{(2k-1)\pi i}{2n}\right) \in \mathbb{C} \text{ mit } k = 1, \dots, 2n.$$



Dabei wird die Darstellung komplexer Zahlen in Polarkoordinaten verwendet.

Dass die Folge der Körpererweiterungen $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ bei den komplexen Zahlen einen gewissen Abschluss erreicht hat, besagt der

Fundamentalsatz der Algebra Jedes Polynom $f \in \mathbb{C}[X]$ mit $n := \deg f \geq 1$ zerfällt in Linearfaktoren, d.h. es gibt $a, z_1, \dots, z_n \in \mathbb{C}$ mit $a \neq 0$ derart, dass

$$f = a \cdot (X - z_1) \cdot \dots \cdot (X - z_n).$$

Für dieses tiefliegende Ergebnis gibt es zahlreiche Beweise. Nach einigen vorhergehenden Anläufen gab GAUSS insgesamt vier verschiedene Beweise dafür, den ersten in seiner Dissertation aus dem Jahr 1799 [GA₁].

Es genügt offenbar Folgendes zu zeigen:

Fundamental-Lemma Jedes Polynom $f \in \mathbb{C}[X]$ mit $n := \deg f \geq 1$ hat mindestens eine komplexe Nullstelle.

Ist nämlich $z \in \mathbb{C}$ eine Nullstelle von f , so gibt es nach dem Lemma aus 1.4.4 eine Zerlegung

$$f = (X - z) \cdot g \quad \text{mit} \quad g \in \mathbb{C}[X] \quad \text{und} \quad \deg g = \deg f - 1.$$

Im nächsten Schritt wendet man das Fundamental-Lemma auf g an, u.s.w. bis nur noch ein konstantes Polynom $a \in \mathbb{C}$ übrig bleibt.

Die komplexen Zahlen sind aus den reellen Zahlen entstanden und die reellen Zahlen sind kein reines Produkt der Algebra, sondern auch der Analysis. Daher ist es unvermeidlich, dass die Beweise des Fundamental-Lemmas Hilfsmittel aus der Analysis benutzen. Beispiele dafür findet man etwa in ([F₁₃, III 4.7]).

Nun wollen wir eine wichtige Folgerung aus dem Fundamentalsatz für reelle Polynome, d.h. Polynome $f \in \mathbb{R}[X]$ ziehen. Dabei können wir annehmen, dass f normiert ist. Dann gibt es eine eindeutige Zerlegung

$$f = (X - x_1) \cdot \dots \cdot (X - x_m) \cdot (X - z_1) \cdot \dots \cdot (X - z_r) \quad \text{mit} \quad m + r = n = \deg f,$$

wobei $x_1, \dots, x_m \in \mathbb{R}$ und $z_1, \dots, z_r \in \mathbb{C} \setminus \mathbb{R}$. Nach dem Lemma in 1.4.4 gibt es eine Zerlegung

$$f = (X - x_1) \cdot \dots \cdot (X - x_m) \cdot g \quad \text{mit} \quad g \in \mathbb{R}[X],$$

so dass g keine reellen Nullstellen hat. Also ist

$$g = (X - z_1) \cdot \dots \cdot (X - z_r)$$

und $r = \deg g$ ist gerade, da ein Polynom $g \in \mathbb{R}[X]$ ungeraden Grades mindestens eine reelle Nullstelle hat.

Nun zeigen wir, dass die nicht reellen Nullstellen von f , das sind die Nullstellen von g , ganz speziell verteilt sind. Dazu benötigen wir folgenden

Hilfssatz

1. Ist $f \in \mathbb{R}[X]$ und $z \in \mathbb{C}$ Nullstelle von f , so ist auch $\bar{z} \in \mathbb{C}$ Nullstelle von f .
2. Für jedes $z \in \mathbb{C}$ gilt $(X - z) \cdot (X - \bar{z}) \in \mathbb{R}[X]$.
3. Ist $f \in \mathbb{R}[X]$ und $z \in \mathbb{C}$, so gilt für die Vielfachheiten der Nullstellen

$$\mu(f; \bar{z}) = \mu(f; z).$$

Anders ausgedrückt: Die komplexen Nullstellen eines Polynoms mit reellen Koeffizienten liegen mit Vielfachheit gezählt symmetrisch zur reellen Achse.

Beweis

1. Ist $f = a_0 + a_1X + \dots + a_nX^n$, so ist wegen $\overline{a_0} = a_0, \dots, \overline{a_n} = a_n$ nach den Rechenregeln für die komplexe Konjugation

$$f(\bar{z}) = a_0 + a_1\bar{z} + \dots + a_n\bar{z}^n = \overline{a_0} + \overline{a_1\bar{z}} + \dots + \overline{a_n z^n} = \overline{f(z)} = \bar{0} = 0.$$

2. Sei $z = x + iy$ mit $x, y \in \mathbb{R}$. Dann ist

$$(X - z) \cdot (X - \bar{z}) = (X - x - iy) \cdot (X - x + iy) = X^2 - (2x)X + (x^2 + y^2).$$

Dass dieses reelle Polynom für $z \notin \mathbb{R}$ keine reellen Nullstellen haben kann, sieht man auch an der Diskriminante

$$D = 4x^2 - 4(x^2 + y^2) = -4y^2 \leq 0.$$

Für $z \notin \mathbb{R}$ ist $y \neq 0$, also $D < 0$.

3. Es genügt, den Fall zu betrachten, dass $z \in \mathbb{C} \setminus \mathbb{R}$ und $f(z) = 0$. Nach 1. ist auch $f(\bar{z}) = 0$, also gibt es eine Zerlegung

$$f = (X - z) \cdot (X - \bar{z}) \cdot g,$$

und aus 2. folgt $g \in \mathbb{R}[X]$. Ist $s := \mu(f; z) > 1$, so ist auch $g(z) = 0$ und $g(\bar{z}) = 0$ nach 1. Schließlich erhält man eine Zerlegung

$$f = (X - z)^s \cdot (X - \bar{z})^s \cdot \tilde{g} \quad \text{mit} \quad \tilde{g} \in \mathbb{R}[X]$$

und $\tilde{g}(z) \neq 0$, also nach 1. auch $\tilde{g}(\bar{z}) \neq 0$. ■

Damit zurück zu dem oben verbliebenen Polynom

$$g = (X - z_1) \cdot \dots \cdot (X - z_r), \quad \text{wobei} \quad z_1, \dots, z_r \in \mathbb{C} \setminus \mathbb{R}.$$

Da die Reihenfolge der z_i gleichgültig und $r = 2k$ gerade ist, können wir nach dem Hilfssatz annehmen, dass

$$z_2 = \bar{z}_1, z_4 = \bar{z}_3, \dots, z_r = \bar{z}_{r-1}.$$

Aus diesen Paaren konjugiert komplexer Nullstellen konstruieren wir die neuen Polynome

$$g_1 := (X - z_1) \cdot (X - \bar{z}_1), \dots, g_k = (X - z_{r-1}) \cdot (X - \bar{z}_{r-1})$$

mit $g = g_1 \cdot \dots \cdot g_k$ und $\deg g_i = 2$ für $i = 1, \dots, k$. Insgesamt haben wir also Folgendes bewiesen:

Fundamentalsatz der Algebra in der reellen Form Jedes normierte Polynom $f \in \mathbb{R}[X]$ mit $\deg f = n \geq 1$ gestattet eine bis auf die Reihenfolge der Faktoren eindeutige Zerlegung

$$f = (X - x_1) \cdot \dots \cdot (X - x_m) \cdot g_1 \cdot \dots \cdot g_k,$$

wobei $n = m + 2k$, $x_1, \dots, x_m \in \mathbb{R}$ und $g_1, \dots, g_k \in \mathbb{R}[X]$ normierte Polynome vom Grad 2 ohne reelle Nullstellen sind. ■

Man beachte, dass in dieser Form des Fundamentalsatzes die komplexen Zahlen gar nicht vorkommen. Man kann aber aus dieser reellen Form die komplexe Form des Fundamentalsatzes ganz elementar ableiten (vgl. etwa [FI₃]).

Beispiel 1 Schon zu Beginn dieses Abschnittes hatten wir die $2n$ -ten Wurzeln von -1 bestimmt, das sind die Nullstellen von $f = X^{2n} + 1$. Da f keine reelle Nullstelle hat, gibt es eine Zerlegung

$$f = g_1 \cdot \dots \cdot g_n,$$

wobei $g_1, \dots, g_n \in \mathbb{R}[X]$ quadratische Faktoren sind. Mit Hilfe der Nullstellen

$$z_k := \exp\left(\frac{(2k-1)\pi i}{2n}\right) \quad \text{mit } k = 1, \dots, 2n$$

kann man die Faktoren explizit bestimmen. Dabei muss man nur sorgfältig in den Polarkoordinaten rechnen.

Der Fall $n = 1$ ist ganz einfach. Hier ist

$$z_1 = \exp\left(\frac{\pi i}{2}\right) = \mathbf{i} \quad \text{und} \quad z_2 = \exp\left(\frac{3\pi i}{2}\right) = \exp\left(\frac{-\pi i}{2}\right) = -\mathbf{i} = \mathbf{i}^{-1},$$

$$\text{also } g_1 = (X - \mathbf{i}) \cdot (X + \mathbf{i}) = X^2 + 1 = f.$$

Im Fall $n = 2$ fassen wir die Nullstellen wie folgt zu Paaren zusammen:

$$z_1 = \exp\left(\frac{\pi i}{4}\right) \quad \text{mit} \quad z_4 = \exp\left(\frac{7\pi i}{4}\right) = \exp\left(\frac{-\pi i}{4}\right) = z_1^{-1} \quad \text{und}$$

$$z_2 = \exp\left(\frac{3\pi i}{4}\right) \quad \text{mit} \quad z_3 = \exp\left(\frac{5\pi i}{4}\right) = \exp\left(\frac{-3\pi i}{4}\right) = z_2^{-1}.$$

Dann folgt unter Benutzung der Formel von EULER aus 1.3.5

$$g_1 = (X - z_1) \cdot (X - z_4) = X^2 - 2 \cos\left(\frac{\pi}{4}\right) X + 1 \quad \text{und}$$

$$g_2 = (X - z_2) \cdot (X - z_3) = X^2 - 2 \cos\left(\frac{3\pi}{4}\right) X + 1.$$

Für allgemeines n fasst man die Nullstellen

$$z_1 \text{ mit } z_{2n}, \quad z_2 \text{ mit } z_{2n-1}, \quad \dots, \quad z_n \text{ mit } z_{n+1}$$

zusammen. Wir überlassen es dem Leser zur Übung, die Polynome

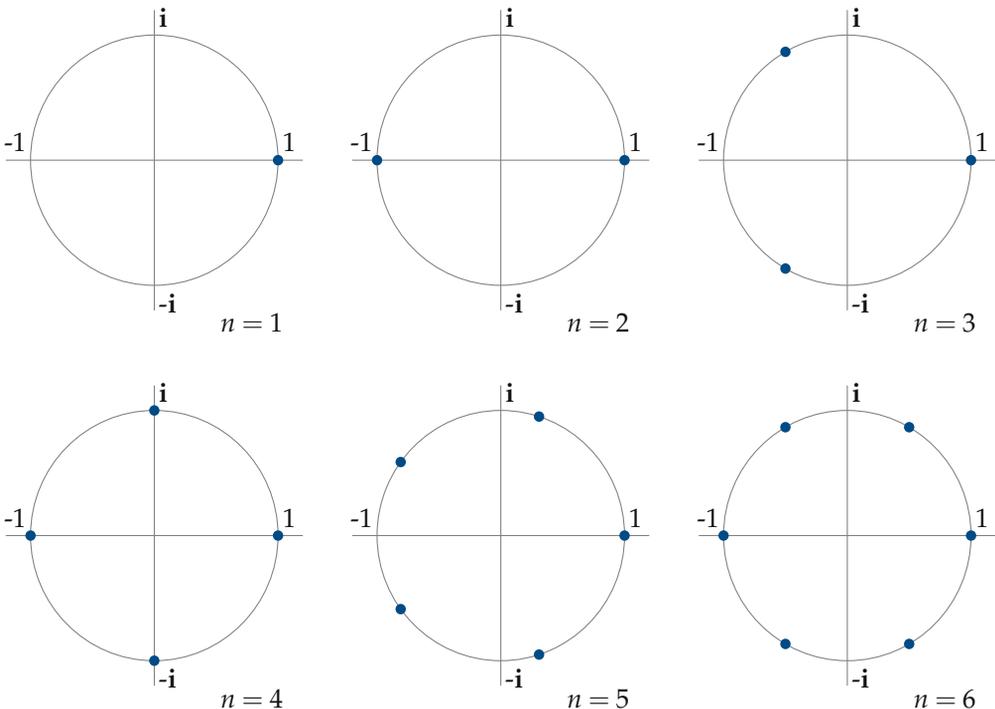
$$g_1 := (X - z_1) \cdot (X - z_{2n}), \dots, g_n := (X - z_n) \cdot (X - z_{n+1})$$

explizit auszurechnen.

Beispiel 2 Die Nullstellen von $X^n - 1 \in \mathbb{R}[X]$ sind für jedes $n \in \mathbb{N}^*$ die n -ten Wurzeln von 1, man nennt sie *Einheitswurzeln*. Man kann sie – wieder in Polarkoordinaten – explizit angeben:

$$z_l := \exp\left(\frac{2\pi i l}{n}\right) \quad \text{mit } l = 0, \dots, n - 1,$$

denn $z_l^n = \exp(2\pi i l) = 1$. Die offensichtlichen reellen Nullstellen sind $z_0 = 1$ für alle n und $z_{\frac{n}{2}} = \exp(\pi i) = -1$ für gerades n . Alle anderen Nullstellen von $X^n - 1$ sind nicht reell.



Wie in Beispiel 1 kann man aus Paaren konjugiert komplexer Nullstellen quadratische Polynome $g_i \in \mathbb{R}[X]$ aufbauen, und man erhält damit die Zerlegung

$$X^n - 1 = (X - 1) \cdot g_1 \cdot \dots \cdot g_k \quad \text{für } n = 2k + 1 \text{ ungerade} \quad \text{und}$$

$$X^n - 1 = (X - 1) \cdot (X + 1) \cdot g_1 \cdot \dots \cdot g_{k-1} \quad \text{für } n = 2k \text{ gerade.}$$

*A right line AB, considered as having not only length,
but also direction, is said to be a VECTOR.*

WILLIAM ROWAN HAMILTON

Kapitel 2

Vektorräume und lineare Abbildungen

Nach den Motivationen in Kapitel 0 und den Grundlagen in Kapitel 1 beginnt nun die eigentliche lineare Algebra. Sie ist entstanden als Hilfsmittel der Geometrie, wird aber inzwischen in fast allen Gebieten der Mathematik benutzt. Der fundamentale Begriff des Vektorraums hat sich erst im 19. Jahrhundert entwickelt. Ein Pionier dabei war H. GRASSMANN – Professor am Gymnasium zu Stettin – mit seiner „Ausdehnungslehre“ [GR], in der er „extensive Größen“ einführt, die G. PEANO [PE₁] später, HAMILTON folgend, „vettori“ nannte. Es hat lange gedauert, bis die fundamentalen Beiträge von GRASSMANN verstanden und gewürdigt wurden. Eine strenge axiomatische Beschreibung von Vektoren findet man bei H. WEYL [WEY] in seinem Buch über allgemeine Relativitätstheorie aus dem Jahr 1918:

1. Vektoren.

Je zwei Vektoren \mathfrak{a} und \mathfrak{b} bestimmen eindeutig einen Vektor $\mathfrak{a} + \mathfrak{b}$ als ihre »Summe«; eine Zahl λ und ein Vektor \mathfrak{a} bestimmen eindeutig einen Vektor $\lambda\mathfrak{a}$, das » λ -fache von \mathfrak{a} « (Multiplikation). Diese Operationen genügen folgenden Gesetzen.

α) Addition.

1. $\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}$ (kommutatives Gesetz).
2. $(\mathfrak{a} + \mathfrak{b}) + \mathfrak{c} = \mathfrak{a} + (\mathfrak{b} + \mathfrak{c})$ (assoziatives Gesetz).
3. Sind \mathfrak{a} und \mathfrak{c} irgend zwei Vektoren, so gibt es einen und nur einen \mathfrak{x} , für welchen die Gleichung $\mathfrak{a} + \mathfrak{x} = \mathfrak{c}$ gilt. Er heißt die Differenz $\mathfrak{c} - \mathfrak{a}$ von \mathfrak{c} und \mathfrak{a} . (Möglichkeit der Subtraktion.)

β) Multiplikation.

1. $(\lambda + \mu)\mathfrak{a} = (\lambda\mathfrak{a}) + (\mu\mathfrak{a})$ (erstes distributives Gesetz).
2. $\lambda(\mu\mathfrak{a}) = (\lambda\mu)\mathfrak{a}$ (assoziatives Gesetz).
3. $1\mathfrak{a} = \mathfrak{a}$.
4. $\lambda(\mathfrak{a} + \mathfrak{b}) = (\lambda\mathfrak{a}) + (\lambda\mathfrak{b})$ (zweites distributives Gesetz).

Schließlich hat ST. BANACH [BA] auch Vektorräume von Funktionen eingeführt und damit die so genannte „Funktionalanalysis“ begründet. Mehr zur historischen Entwicklung findet man etwa bei [KOE, Kap. 1, §2].

2.1 Grundlagen

2.1.1 Vektorräume

Die in 0.1.2 zusammengestellten Rechenregeln für Vektoren des \mathbb{R}^n sind die Grundlage für die axiomatische Definition eines Vektorraumes. Statt \mathbb{R} wird ein beliebiger Körper K zugelassen (die Elemente von K werden *Skalare* genannt); mit Hilfe des in 1.2.3 eingeführten Begriffs der Gruppe kann man die Regeln etwas kürzer formulieren.

Definition Ein *Vektorraum* über einem Körper K besteht aus einer Menge V zusammen mit

- einer Addition $+$: $V \times V \rightarrow V$, $(v, w) \mapsto v + w$, und
- einer Multiplikation mit Skalaren \bullet : $K \times V \rightarrow V$, $(\lambda, v) \mapsto \lambda \bullet v$,

so dass gilt:

V1 $(V, +)$ ist eine abelsche Gruppe mit einem Nullelement \mathbf{o} (es heißt *Nullvektor*).

Der zu v negative Vektor wird mit $-v$ bezeichnet.

V2 Für alle $\lambda, \mu \in K$ und alle $v, w \in V$ ist

$$\begin{aligned} (\lambda \cdot \mu) \bullet v &= \lambda \bullet (\mu \bullet v), & 1 \bullet v &= v, \\ (\lambda + \mu) \bullet v &= \lambda \bullet v + \mu \bullet v, & \lambda \bullet (v + w) &= \lambda \bullet v + \lambda \bullet w. \end{aligned}$$

Genau genommen ist ein Vektorraum ein Tripel $(V, +, \bullet)$; kürzer sagt man, V ist ein K -Vektorraum, oder ein Vektorraum über K .

Aus den Axiomen folgen weitere

Rechenregeln für Vektoren Ist V ein K -Vektorraum, $v \in V$ und $\lambda \in K$, so gilt:

- a) $0 \bullet v = \mathbf{o}$.
- b) $\lambda \bullet \mathbf{o} = \mathbf{o}$.
- c) $\lambda \bullet v = \mathbf{o} \Rightarrow \lambda = 0$ oder $v = \mathbf{o}$.
- d) $(-1) \bullet v = -v$.

Beweis a) $0 \bullet v = (0 + 0) \bullet v = 0 \bullet v + 0 \bullet v$.

b) $\lambda \bullet \mathbf{o} = \lambda \bullet (\mathbf{o} + \mathbf{o}) = \lambda \bullet \mathbf{o} + \lambda \bullet \mathbf{o}$.

c) Ist $\lambda \bullet v = \mathbf{o}$, aber $\lambda \neq 0$, so folgt

$$v = \mathbf{1} \bullet v = (\lambda^{-1} \cdot \lambda) \bullet v = \lambda^{-1} \bullet (\lambda \bullet v) = \lambda^{-1} \bullet \mathbf{o} = \mathbf{o}.$$

d) $v + (-1) \bullet v = \mathbf{1} \bullet v + (-1) \bullet v = (1 - 1) \bullet v = 0 \bullet v = \mathbf{o}$. ■

Beispiel 1 Analog zum \mathbb{R}^n in 0.1.2 kann man für jeden Körper K und $n \in \mathbb{N}^*$ das direkte Produkt K^n zu einem K -Vektorraum machen, indem man für

$$v = (x_1, \dots, x_n) \quad \text{und} \quad w = (y_1, \dots, y_n) \in K^n \quad \text{sowie} \quad \lambda \in K$$

$$v + w := (x_1 + y_1, \dots, x_n + y_n) \quad \text{und} \quad \lambda \bullet v := (\lambda \cdot x_1, \dots, \lambda \cdot x_n)$$

erklärt. Nullvektor ist in diesem Fall $\mathbf{o} = (0, \dots, 0) \in K^n$. Man nennt K^n mit diesen Verknüpfungen den n -dimensionalen **Standardraum** über K .

Entscheidend für den Nutzen der abstrakten Definition eines Vektorraumes ist es, dass es neben den Standardräumen auch viel allgemeinere Beispiele gibt:

Beispiel 2 Ist K ein Körper und M eine beliebige nicht leere Menge, so kann man die Menge

$$V := \text{Abb}(M, K) = \{f : M \rightarrow K\}$$

aller Abbildungen von M nach K zu einem K -Vektorraum machen, indem man für $f, g \in V$ und $\lambda \in K$ die Abbildungen $f + g$ und $\lambda \bullet f$ erklärt durch

$$(f + g)(x) := f(x) + g(x) \quad \text{und} \quad (\lambda \bullet f)(x) := \lambda \cdot f(x)$$

für alle $x \in M$. Der Nachweis der Vektorraum-Axiome ist eine einfache Übungsaufgabe. Nullvektor ist die Nullabbildung \mathbf{o} mit $\mathbf{o}(x) = 0$ für alle $x \in M$.

Offensichtlich ist Beispiel 1 ein Spezialfall von Beispiel 2 mit $M = \{1, \dots, n\}$, denn man kann

$$K^n = \text{Abb}(\{1, \dots, n\}, K)$$

setzen.

Beispiel 3 Ein Spezialfall von Beispiel 2 ist der Vektorraum

$$\mathcal{F} := \text{Abb}(\mathbb{N}, \mathbb{R}) = \{(x_i) : i \in \mathbb{N}, x_i \in \mathbb{R}\}$$

aller reellen Zahlenfolgen. Für $(x_i), (y_i) \in \mathcal{F}$ sowie $\lambda \in \mathbb{R}$ ist

$$(x_i) + (y_i) := (x_i + y_i) \quad \text{und} \quad \lambda \bullet (x_i) := (\lambda \cdot x_i).$$

Auch dieses Beispiel ist ein erster Hinweis auf die Bedeutung von Vektorräumen in der Analysis.

Beispiel 4 In 1.4.2 hatten wir für jeden Körper K den Ring $K[X]$ der Polynome mit Koeffizienten aus K betrachtet. Zusammen mit der Addition von Polynomen ist $K[X]$

eine abelsche Gruppe. Man hat auch eine naheliegende Multiplikation mit Skalaren, indem man

$$\lambda \bullet (a_0 + a_1 X + \dots + a_n X^n) := \lambda \cdot a_0 + (\lambda \cdot a_1) X + \dots + (\lambda \cdot a_n) X^n$$

setzt. Dadurch wird $K[X]$ zu einem K -Vektorraum.

Beispiel 5 Die Menge \mathbb{R} der reellen Zahlen ist nicht nur ein \mathbb{R} -Vektorraum, sondern auch ein \mathbb{Q} -Vektorraum, denn für $\lambda \in \mathbb{Q}$ und $x \in \mathbb{R}$ kann man

$$\lambda \bullet x := \lambda \cdot x$$

setzen, wobei $\lambda \cdot x$ das Produkt reeller Zahlen bedeutet. Das ist nicht nur eine Spielerei, sondern ein wichtiges Werkzeug zum Studium von Körpererweiterungen, in diesem Fall $\mathbb{Q} \subset \mathbb{R}$. Ganz analog ist \mathbb{C} ein \mathbb{R} -Vektorraum, der in 1.3.7 eingeführte Körper \mathbb{F}_4 ist ein Vektorraum über dem Primkörper \mathbb{F}_2 .

Beispiel 6 Analog zur Konstruktion des Vektorraumes K^n aus dem Körper K kann man aus mehreren Vektorräumen ein Produkt bilden.

Sind K -Vektorräume V_1, \dots, V_n gegeben, so kann man auf der Menge

$$V := V_1 \times \dots \times V_n = \{(v_1, \dots, v_n) : v_i \in V_i \text{ für } i = 1, \dots, n\}$$

eine „komponentenweise“ Addition durch

$$(v_1, \dots, v_n) + (v'_1, \dots, v'_n) := (v_1 + v'_1, \dots, v_n + v'_n)$$

erklären. Dabei bezeichnen die Zeichen $+$ die Additionen in den Vektorräumen V_i , die Addition in V wird mit $+$ bezeichnet. Analog hat man in V eine Multiplikation mit Skalaren $\lambda \in K$

$$\lambda \bullet (v_1, \dots, v_n) := (\lambda \cdot v_1, \dots, \lambda \cdot v_n).$$

Es ist ganz leicht nachzuweisen, dass V dadurch zu einem K -Vektorraum wird; man nennt V das *direkte Produkt* der Vektorräume V_1, \dots, V_n . In diesem Sinne ist

$$K^n = K \times \dots \times K.$$

Beispiel 7 Sind $m, n \in \mathbb{N}^*$, so bezeichnen wir mit $M(m \times n; K)$ die Menge aller Matrizen mit m Zeilen, n Spalten und Einträgen aus K . Für

$$A = (a_{ij}), \quad B = (b_{ij}) \in M(m \times n; K) \quad \text{und } \lambda \in K$$

erhält man neue Matrizen

$$A + B := (a_{ij} + b_{ij}) \quad \text{und} \quad \lambda \bullet A := (\lambda \cdot a_{ij})$$

in $M(m \times n; K)$. Nullelement ist die *Nullmatrix*, bei der alle Einträge gleich 0 sind. Dass $M(m \times n; K)$ auf diese Weise zu einem K -Vektorraum wird, sieht man wie in Beispiel 1.

In der Tat unterscheidet sich die Menge $M(m \times n; K)$ von $K^{m \cdot n}$ nur dadurch, in welcher Weise die Einträge aufgeschrieben werden.

Nach diesen Beispielen ist wohl klar, dass die Unterscheidung der Bezeichnungen $+$, $-$, \cdot und $+$, $-$, \bullet für die Operationen im Körper und im Vektorraum aufgegeben werden kann. Wir lassen die fetten Symbole fallen; der Malpunkt \cdot wird auch weggelassen, wo er entbehrlich scheint. Nur der Nullvektor \mathbf{o} bleibt klein und fett, zur Unterscheidung von der $0 \in K$.

2.1.2 Untervektorräume

Schon in 0.4.1 hatten wir Untervektorräume der Standardräume \mathbb{R}^n betrachtet. Im allgemeinen Fall hat man die entsprechende

Definition Sei $(V, +, \cdot)$ ein K -Vektorraum. Eine Teilmenge $W \subset V$ heißt **Untervektorraum**, wenn folgendes gilt:

UV1 $W \neq \emptyset$.

UV2 $v, w \in W \Rightarrow v + w \in W$.

UV3 $v \in W, \lambda \in K \Rightarrow \lambda v \in W$.

Die Bedingungen UV2 und UV3 bedeuten, dass W **abgeschlossen** ist unter der Addition und der Multiplikation mit Skalaren. Der Name Untervektorraum ist gerechtfertigt durch die folgende

Bemerkung Ist $W \subset V$ ein Untervektorraum, so ist er mit der aus V induzierten Addition und Multiplikation mit Skalaren selbst ein Vektorraum.

Beweis Zunächst ist W mit der Addition aus V wieder eine abelsche Gruppe: Assoziativität und Kommutativität gelten in V , somit auch in W . Da $W \neq \emptyset$ gibt es ein $v \in W$, also ist $\mathbf{o} = 0 \cdot v \in W$ und $-v = (-1) \cdot v \in W$ nach UV3. Die Regeln aus V2 gelten in V und somit auch in W . ■

Beispiel 1 Die trivialen Beispiele für Untervektorräume eines beliebigen Vektorraumes V sind $W_0 = \{\mathbf{o}\}$ und $W_1 = V$.

Beispiel 2 Im Standardraum $V = \mathbb{R}^n$ hat man die folgende Situation:

- Im \mathbb{R}^1 gibt es nur die trivialen Untervektorräume.
- Im \mathbb{R}^2 ist jede Gerade durch \mathbf{o} , d.h. $W = \mathbb{R} \cdot w$ mit $\mathbf{o} \neq w \in \mathbb{R}^2$, ein nicht trivialer Untervektorraum.

- Im \mathbb{R}^3 ist jede Gerade durch \mathbf{o} , d.h. $W = \mathbb{R} \cdot w$ mit $\mathbf{o} \neq w \in \mathbb{R}^3$, und jede Ebene durch \mathbf{o} , d.h. $W = \mathbb{R} \cdot w_1 + \mathbb{R} \cdot w_2$ mit $w_1, w_2 \in \mathbb{R}^3$ linear unabhängig, ein nicht trivialer Untervektorraum (vgl. 0.4.2).
- Im \mathbb{R}^n ist jede Lösungsmenge eines homogenen linearen Gleichungssystems ein Untervektorraum (vgl. 0.5).

Mit Hilfe von etwas mehr Theorie, insbesondere dem Begriff der „Dimension“ eines Vektorraumes wird sich zeigen, dass es im \mathbb{R}^n keine anderen als die oben angegebenen Beispiele für Untervektorräume gibt. Das gilt ganz analog für den Standardraum K^n über einem beliebigen Körper.

Ganz anders ist die Situation in

Beispiel 3 Sei $I \subset \mathbb{R}$ ein Intervall und $V := \text{Abb}(I, \mathbb{R})$ der Vektorraum aller auf I definierten reellwertigen Funktionen. Von den vielen möglichen Untervektorräumen von V seien nur einige aufgeführt:

$$\mathcal{B} := \{f \in V : f \text{ ist beschränkt}\} \subset V$$

$$\mathcal{C} := \{f \in V : f \text{ ist stetig}\} \subset V$$

$$\mathcal{I} := \{f \in V : f \text{ ist integrierbar}\} \subset V$$

$$\mathcal{D} := \{f \in V : f \text{ ist differenzierbar}\} \subset V$$

$$\mathcal{A} := \{f \in V : f \text{ ist reell-analytisch}\} \subset V$$

Dass die Bedingungen UV2 und UV3 für diese Teilmengen von V erfüllt sind, lernt man in der Analysis. Der Leser möge auch überlegen, welche Inklusionen es zwischen den angegebenen Untervektorräumen von V gibt.

Beispiel 4 Im Vektorraum $V = K[X]$ der Polynome mit Koeffizienten aus K hat man für jedes $d \in \mathbb{N}$ einen Untervektorraum

$$K[X]_d := \{f \in K[X] : \deg f \leq d\}$$

der Polynome vom Grad höchstens gleich d .

2.1.3 Operationen mit Untervektorräumen

Sind $W_1, W_2 \subset \mathbb{R}^3$ zwei verschiedene Ebenen durch \mathbf{o} , so ist $W_1 \cap W_2$ eine Gerade durch \mathbf{o} , also wieder ein Untervektorraum. Allgemein gilt:

Lemma 1 Sind $W_1, \dots, W_r \subset V$ Untervektorräume, so ist auch

$$W := W_1 \cap \dots \cap W_r \subset V$$

ein Untervektorraum.

Beweis Da \mathbf{o} in allen W_i enthalten ist, folgt $\mathbf{o} \in W$, also $W \neq \emptyset$. Sind $v, w \in W$, so folgt $v, w \in W_i$ für alle i , also $v + w \in W_i$ und $v + w \in W$. Ebenso folgt aus $\lambda \in K$ und $v \in W$, dass $\lambda v \in W$. ■

Mit den gleichen Argumenten beweist man, dass für eine beliebig große Indexmenge $I \neq \emptyset$ der Durchschnitt

$$W := \bigcap_{i \in I} W_i \subset V$$

von Untervektorräumen W_i wieder ein Untervektorraum von V ist. Ein Beispiel dafür ist etwa $V := \text{Abb}(\mathbb{R}, \mathbb{R})$, $I := \mathbb{Z}$ und

$$W_i := \{f \in V : f(i) = 0\}.$$

Dann ist $W = \{f \in V : f|_{\mathbb{Z}} = 0\}$.

Im Gegensatz zum Durchschnitt ist die Vereinigung von Untervektorräumen nur in extremen Ausnahmefällen ein Untervektorraum.

Bemerkung Seien $W, W' \subset V$ Untervektorräume derart, dass $W \cup W' \subset V$ wieder ein Untervektorraum ist. Dann folgt $W \subset W'$ oder $W' \subset W$.

Beweis Es ist zu zeigen, dass aus $W \not\subset W'$ folgt, dass $W' \subset W$ sein muss. Sei also $w' \in W'$ beliebig und $w \in W \setminus W'$. Da $w, w' \in W \cup W'$ folgt aus der Annahme, dass $W \cup W'$ ein Untervektorraum ist, $w + w' \in W \cup W'$.

Aus $w + w' \in W'$ würde $w = (w + w') - w' \in W'$ folgen. Also muss $w + w' \in W$ sein, und es folgt $w' = (w + w') - w \in W$. ■

Wir zeigen nun, dass es zu endlich vielen Untervektorräumen einen eindeutig bestimmten kleinsten Untervektorraum gibt, der die Vereinigung enthält.

Lemma 2 Seien $W_1, \dots, W_r \subset V$ Untervektorräume und

$$W := \{v_1 + \dots + v_r : v_1 \in W_1, \dots, v_r \in W_r\} \subset V$$

die Menge aller Summen von Vektoren aus W_1, \dots, W_r . Dann gilt:

- $W \subset V$ ist ein Untervektorraum.
- W ist der kleinste Untervektorraum von V , der $W_1 \cup \dots \cup W_r$ enthält.

Beweis a) $W \neq \emptyset$, denn $\mathbf{o} = \mathbf{o} + \dots + \mathbf{o} \in W$. Aus

$$v = v_1 + \dots + v_r \in W, \quad w = w_1 + \dots + w_r \in W \quad \text{und} \quad \lambda \in K$$

folgt $v + w = (v_1 + w_1) + \dots + (v_r + w_r) \in W$ und $\lambda v = \lambda v_1 + \dots + \lambda v_r \in W$.

b) Ist $W' \subset V$ ein Untervektorraum mit $W_1 \cup \dots \cup W_r \subset W'$, so muss mit

$$v_1 \in W_1, \dots, v_r \in W_r \text{ auch } v_1 + \dots + v_r \in W' \text{ sein.}$$

Also folgt $W \subset W'$. ■

Mit den Bezeichnungen wie oben kann man

$$W_1 + \dots + W_r := W$$

als die **Summe** von W_1, \dots, W_r bezeichnen. Wie in Teil b) gezeigt, ist $W_1 + \dots + W_r$ der Durchschnitt aller Untervektorräume $W' \subset V$ mit $W_1 \cup \dots \cup W_r \subset W'$.

Eine Variante des gerade behandelten Problems ist folgende:

Gegeben Vektoren $v_1, \dots, v_m \in V$, wobei $m \in \mathbb{N}^*$. Gesucht ist der kleinste Untervektorraum $W \subset V$, der v_1, \dots, v_m enthält. Entscheidendes Hilfsmittel ist folgendes: Ein Vektor $v \in V$ heißt **Linearkombination** von v_1, \dots, v_m , wenn es $\lambda_1, \dots, \lambda_m \in K$ gibt so dass

$$v = \lambda_1 v_1 + \dots + \lambda_m v_m.$$

Offensichtlich ist ein Untervektorraum $W \subset V$ abgeschlossen unter Linearkombinationen, d.h. für

$$v_1, \dots, v_m \in W \quad \text{und} \quad \lambda_1, \dots, \lambda_m \in K \quad \text{gilt} \quad \lambda_1 v_1 + \dots + \lambda_m v_m \in W.$$

Die Menge

$$\text{Span}_K(v_1, \dots, v_m) := \{\lambda_1 v_1 + \dots + \lambda_m v_m : \lambda_1, \dots, \lambda_m \in K\}$$

aller Linearkombinationen von v_1, \dots, v_m heißt der von v_1, \dots, v_m **aufgespannte** Raum. Diese Bezeichnung ist gerechtfertigt durch den

Satz In einem K -Vektorraum V seien $v_1, \dots, v_m \in V$ gegeben. Dann gilt

a) $W := \text{Span}_K(v_1, \dots, v_m) \subset V$ ist Untervektorraum.

b) W ist der kleinste Untervektorraum von V , der v_1, \dots, v_m enthält.

Beweis a) Aus $v = \sum_{i=1}^m \lambda_i v_i \in W$ und $w = \sum_{i=1}^m \mu_i v_i \in W$ folgt

$$v + w = \sum_{i=1}^m (\lambda_i + \mu_i) v_i \in W.$$

Außerdem gilt $\lambda v = \lambda \sum_{i=1}^m \lambda_i v_i = \sum_{i=1}^m (\lambda \lambda_i) v_i \in W$.

b) $v_i = 0 \cdot v_1 + \dots + 0 \cdot v_{i-1} + 1 \cdot v_i + 0 \cdot v_{i+1} + \dots + 0 \cdot v_m \in W$.

Ist $W' \subset V$ ein Untervektorraum mit $v_1, \dots, v_m \in W'$, dann ist jede Linearkombination von v_1, \dots, v_m und somit auch W in W' enthalten. ■

Man kann auch noch den Fall $m = 0$ zulassen und formal

$$\text{Span}_K(\emptyset) := \{\mathbf{o}\}$$

setzen.

2.1.4 Lineare Unabhängigkeit

Nach Definition hat jeder Vektor $v \in \text{Span}_K(v_1, \dots, v_n) \subset V$ eine Darstellung als Linearkombination

$$v = \lambda_1 v_1 + \dots + \lambda_n v_n \quad \text{mit} \quad \lambda_1, \dots, \lambda_n \in K.$$

Sehr wichtig ist die Frage, ob die Skalare $\lambda_1, \dots, \lambda_n$ durch v eindeutig bestimmt sind. Dann kann man nämlich v weitgehend ersetzen durch das n -Tupel $(\lambda_1, \dots, \lambda_n) \in K^n$, denn die Abbildung

$$K^n \rightarrow \text{Span}_K(v_1, \dots, v_n), (\lambda_1, \dots, \lambda_n) \mapsto \lambda_1 v_1 + \dots + \lambda_n v_n,$$

ist dann nicht nur surjektiv, sondern auch injektiv und somit bijektiv. Das wird sich als höchst nützlich erweisen, denn mit den Vektoren im K^n kann man einfacher rechnen als in einem beliebigen V .

An dieser Stelle sieht man auch, dass es wichtig sein kann, die Vektoren v_1, \dots, v_n in einer festen Reihenfolge anzugeben.

Wir beginnen mit dem Nullvektor $v = \mathbf{o}$, er hat die sogenannte *triviale Darstellung*

$$\mathbf{o} = 0 \cdot v_1 + \dots + 0 \cdot v_n.$$

Es kann aber auch andere Darstellungen geben. Ist etwa $v_1 = \mathbf{o}$, so ist

$$\mathbf{o} = 1 \cdot v_1 + 0 \cdot v_2 + \dots + 0 \cdot v_n. \quad (1)$$

Im Fall $n \geq 2$ und $v_2 = \lambda v_1$ ist

$$\mathbf{o} = -\lambda v_1 + 1 \cdot v_2 + 0 \cdot v_3 + \dots + 0 \cdot v_n. \quad (2)$$

(1) und (2) sind nicht triviale Darstellungen des Nullvektors, da jeweils ein Skalar $1 \neq 0$ auftritt. Die Frage, ob der Nullvektor eindeutig darstellbar ist, ist Grundlage für die folgende

Definition Ein n -Tupel (v_1, \dots, v_n) von Vektoren aus einem K -Vektorraum V heißt *linear unabhängig*, wenn aus

$$\mathbf{o} = \lambda_1 v_1 + \dots + \lambda_n v_n \quad \text{folgt, dass} \quad \lambda_1 = \dots = \lambda_n = 0 \in K.$$

Anders ausgedrückt: Der Nullvektor hat nur die triviale Darstellung.

Das n -Tupel (v_1, \dots, v_n) heißt *linear abhängig*, wenn es nicht linear unabhängig ist, d.h. wenn es eine nicht triviale Darstellung des Nullvektors gibt.

Da eine Summe unabhängig von der Reihenfolge der Summanden ist, hängt auch die lineare Unabhängigkeit eines n -Tupels (v_1, \dots, v_n) nicht von der Reihenfolge ab. Ein einziger Vektor v ist nach der Rechenregel c) aus 2.1.1 genau dann linear unabhängig, wenn $v \neq \mathbf{o}$.

Beispiel 1 In $V = \mathbb{R}^3$ betrachten wir die zwei Vektoren $v_1 = (1, 2, 3)$ und $v_2 = (4, 5, 6)$. Die Bedingung

$$\lambda_1 \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + \lambda_2 \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

ergibt drei lineare Gleichungen für λ_1, λ_2 :

$$\begin{aligned} \lambda_1 + 4\lambda_2 &= 0 \\ 2\lambda_1 + 5\lambda_2 &= 0 \\ 3\lambda_1 + 6\lambda_2 &= 0 \end{aligned} \quad \text{mit der Matrix } A = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}.$$

Durch elementare Zeilenumformungen von A erhält man

$$\tilde{A} = \begin{pmatrix} 1 & 4 \\ 0 & -3 \\ 0 & 0 \end{pmatrix},$$

also $\lambda_1 + 4\lambda_2 = 0$ und $-3\lambda_2 = 0$. Daraus folgt $\lambda_2 = 0$ und $\lambda_1 = 0$, also ist (v_1, v_2) linear unabhängig. Somit ist $\text{Span}_{\mathbb{R}}(v_1, v_2) \subset \mathbb{R}^3$ eine Ebene durch \mathbf{o} .

Beispiel 2 In $V = \mathbb{R}^3$ betrachten wir die drei Vektoren

$$v_1 = (1, 2, 3), v_2 = (4, 5, 6), v_3 = (7, 8, 9).$$

Die Bedingung $\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 = \mathbf{o}$ ergibt drei lineare Gleichungen für $\lambda_1, \lambda_2, \lambda_3$:

$$\begin{aligned} \lambda_1 + 4\lambda_2 + 7\lambda_3 &= 0 \\ 2\lambda_1 + 5\lambda_2 + 8\lambda_3 &= 0 \\ 3\lambda_1 + 6\lambda_2 + 9\lambda_3 &= 0 \end{aligned} \quad \text{mit der Matrix } A = \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix}.$$

Daraus erhält man

$$\tilde{A} = \begin{pmatrix} 1 & 4 & 7 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix},$$

also $\lambda_1 + 4\lambda_2 + 7\lambda_3 = 0$ und $3\lambda_2 + 6\lambda_3 = 0$. Nach den Regeln aus 0.5.3 kann man $\lambda_3 = 1$ setzen, dann folgt $\lambda_2 = -2$ und $\lambda_1 = 1$. Also ist $v_1 - 2v_2 + v_3 = \mathbf{o}$ und (v_1, v_2, v_3) ist linear abhängig. Weiter folgt

$$v_3 = 2v_2 - v_1, \quad \text{also} \quad \text{Span}_{\mathbb{R}}(v_1, v_2, v_3) = \text{Span}_{\mathbb{R}}(v_1, v_2).$$

In der Spalte j_1 : $\lambda_1 a_{1j_1} = 0$, also $\lambda_1 = 0$ da $a_{1j_1} \neq 0$.

In der Spalte j_2 : $\lambda_2 a_{2j_2} = 0$, da $\lambda_1 = 0$, also $\lambda_2 = 0$ da $a_{2j_2} \neq 0$.

⋮

In der Spalte j_r : $\lambda_r a_{rj_r} = 0$, da $\lambda_1 = \dots = \lambda_{r-1} = 0$, also $\lambda_r = 0$ da $a_{rj_r} \neq 0$.

Insgesamt folgt also $\lambda_1 = \dots = \lambda_r = 0$.

Diese Tatsache wird sich noch öfters als nützlich erweisen. Ganz analog kann man zeigen, dass die r Pivotspalten linear unabhängig sind.

Beispiel 6 Sind $v_1, v_2 \in \mathbb{R}^n$ von \mathbf{o} verschieden und senkrecht aufeinander, so sind sie auch linear unabhängig.

Die Annahme $\lambda_1 v_1 + \lambda_2 v_2 = \mathbf{o}$ wird skalar mit v_1 multipliziert. Das ergibt

$$0 = \langle v_1, \lambda_1 v_1 + \lambda_2 v_2 \rangle = \lambda_1 \langle v_1, v_1 \rangle + \lambda_2 \langle v_1, v_2 \rangle.$$

Da $\langle v_1, v_1 \rangle \neq 0$ und $\langle v_1, v_2 \rangle = 0$ folgt $\lambda_1 = 0$. Analog erhält man durch skalare Multiplikation mit v_2 , dass $\lambda_2 = 0$.

Analog zeigt man, dass von \mathbf{o} verschiedene paarweise senkrechte Vektoren v_1, \dots, v_m im \mathbb{R}^n linear unabhängig sind.

Beispiel 7 Im Vektorraum $V = \mathbb{R}[X]$ der Polynome mit reellen Koeffizienten betrachten wir für beliebiges $n \in \mathbb{N}$ die *Monome*

$$X^0 = 1, X^1 = X, X^2, \dots, X^n.$$

Die Bedingung $\lambda_0 + \lambda_1 X + \dots + \lambda_n X^n = \mathbf{o}$ bedeutet, dass dieses Polynom das Nullpolynom ist. Ein Polynom

$$f = a_0 + a_1 X + \dots + a_n X^n$$

ist aber genau dann das Nullpolynom, wenn $a_0 = a_1 = \dots = a_n = 0$. Also folgt

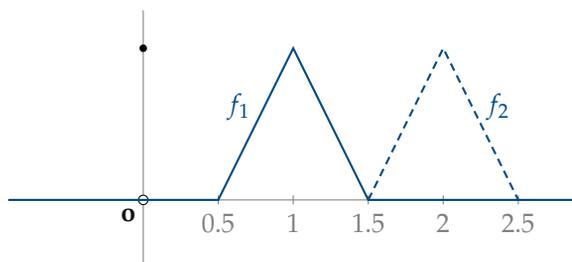
$$\lambda_0 = \lambda_1 = \dots = \lambda_n = 0,$$

d.h. (X^0, X^1, \dots, X^n) ist linear unabhängig.

Man beachte, dass bei diesem Nachweis ein Polynom als formaler Ausdruck und nicht als eine Funktion behandelt wird.

Beispiel 8 Im Vektorraum $\mathcal{C}(\mathbb{R}, \mathbb{R})$ der stetigen Funktionen betrachten wir spezielle „Hütchenfunktionen“ f_1, \dots, f_n . Dabei ist f_1 gegeben durch

$$f_1(x) := \begin{cases} 0 & \text{für } x \leq 0.5, \\ 2x - 1 & \text{für } 0.5 \leq x \leq 1, \\ -2x + 3 & \text{für } 1 \leq x \leq 1.5, \\ 0 & \text{für } x \geq 1.5, \end{cases}$$



und allgemein

$$f_k(x) := \begin{cases} 0 & \text{für } x \leq k - 0.5, \\ 2x - 2k + 1 & \text{für } k - 0.5 \leq x \leq k, \\ -2x + 2k + 1 & \text{für } k \leq x \leq k + 0.5, \\ 0 & \text{für } x \geq k + 0.5. \end{cases}$$

Offensichtlich ist f_k stetig mit $f_k(k) = 1$.

Wir behaupten nun, dass (f_1, \dots, f_n) für beliebiges $n \in \mathbb{N}^*$ linear unabhängig ist.

Angenommen $\lambda_1 f_1 + \dots + \lambda_n f_n = \mathbf{o}$, wobei die Null rechts die Nullfunktion mit $\mathbf{o}(x) = 0 \in \mathbb{R}$ für alle $x \in \mathbb{R}$ bezeichnet. Dann gilt

$$\lambda_1 f_1(x) + \dots + \lambda_n f_n(x) = 0 \in \mathbb{R}$$

für alle $x \in \mathbb{R}$. Setzt man $x = 1$ ein, so folgt $\lambda_1 \cdot 1 + 0 + \dots + 0 = 0$, also $\lambda_1 = 0$, denn $f_2(1) = \dots = f_n(1) = 0$. Analog folgt $\lambda_2 = \dots = \lambda_n = 0$.

Beispiel 9 Die Funktionen $1, \cos, \sin$ aus dem Vektorraum aller auf ganz \mathbb{R} analytischen Funktionen sind linear unabhängig. Denn angenommen

$$\lambda_1 \cdot 1 + \lambda_2 \cdot \cos + \lambda_3 \cdot \sin = \mathbf{o}.$$

Diese Relation zwischen Funktionen bedeutet, dass

$$\lambda_1 \cdot 1 + \lambda_2 \cdot \cos x + \lambda_3 \cdot \sin x = 0$$

für alle $x \in \mathbb{R}$. Nun genügt es, für x geeignete Werte einzusetzen:

$$\begin{aligned} x = 0: & \quad \lambda_1 \cdot 1 + \lambda_2 \cdot 1 + \lambda_3 \cdot 0 = 0 \\ x = \frac{\pi}{2}: & \quad \lambda_1 \cdot 1 + \lambda_2 \cdot 0 + \lambda_3 \cdot 1 = 0 \\ x = \pi: & \quad \lambda_1 \cdot 1 + \lambda_2 \cdot (-1) + \lambda_3 \cdot 0 = 0 \end{aligned}$$

Das ergibt ein homogenes lineares Gleichungssystem für $\lambda_1, \lambda_2, \lambda_3$ mit der Koeffizientenmatrix

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix}, \quad \text{umgeformt auf} \quad \begin{pmatrix} 1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

Also ist $\lambda_1 = \lambda_2 = \lambda_3 = 0$ die einzige Lösung.

Ganz analog kann man zeigen, dass die Funktionen $1, \sin x, \sin 2x$ linear unabhängig sind.

Beispiel 10 Ein allgemeineres Beispiel für linear unabhängige differenzierbare Funktionen erhält man mit einfachen Hilfsmitteln der Analysis. Sind $\alpha_1, \dots, \alpha_n \in \mathbb{R}$ beliebige paarweise verschiedene Zahlen, so sind die Funktionen

$$e^{\alpha_1 x}, e^{\alpha_2 x}, \dots, e^{\alpha_n x}$$

linear unabhängig. Das kann man durch Induktion über n beweisen. Der Fall $n = 1$ ist klar, denn $e^{\alpha_1 x} \neq \mathbf{0}$ für beliebiges $\alpha_1 \in \mathbb{R}$. Sei also

$$\lambda_1 e^{\alpha_1 x} + \dots + \lambda_{n-1} e^{\alpha_{n-1} x} + \lambda_n e^{\alpha_n x} = \mathbf{0} \quad (*)$$

mit $\lambda_1, \dots, \lambda_n \in \mathbb{R}$. Da $e^{-\alpha_n x} \neq 0$ für alle $x \in \mathbb{R}$ kann man (*) mit diesem Faktor multiplizieren, das ergibt

$$\lambda_1 e^{(\alpha_1 - \alpha_n)x} + \dots + \lambda_{n-1} e^{(\alpha_{n-1} - \alpha_n)x} + \lambda_n = \mathbf{0}. \quad (**)$$

Differenziert man (**), so folgt

$$(\alpha_1 - \alpha_n) \lambda_1 e^{(\alpha_1 - \alpha_n)x} + \dots + (\alpha_{n-1} - \alpha_n) \lambda_{n-1} e^{(\alpha_{n-1} - \alpha_n)x} = \mathbf{0}.$$

Da auch die Faktoren $(\alpha_1 - \alpha_n), \dots, (\alpha_{n-1} - \alpha_n)$ paarweise verschieden sind, folgt aus der Induktionsannahme

$$(\alpha_1 - \alpha_n) \lambda_1 = \dots = (\alpha_{n-1} - \alpha_n) \lambda_{n-1} = 0.$$

Da die Faktoren $(\alpha_1 - \alpha_n), \dots, (\alpha_{n-1} - \alpha_n)$ von Null verschieden sind, muss

$$\lambda_1 = \dots = \lambda_{n-1} = 0$$

sein. Aus (**) folgt dann auch $\lambda_n = 0$.

Insbesondere folgt, dass die Funktionen $1, e^x, e^{2x}, \dots, e^{nx}$ für jedes $n \in \mathbb{N}$ linear unabhängig sind. Um einen Beweis durch Induktion zu ermöglichen, ist es von Vorteil, zunächst die allgemeinere Aussage zu beweisen.

Beispiel 11 Der Körper \mathbb{R} ist ein Vektorraum über dem Körper \mathbb{Q} . Die „Vektoren“ $1, \sqrt{2} \in \mathbb{R}$ sind über \mathbb{Q} linear unabhängig. Denn angenommen es ist

$$\lambda_1 \cdot 1 + \lambda_2 \cdot \sqrt{2} = \mathbf{0} = 0 \quad \text{mit } \lambda_1, \lambda_2 \in \mathbb{Q}.$$

Wäre $\lambda_2 \neq 0$, so würde $\sqrt{2} = -\frac{\lambda_1}{\lambda_2} \in \mathbb{Q}$ folgen. Das ist ein Widerspruch zur Bemerkung aus 0.1.1. Aus $\lambda_2 = 0$ folgt aber $\lambda_1 \cdot 1 = 0$, also $\lambda_1 = 0$.

Nach diesen Beispielen geben wir noch etwas andersartige Charakterisierungen von linearer Unabhängigkeit und Abhängigkeit.

Lemma 1 Ein n -Tupel (v_1, \dots, v_n) aus einem K -Vektorraum V ist genau dann linear unabhängig, wenn jedes $v \in \text{Span}_K(v_1, \dots, v_n)$ eine eindeutige Darstellung als Linearkombination

$$v = \lambda_1 v_1 + \dots + \lambda_n v_n$$

besitzt.

Beweis Wenn jedes v eine eindeutige Darstellung besitzt, dann auch $v = \mathbf{o}$. Das bedeutet aber die lineare Unabhängigkeit.

Die umgekehrte Richtung besagt, dass aus der Eindeutigkeit bei $v = \mathbf{o}$ die Eindeutigkeit für beliebige v folgt; das muss man nachrechnen. Sei also $v \in V$ und

$$v = \lambda_1 v_1 + \dots + \lambda_n v_n = \mu_1 v_1 + \dots + \mu_n v_n.$$

Bildet man die Differenz, so folgt

$$\mathbf{o} = (\lambda_1 - \mu_1)v_1 + \dots + (\lambda_n - \mu_n)v_n.$$

Wegen der linearen Unabhängigkeit folgt $\lambda_i - \mu_i = 0$, also $\lambda_i = \mu_i$ für $i = 1, \dots, n$. ■

Lemma 2 Ein n -Tupel (v_1, \dots, v_n) aus einem K -Vektorraum V ist genau dann linear abhängig, wenn mindestens einer der Vektoren Linearkombination der anderen ist, d.h. es gibt mindestens ein $i \in \{1, \dots, n\}$, so dass

$$v_i \in \text{Span}_K(v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n).$$

Beweis Ist (v_1, \dots, v_n) linear abhängig, so gibt es eine Darstellung

$$\mathbf{o} = \lambda_1 v_1 + \dots + \lambda_n v_n$$

mit mindestens einem $\lambda_i \neq 0$. Zur Vereinfachung der Schreibweise nehmen wir $i = 1$ an. Dann folgt

$$v_1 = -\frac{\lambda_2}{\lambda_1} v_2 - \dots - \frac{\lambda_n}{\lambda_1} v_n,$$

also $v_1 \in \text{Span}_K(v_2, \dots, v_n)$.

Setzen wir umgekehrt $v_1 \in \text{Span}_K(v_2, \dots, v_n)$ voraus, so folgt

$$v_1 = \lambda_2 v_2 + \dots + \lambda_n v_n \quad \text{also} \quad \mathbf{o} = 1 \cdot v_1 - \lambda_2 v_2 - \dots - \lambda_n v_n.$$

Also ist (v_1, \dots, v_n) linear abhängig. ■

Nach Lemma 2 ist also (v_1, \dots, v_n) genau dann linear unabhängig, wenn kein v_i Linearkombination der anderen ist. Diese Bedingung erscheint plausibler als die Definition, sie ist aber in Beweisen schlechter zu handhaben. Die oben ausgeführten Beispiele sind eine erste Bestätigung dafür.

2.2 Basis und Dimension

2.2.1 Erzeugendensysteme und Basen

Nachdem wir den Unterschied zwischen linearer Abhängigkeit und Unabhängigkeit erläutert haben, kann man nun ein Maß für die „Größe“ eines Vektorraums angeben, die „Dimension“. Die dazu erforderlichen technischen Details hatte schon H. GRASSMANN in seiner Ausdehnungslehre [GR] beschrieben. Aber das war ziemlich unbeachtet geblieben. Erst um 1930 wurde in der Göttinger Schule der Algebra daran angeknüpft, etwa von SCHREIER-SPERNER [S-S]. Zunächst benötigt man den entscheidenden Begriff der Basis, wir beschränken uns hier auf den endlichen Fall.

Definition Ist V ein K -Vektorraum, so heißt ein n -Tupel $\mathcal{B} = (v_1, \dots, v_n)$ von Vektoren aus V eine endliche **Basis** von V über K , wenn folgendes gilt:

B1 $\text{Span}_K(v_1, \dots, v_n) = V$.

B2 (v_1, \dots, v_n) ist linear unabhängig.

Nach Lemma 1 aus 2.1.4 kann man die beiden Bedingungen B1 und B2 ersetzen durch

B Jedes $v \in V$ hat eine eindeutige Darstellung $v = \lambda_1 v_1 + \dots + \lambda_n v_n$ mit $\lambda_1, \dots, \lambda_n \in K$.

Anders ausgedrückt bedeutet das, dass die Abbildung

$$K^n \rightarrow V, (\lambda_1, \dots, \lambda_n) \mapsto \lambda_1 v_1 + \dots + \lambda_n v_n,$$

bijektiv ist. Es wird sich zeigen, dass man dann V weitgehend ersetzen kann durch den K^n , in dem man besonders einfach rechnen kann.

Folgende weitere Namen sind üblich und nützlich als abkürzende Redeweisen:

Man nennt das n -Tupel (v_1, \dots, v_n) ein endliches **Erzeugendensystem** von V , wenn $\text{Span}_K(v_1, \dots, v_n) = V$.

V heißt **endlich erzeugt**, wenn es ein endliches Erzeugendensystem von V gibt.

Standardbeispiel ist der Vektorraum K^n : Die n Vektoren

$$e_1 = (1, 0, \dots, 0), \dots, e_i = (0, \dots, 0, 1, 0, \dots, 0), \dots, e_n = (0, \dots, 0, 1)$$

sind ein linear unabhängiges Erzeugendensystem. Man nennt $\mathcal{K} := (e_1, \dots, e_n)$ die **kanonische Basis** oder **Standardbasis** von K^n .

Da wir hier nur endliche Basen betrachten, werden wir zur Abkürzung im folgenden nur von einer Basis sprechen. In dieser Sprechweise ist eine Basis dann ein linear unabhängiges Erzeugendensystem.

Ist $\mathcal{B} = (v_1, \dots, v_n)$ eine Basis von V , so nennt man die Zahl n die *Länge* der Basis. Dabei ist $n \in \mathbb{N}$; für $n = 0$ spricht man von der leeren Basis. In diesem Fall ist

$$V = \text{Span}_K(\emptyset) = \{\mathbf{o}\}$$

der Nullvektorraum. Nun ist es naheliegend, als „Dimension“ von V die Länge einer Basis von V zu erklären. Dabei treten zwei entscheidende Fragen auf:

- 1) Hat jeder Vektorraum V eine endliche Basis?
- 2) Haben je zwei endliche Basen von V gleiche Länge?

Frage 2) werden wir anschließend positiv beantworten.

Aus Bedingung B1 folgt, dass V endlich erzeugt ist. Eine negative Antwort auf Frage 1) ergibt sich somit aus den folgenden Beispielen.

Beispiel 1 Der Vektorraum $K[X]$ der Polynome ist nicht endlich erzeugt.

Beweis Es genügt zu zeigen, dass für endlich viele Polynome f_1, \dots, f_n stets

$$\text{Span}_K(f_1, \dots, f_n) \subsetneq K[X].$$

Wir können $n \geq 1$ und $f_i \neq 0$ für alle i annehmen. Jedes Polynom f_i hat einen Grad $d_i \in \mathbb{N}$, wir setzen $d := \max\{d_1, \dots, d_n\}$. Ist

$$f := \lambda_1 f_1 + \dots + \lambda_n f_n \in \text{Span}_K(f_1, \dots, f_n),$$

so ist offensichtlich der Grad von f höchstens gleich d . Alle Polynome höheren Grades können keine Linearkombination von f_1, \dots, f_n sein. ■

Beispiel 2 Der Vektorraum \mathbb{R} ist über \mathbb{Q} nicht endlich erzeugt.

Beweis Angenommen es gäbe $x_1, \dots, x_n \in \mathbb{R}$ so dass

$$\mathbb{R} = \text{Span}_{\mathbb{Q}}(x_1, \dots, x_n).$$

Dann wäre die Abbildung

$$\mathbb{Q}^n \rightarrow \mathbb{R}, (\lambda_1, \dots, \lambda_n) \mapsto \lambda_1 x_1 + \dots + \lambda_n x_n$$

surjektiv. Das ergibt einen Widerspruch zum Satz aus 1.1.4, denn mit \mathbb{Q} ist auch \mathbb{Q}^n abzählbar; \mathbb{R} ist dagegen überabzählbar. ■

Nach der Definition einer Basis ist jeder Vektorraum mit endlicher Basis auch endlich erzeugt. Umgekehrt zeigen wir nun, dass jeder endlich erzeugte Vektorraum auch eine endliche Basis besitzt. Das ist eine eingeschränkt positive Antwort auf die oben formulierte Frage 1). Genauer gilt:

Basis-Auswahlsatz *Ist V ein K -Vektorraum und gilt*

$$V = \text{Span}_K(v_1, \dots, v_n),$$

so gibt es ein $m \in \mathbb{N}$ mit $0 \leq m \leq n$ und Indizes $i_1, \dots, i_m \in \{1, \dots, n\}$ derart, dass

$$\mathcal{B} := (v_{i_1}, \dots, v_{i_m})$$

eine Basis von V ist.

Will man Doppelindizes vermeiden, so kann man die Nummerierung so gewählt denken, dass $i_1 = 1, \dots, i_m = m$. Dann ist

$$\mathcal{B} := (v_1, \dots, v_m)$$

eine Basis von V .

Aus dem Basis-Auswahlsatz folgt sofort das

Korollar *Jeder endlich erzeugte Vektorraum hat eine endliche Basis.* ■

Beweis des Basis-Auswahlsatzes Ist (v_1, \dots, v_n) linear unabhängig, so ist $m = n$.

Ist (v_1, \dots, v_n) linear abhängig, so ist nach Lemma 2 aus 2.1.4 einer, etwa v_n , Linearkombination der anderen, also

$$\text{Span}_K(v_1, \dots, v_n) = \text{Span}_K(v_1, \dots, v_{n-1}) = V.$$

Nun prüft man nach, ob (v_1, \dots, v_{n-1}) linear unabhängig ist. Wenn ja ist man fertig, andernfalls kann man

$$\text{Span}_K(v_1, \dots, v_{n-2}) = V$$

annehmen. Diese Iteration führt nach höchstens n Schritten zum Ziel. Denn ist man bei $\text{Span}_K(v_1) = V$ angekommen, so ist $v_1 \neq \mathbf{o}$ oder $v_1 = \mathbf{o}$. Im ersten Fall ist $m = 1$, im zweiten $m = 0$ und

$$\text{Span}_K(\emptyset) = \{\mathbf{o}\}. \quad \blacksquare$$

Ist $V = \text{Span}_K(v_1, \dots, v_n) \subset K^N$, so kann man in jedem Schritt durch Lösung eines linearen Gleichungssystems entscheiden, ob die verbliebenen Vektoren linear unabhängig sind.

In Beispiel 2 aus 2.1.4 mit $v_1, v_2, v_3 \in \mathbb{R}^3$ hatten wir $v_1 - 2v_2 + v_3 = \mathbf{o}$ erhalten. Also kann man bei $V = \text{Span}_{\mathbb{R}}(v_1, v_2, v_3)$ jeden der drei Vektoren weglassen; die beiden verbleibenden bilden eine Basis von V .

Im Abschnitt 2.2.4 beschreiben wir ein Verfahren mit weniger Rechenaufwand, bei dem allerdings im allgemeinen andere Vektoren w_1, \dots, w_m bestimmt werden, so dass (w_1, \dots, w_m) eine Basis von V ist.

2.2.2 Dimension eines Vektorraums

Nun zum zweiten Problem, bei dem die Längen verschiedener Basen verglichen werden. Dazu verwendet man ein schon von GRASSMANN [GR] angegebenes und von STEINITZ [ST] später wieder beschriebenes Verfahren des Austauschs von Vektoren. Daher wird das folgende Ergebnis oft als Satz von STEINITZ bezeichnet.

Basis-Austauschsatz *Im K -Vektorraum V seien eine Basis $\mathcal{B} = (v_1, \dots, v_n)$ sowie ein linear unabhängiges System (w_1, \dots, w_m) gegeben. Dann muss $m \leq n$ sein, und man kann $i_1, \dots, i_m \in \{1, \dots, n\}$ finden, so dass in der Basis v_{i_1}, \dots, v_{i_m} durch w_1, \dots, w_m ersetzt werden können.*

Ist die Nummerierung so gewählt, dass $i_1 = 1, \dots, i_m = m$, so ist

$$\mathcal{B}' := (w_1, \dots, w_m, v_{m+1}, \dots, v_n)$$

wieder eine Basis von V .

Man beachte, dass die Ungleichung $m \leq n$ keineswegs selbstverständlich ist. Im K^n hat man die kanonische Basis (e_1, \dots, e_n) . Also kann es nach dem Austauschsatz höchstens n linear unabhängige Vektoren in K^n geben. Im \mathbb{R}^2 oder \mathbb{R}^3 ist das geometrisch klar. Aber bei 1001 Vektoren im \mathbb{R}^{1000} gibt es kein anschauliches Argument für die lineare Abhängigkeit.

Wir vermerken zunächst die wichtigste Folgerung:

Korollar 1 *Je zwei endliche Basen eines Vektorraums haben gleiche Länge.*

Beweis des Korollars Sind $\mathcal{B} = (v_1, \dots, v_n)$ und $\mathcal{B}' = (w_1, \dots, w_m)$ Basen von V , so kann man den Austauschsatz in beiden Richtungen anwenden. Es folgt $m \leq n$ und $n \leq m$, also $m = n$. ■

Mit Hilfe von Korollar 1 kann man nun die Idee für die Definition der „Dimension“ eines Vektorraumes als Länge einer Basis umsetzen.

Definition Sei V ein K -Vektorraum. Ist V endlich erzeugt, so gibt es nach dem Basisauswahlsatz in 2.2.1 eine endliche Basis $\mathcal{B} = (v_1, \dots, v_n)$ und man definiert die **Dimension** von V über K als

$$\dim_K V := \text{Länge von } \mathcal{B} = n.$$

Ist V nicht endlich erzeugt, so setzt man formal $\dim_K V := \infty$.

Ist klar, welches K gemeint ist, schreibt man kürzer \dim statt \dim_K .

Eine weitere direkte Folgerung aus dem Austauschatz ist

Korollar 2 Gibt es für jedes $m \in \mathbb{N}$ linear unabhängige Vektoren $w_1, \dots, w_m \in V$, so ist $\dim V = \infty$. ■

Beispiel 1 Im K^n hat man die kanonische Basis $\mathcal{K} = (e_1, \dots, e_n)$, also ist

$$\dim_K K^n = n.$$

Das scheint ziemlich selbstverständlich. Aber es gibt natürlich viele andere Basen des K^n und es ist keinesfalls offensichtlich, dass sie alle auch die Länge n haben.

Beispiel 2 Wir betrachten die Körper $\mathbb{R} \subset \mathbb{C}$. Als \mathbb{R} -Vektorraum hat \mathbb{C} die Basis $(1, i)$, also ist $\dim_{\mathbb{R}} \mathbb{C} = 2$. Dagegen ist $\dim_{\mathbb{C}} \mathbb{C} = \dim_{\mathbb{C}} \mathbb{C}^1 = 1$.

Beispiel 3 Für $\mathbb{Q} \subset \mathbb{R}$ ist $\dim_{\mathbb{Q}} \mathbb{R} = \infty$, denn nach Beispiel 2 aus 2.2.1 ist \mathbb{R} über \mathbb{Q} nicht endlich erzeugt.

Beispiel 4 Für den Vektorraum $K[X]$ der Polynome mit Koeffizienten aus dem Körper K gilt

$$\dim_K K[X] = \infty.$$

Das folgt sofort aus Beispiel 1 von 2.2.1, denn eine endliche Basis muss insbesondere ein endliches Erzeugendensystem sein. ■

Beispiel 5 Für den Vektorraum $\mathcal{C}(\mathbb{R}, \mathbb{R})$ der stetigen Funktionen $f : \mathbb{R} \rightarrow \mathbb{R}$ gilt

$$\dim_{\mathbb{R}} \mathcal{C}(\mathbb{R}, \mathbb{R}) = \infty.$$

Das kann man leicht aus Beispiel 4 folgern, denn Polynome sind stetige Funktionen. Ein anderes Argument erhält man mit den in Beispiel 8 aus 2.1.4 benutzten stetigen Funktionen f_k : Angenommen, es gäbe eine endliche Basis (g_1, \dots, g_n) von $\mathcal{C}(\mathbb{R}, \mathbb{R})$ über \mathbb{R} . Die Funktionen (f_1, \dots, f_{n+1}) aus $\mathcal{C}(\mathbb{R}, \mathbb{R})$ sind nach obigem Beispiel linear unabhängig; das ergibt sofort einen Widerspruch zum Basis-Austauschsatz. ■

Bevor wir den Austauschatz beweisen, geben wir noch eine weitere Folgerung an, die sehr nützlich ist für die Konstruktion von Basen.

Basis-Ergänzungssatz Ist der K -Vektorraum V endlich erzeugt und (w_1, \dots, w_m) in V linear unabhängig, so gibt es Vektoren v_{m+1}, \dots, v_n in V derart, dass

$$\mathcal{B} := (w_1, \dots, w_m, v_{m+1}, \dots, v_n)$$

eine Basis von V ist.

Beweis des Basis-Ergänzungssatzes Da V endlich erzeugt ist, gibt es ein Erzeugendensystem (v_1, \dots, v_N) . Nach dem Basis-Auswahlsatz kann man ein $n \leq N$ finden so dass

$$\mathcal{B} = (v_1, \dots, v_n) \text{ Basis von } V \text{ ist.}$$

Damit folgt die Behauptung durch Anwendung des Basis-Austauschsatzes. ■

Beispiel 6 Sei $V = \mathbb{R}^2$, $m = 1$ und $w_1 = (x_1, x_2) \neq (0, 0)$.

Ist $x_1 \neq 0$ und $x_2 \neq 0$, so kann man $v = e_1$ oder $v = e_2$ wählen; in jedem Fall ist (w_1, v) eine Basis von \mathbb{R}^2 .

Im Fall $x_1 = 0$ geht es mit $v = e_1$, im Fall $x_2 = 0$ mit $v = e_2$.

Beispiel 7 Sei allgemeiner $V = K^n$, $0 \leq m \leq n$ und $k := n - m$. Dann kann man zu linear unabhängigem (w_1, \dots, w_m) nach dem Basis-Ergänzungssatz Indizes i_1, \dots, i_k finden, so dass

$$\mathcal{B} := (w_1, \dots, w_m, e_{i_1}, \dots, e_{i_k})$$

eine Basis von K^n wird. Wie man geeignete Indizes i_1, \dots, i_k aus den w_1, \dots, w_m durch Rechnung erhalten kann, wird in 2.2.4 erläutert.

Beispiel 8 Im \mathbb{R}^3 ist zu linear unabhängigen Vektoren w_1, w_2 eine Basis gegeben durch

$$\mathcal{B} := (w_1, w_2, w_1 \times w_2)$$

Man benutze dabei Lemma 2 aus 0.3.7.

Beim *Beweis des Basis-Austauschsatzes* werden schrittweise einzelne Vektoren ausgetauscht. Wie ein einzelner Schritt aussieht wird geregelt durch das

Austauschlemma Sei $\mathcal{B} = (v_1, \dots, v_n)$ Basis von V und $w \in V$ mit

$$w = \mu_1 v_1 + \dots + \mu_n v_n.$$

Ist $\mu_i \neq 0$, so kann man v_i gegen w austauschen, d.h.

$$\mathcal{B}' := (v_1, \dots, v_{i-1}, w, v_{i+1}, \dots, v_n)$$

ist wieder eine Basis von V .

Beweis des Austauschlemmas Wir nehmen $i = 1$, also $\mu_1 \neq 0$ an und zeigen zunächst B1, d.h. $V = \text{Span}_K(\mathcal{B}')$.

„ \subset “ Ist $v \in V$, so hat man eine Darstellung $v = \lambda_1 v_1 + \dots + \lambda_n v_n$. Aus der Darstellung von w folgt

$$v_1 = \frac{1}{\mu_1} w - \frac{\mu_2}{\mu_1} v_2 - \dots - \frac{\mu_n}{\mu_1} v_n.$$

Setzt man das in die Darstellung von v ein, so erhält man

$$v = \frac{\lambda_1}{\mu_1} w + \left(\lambda_2 - \frac{\lambda_1 \mu_2}{\mu_1} \right) v_2 + \dots + \left(\lambda_n - \frac{\lambda_1 \mu_n}{\mu_1} \right) v_n.$$

Also ist $v \in \text{Span}_K(\mathcal{B}')$.

„ \supset “ Folgt sofort aus

$$v = \lambda_1 w + \lambda_2 v_2 + \dots + \lambda_n v_n = \lambda_1 \mu_1 v_1 + (\lambda_2 + \lambda_1 \mu_2) v_2 + \dots + (\lambda_n + \lambda_1 \mu_n) v_n. \quad (*)$$

Zum Nachweis der linearen Unabhängigkeit von \mathcal{B}' sei $\lambda_1 w + \lambda_2 v_2 + \dots + \lambda_n v_n = \mathbf{o}$. Da \mathcal{B} linear unabhängig ist, folgt aus (*), dass

$$\lambda_1 \mu_1 = \lambda_2 + \lambda_1 \mu_2 = \dots = \lambda_n + \lambda_1 \mu_n = 0.$$

Wegen $\mu_1 \neq 0$ folgt $\lambda_1 = 0$ und somit auch $\lambda_2 = \dots = \lambda_n = 0$. ■

Nach diesen Vorbereitungen kann man den *Beweis des Basis-Austauschsatzes* durch wiederholte Anwendung des Austauschlemmas, genauer durch Induktion nach m führen. Man beachte dabei einen entscheidenden Punkt: Die Ungleichung $m \leq n$ wird nicht vorausgesetzt, sie muss bewiesen werden!

Für $m = 0$ ist $m \leq n$ immer erfüllt, es gibt nichts auszutauschen. Für $m = 1$ folgt aus $w_1 \neq \mathbf{o}$ dass $V \neq \{\mathbf{o}\}$, also ist $n \geq 1$ und die Behauptung ist die Aussage des Austauschlemmas.

Ist nun (w_1, \dots, w_m) linear unabhängig gegeben, so ist auch (w_1, \dots, w_{m-1}) linear unabhängig. Nach Induktionsannahme ist $m - 1 \leq n$, also $m \leq n + 1$ und

$$\mathcal{B}' := (w_1, \dots, w_{m-1}, v_m, \dots, v_n)$$

ist eine Basis. Um $m \leq n$ zu zeigen muss nur noch der Fall $m - 1 = n$ ausgeschlossen werden. Dann wäre aber (w_1, \dots, w_m) linear unabhängig und (w_1, \dots, w_{m-1}) Basis. Das ist unmöglich, denn wenn $w_m \in \text{Span}_K(w_1, \dots, w_{m-1})$, so gibt es eine Darstellung

$$w_m = \lambda_1 w_1 + \dots + \lambda_{m-1} w_{m-1}, \text{ also } -\lambda_1 w_1 - \dots - \lambda_{m-1} w_{m-1} + 1 \cdot w_m = \mathbf{o},$$

d.h. (w_1, \dots, w_m) ist linear abhängig. Also ist $m \leq n$ nachgewiesen.

Nun muss noch w_m eingetauscht werden. Da \mathcal{B}' eine Basis ist, gibt es eine Darstellung

$$w_m = \mu_1 w_1 + \dots + \mu_{m-1} w_{m-1} + \mu_m v_m + \dots + \mu_n v_n.$$

Der Fall $\mu_m = \dots = \mu_n = 0$ kann nicht eintreten, denn (w_1, \dots, w_m) ist nach Voraussetzung linear unabhängig. Daher gibt es ein $i \in \{m, \dots, n\}$ mit $\mu_i \neq 0$; wir können $i = m$ annehmen. Nach dem Austauschlemma kann man also v_m durch w_m ersetzen, was zu zeigen blieb. ■

Um zu sehen, ob ein Erzeugendensystem eine Basis ist, kann folgende Aussage helfen:

Korollar 3 Ist $\dim V = n$ und $V = \text{Span}(v_1, \dots, v_n)$, so ist (v_1, \dots, v_n) eine Basis von V .

Beweis Es bleibt zu zeigen, dass (v_1, \dots, v_n) linear unabhängig ist. Wenn nicht, so könnte man nach dem Basis-Auswahlsatz eine Basis $(v_{i_1}, \dots, v_{i_m})$ mit $m < n$ auswählen. Das ist ein Widerspruch zu Korollar 1. ■

Es sei noch bemerkt, dass man das entscheidende Korollar 1 auch ohne den Basis-Austauschsatz mit Hilfe der in Kapitel 0 im Fall $K = \mathbb{R}$ bewiesenen, aber für beliebige Körper gültigen Aussagen über lineare Gleichungssysteme erhalten kann. Man benutzt dazu das folgende

Lemma Gegeben sei ein Vektorraum V mit $V = \text{Span}(v_1, \dots, v_m)$ sowie Vektoren $w_1, \dots, w_n \in V$. Ist $n > m$, so sind (w_1, \dots, w_n) linear abhängig.

Beweis Um eine nicht-triviale Linearkombination

$$\lambda_1 w_1 + \dots + \lambda_n w_n = \mathbf{0} \quad (*)$$

zu finden, stellen wir ein homogenes lineares Gleichungssystem für $\lambda = (\lambda_1, \dots, \lambda_n)$ auf. Da (v_1, \dots, v_m) ein Erzeugendensystem ist, gibt es eine Matrix $A = (a_{ij}) \in M(m \times n; K)$ derart, dass

$$w_j = \sum_{i=1}^m a_{ij} v_i \quad \text{für } j = 1, \dots, n.$$

Durch Einsetzen und Umordnung der Summanden erhält man

$$\sum_{j=1}^n \lambda_j w_j = \sum_{j=1}^n \lambda_j \left(\sum_{i=1}^m a_{ij} v_i \right) = \sum_{i=1}^m \left(\sum_{j=1}^n a_{ij} \lambda_j \right) v_i.$$

Daraus folgt, dass jedes beliebige Lösung λ des homogenen Gleichungssystems

$$\sum_{j=1}^n a_{ij} \lambda_j = 0, \quad i = 1, \dots, m,$$

eine Linearkombination $(*)$ ergibt. Im Fall $m < n$ gibt es nach 0.5.4 wegen $\text{rang } A \leq m$ nicht-triviale Lösungen λ , also sind (w_1, \dots, w_n) linear abhängig. ■

Der Leser möge sich überlegen, wie obiges Korollar 1 auch aus diesem Lemma folgt.

2.2.3 Charakterisierungen einer Basis

In 2.2.1 hatten wir eine Basis erklärt durch die Bedingungen B1 und B2 als ein linear unabhängiges Erzeugendensystem. Manchmal ist es nützlich zu wissen, dass man diese Bedingungen etwas variieren kann. Das ist sehr einfach ohne Benutzung der Sätze aus 2.2.2 zu sehen.

Lemma 1 Ein n -Tupel (v_1, \dots, v_n) von Vektoren aus dem K -Vektorraum V ist genau dann eine Basis von V , wenn gilt:

B1 (v_1, \dots, v_n) ist ein Erzeugendensystem von V , d.h. $V = \text{Span}_K(v_1, \dots, v_n)$.

B2* Das Erzeugendensystem (v_1, \dots, v_n) ist **unverkürzbar**, d.h. für jedes $i \in \{1, \dots, n\}$ ist $(v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n)$ kein Erzeugendensystem mehr.

Man beachte, dass damit nichts über die Länge von möglichen ganz anderen Erzeugendensystemen ausgesagt ist.

Beweis Es ist zu zeigen, dass $B2 \Leftrightarrow B2^*$ gilt, falls B1 vorausgesetzt wird.

$B2 \Rightarrow B2^*$: Ist (v_1, \dots, v_n) verkürzbar, so können wir annehmen, dass

$$v_1 = \lambda_2 v_2 + \dots + \lambda_n v_n, \text{ also } 1 \cdot v_1 - \lambda_2 v_2 - \dots - \lambda_n v_n = \mathbf{o}.$$

Also ist (v_1, \dots, v_n) linear abhängig.

$B2^* \Rightarrow B2$: Ist (v_1, \dots, v_n) linear abhängig, so kann man nach Lemma 2 aus 2.1.4 annehmen, dass

$$v_1 \in \text{Span}_K(v_2, \dots, v_n).$$

Dann ist aber (v_1, \dots, v_n) verkürzbar. ■

Lemma 2 Ein n -Tupel (v_1, \dots, v_n) von Vektoren ist genau dann eine Basis von V , wenn gilt:

B1* (v_1, \dots, v_n) ist **unverlängerbar** linear unabhängig, d.h. für jedes $v \in V$ ist (v_1, \dots, v_n, v) linear abhängig.

B2 (v_1, \dots, v_n) ist linear unabhängig.

Man beachte den Unterschied zum Basis-Austauschsatz: Dort werden die Längen beliebiger linear unabhängiger Tupel verglichen; hier geht es nur darum, ein festes n -Tupel zu verlängern.

Beweis Es ist zu zeigen, dass $B1 \Leftrightarrow B1^*$ gilt, falls $B2$ vorausgesetzt wird.

$B1 \Rightarrow B1^*$: Ist $V = \text{Span}_K(v_1, \dots, v_n)$ so hat jedes $v \in V$ eine Darstellung

$$v = \lambda_1 v_1 + \dots + \lambda_n v_n, \text{ also } 1 \cdot v - \lambda_1 v_1 - \dots - \lambda_n v_n = \mathbf{o};$$

also ist (v_1, \dots, v_n, v) linear abhängig.

$B1^* \Rightarrow B1$: Es ist $V = \text{Span}_K(v_1, \dots, v_n)$ zu zeigen. Für jedes $v \in V$ ist nach Voraussetzung (v_1, \dots, v_n, v) linear abhängig, d.h. es gibt eine nicht triviale Darstellung

$$\mathbf{o} = \lambda_1 v_1 + \dots + \lambda_n v_n + \lambda v.$$

Da (v_1, \dots, v_n) linear unabhängig ist, muss $\lambda \neq 0$ sein. Also folgt

$$v = -\frac{\lambda_1}{\lambda} v_1 - \dots - \frac{\lambda_n}{\lambda} v_n \in \text{Span}_K(v_1, \dots, v_n). \quad \blacksquare$$

Korollar Sei $W \subset V$ ein Untervektorraum. Ist V endlich erzeugt, so ist auch W endlich erzeugt und es gilt

$$\dim W \leq \dim V.$$

Aus $\dim W = \dim V$ folgt $W = V$.

Vorsicht! Die zweite Aussage gilt nicht mehr, wenn $\dim W = \dim V = \infty$. Einfache Beispiele erhält man in $V = \text{Abb}(I, \mathbb{R})$ (Beispiel 3 in 2.1.2).

Beweis Angenommen W wäre nicht endlich erzeugt. Dann genügt es zu zeigen, dass es in W für jedes $m \in \mathbb{N}$ ein m -Tupel (w_1, \dots, w_m) von linear unabhängigen Vektoren gibt. Da $\dim V < \infty$ widerspricht das dem Basis-Austauschsatz. Seien in W schon (w_1, \dots, w_{m-1}) linear unabhängig gefunden. Wenn W nicht endlich erzeugt ist, muss

$$\text{Span}_K(w_1, \dots, w_{m-1}) \subsetneq \text{Span}_K W$$

gelten. Es gibt also mindestens einen weiteren Vektor $w_m \in W$, so dass

$$\text{Span}_K(w_1, \dots, w_{m-1}) \subsetneq \text{Span}_K(w_1, \dots, w_{m-1}, w_m).$$

Mit dem gleichen Argument wie im Beweis von $B1^* \Rightarrow B1$ in obigem Lemma 2 ergibt sich daraus, dass auch das m -Tupel (w_1, \dots, w_m) linear unabhängig ist. Also ist gezeigt, dass W endlich erzeugt ist. Der Rest folgt direkt aus dem Basis-Austauschsatz. Ist (w_1, \dots, w_m) Basis von W und (v_1, \dots, v_n) Basis von V , so muss $m \leq n$ sein. Ist $m = n$, so ist (w_1, \dots, w_m) nach dem Basis-Ergänzungssatz auch Basis von V , also ist $W = V$. \blacksquare

Vorsicht! Die in den letzten beiden Abschnitten bewiesenen Aussagen klingen alle recht plausibel. Man sollte sich allerdings klar machen, dass an mehreren Stellen in den Beweisen durch Skalare dividiert wurde. Man kann analog zu Vektorräumen auch

Moduln definieren, da stammen die Skalare nicht mehr aus einem Körper sondern nur noch aus einem Ring. Dass da alles komplizierter wird, wollen wir durch ganz einfache Beispiele andeuten.

Im K -Vektorraum $V = K$ hat jedes unverkürzbare Erzeugendensystem die Länge 1. Hat man in K zwei erzeugende Elemente λ, μ und ist $\lambda \neq 0$, so folgt

$$\mu = \frac{\mu}{\lambda} \lambda.$$

Also ist das Erzeugendensystem (λ, μ) von K verkürzbar.

Der Ring \mathbb{Z} wird erzeugt von 1, aber auch von 2 und 3, denn jedes $n \in \mathbb{Z}$ lässt sich darstellen als

$$n = k \cdot 2 + l \cdot 3 \quad \text{mit } k, l \in \mathbb{Z}.$$

Aber das Erzeugendensystem $(2, 3)$ von \mathbb{Z} ist unverkürzbar!

Außerdem muss – im Gegensatz zu obigem Korollar für Vektorräume über einem Körper K – ein Untermodul eines endlich erzeugten Moduls über einem Ring R nicht mehr endlich erzeugt sein. Wir skizzieren ein

Beispiel Sei R der Ring aller Folgen (a_n) rationaler Zahlen, wobei Addition und Multiplikation gegeben sind durch

$$(a_n) + (b_n) := (a_n + b_n) \quad \text{und} \quad (a_n) \cdot (b_n) := (a_n \cdot b_n).$$

R ist ein Modul über sich selbst, erzeugt von der einen konstanten Folge (1) . Nun definieren wir

$$\mathfrak{a} := \{(a_n) \in R : \text{es gibt ein } N \in \mathbb{N} \text{ so dass } a_n = 0 \text{ für } n > N\}.$$

Offensichtlich ist $(\mathfrak{a}, +) \subset (R, +)$ eine Untergruppe und es gilt

$$(a_n) \in \mathfrak{a}, (b_n) \in R \Rightarrow (b_n) \cdot (a_n) \in \mathfrak{a}.$$

Daher ist $\mathfrak{a} \subset R$ ein Untermodul (anders ausgedrückt ein Ideal in R). Für endlich viele Folgen $(a_n)^{(1)}, \dots, (a_n)^{(k)} \in \mathfrak{a}$ sei

$$\mathfrak{a}' := R \cdot (a_n)^{(1)} + \dots + R \cdot (a_n)^{(k)} \subset \mathfrak{a}$$

die Menge aller Linearkombinationen. Ist nun $a_n^{(i)} = 0$ für $n > N_i$, so folgt

$$\mathfrak{a}' \subset \{(b_n) \in R : b_n = 0 \text{ für } n > \max\{N_1, \dots, N_k\}\} \subsetneq \mathfrak{a}.$$

Also ist \mathfrak{a} nicht endlich erzeugt. In der Terminologie der „höheren“ Algebra ist R nicht noethersch.

2.2.4 Praktische Verfahren zur Bestimmung einer Basis

Wir behandeln in diesem Abschnitt die praktische Lösung der folgenden Probleme:

Problem 1 Gegeben seien Vektoren $v_1, \dots, v_m \in K^n$. Sind sie linear unabhängig?

Problem 2 Gegeben seien Vektoren $v_1, \dots, v_m \in K^n$.
Gesucht ist eine Basis von $\text{Span}_K(v_1, \dots, v_m)$.

Problem 3 Gegeben sind linear unabhängige Vektoren $v_1, \dots, v_m \in K^n$.
Gesucht sind Vektoren $v_{m+1}, \dots, v_n \in K^n$ derart, dass

$$(v_1, \dots, v_m, v_{m+1}, \dots, v_n) \text{ eine Basis von } K^n \text{ ist.}$$

Die Lösung von Problem 1 kann man auf die Lösung eines linearen Gleichungssystems zurückführen.

Beispiel 1 Ist etwa $n = 3$, $v_1 = (1, 1, 1)$, $v_2 = (1, 3, 5)$, $v_3 = (2, 4, 6) \in \mathbb{R}^3$, so erhält man aus

$$\lambda_1 \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 1 \\ 3 \\ 5 \end{pmatrix} + \lambda_3 \begin{pmatrix} 2 \\ 4 \\ 6 \end{pmatrix} = \begin{pmatrix} \lambda_1 + \lambda_2 + 2\lambda_3 \\ \lambda_1 + 3\lambda_2 + 4\lambda_3 \\ \lambda_1 + 5\lambda_2 + 6\lambda_3 \end{pmatrix} \stackrel{!}{=} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

das homogene lineare Gleichungssystem mit der Koeffizientenmatrix

$$\begin{pmatrix} 1 & 1 & 2 \\ 1 & 3 & 4 \\ 1 & 5 & 6 \end{pmatrix}, \text{ auf Zeilenstufenform gebracht } \begin{pmatrix} 1 & 1 & 2 \\ 0 & 2 & 2 \\ 0 & 0 & 0 \end{pmatrix}.$$

Also ist $(\lambda_1, \lambda_2, \lambda_3) = (1, 1, -1)$ eine Lösung, d.h. $v_1 + v_2 - v_3 = \mathbf{o}$. Daraus folgt, dass v_1, v_2, v_3 linear abhängig sind. In diesem Beispiel kann man natürlich schnell direkt sehen, dass $v_3 = v_1 + v_2$, aber das angegebene Verfahren führt immer zum Ziel.

Es gibt eine Alternative zu dem gerade beschriebenen Verfahren, das auch bei den anderen Problemen nützlich ist. Es beruht auf den immer wieder benutzten Umformungen einer Matrix; daran wollen wir zunächst in allgemeinerem Rahmen erinnern.

Bezeichnen v_1, \dots, v_m die Zeilen der Matrix A , so betrachtet man die folgenden elementaren Umformungen, wobei $i \neq j$:

- Typ (1) Vertausche v_i mit v_j .
Typ (2) Ersetze v_j durch $v_j + \lambda v_i$ bei beliebigem $\lambda \in K$.

Grundlegend ist das folgende

Lemma Sei \tilde{A} aus A durch endlich viele elementare Zeilenumformungen entstanden, und bezeichne w_1, \dots, w_m die Zeilen von \tilde{A} , so gilt

$$\text{Span}_K(w_1, \dots, w_m) = \text{Span}_K(v_1, \dots, v_m).$$

Anders ausgedrückt: Der von den Zeilen aufgespannte Unterraum des K^n ändert sich bei elementaren Umformungen nicht.

Beweis Es genügt einen einzigen Schritt zu betrachten. Typ (1) ist klar, denn bei Linearkombinationen ist die Summe unabhängig von der Reihenfolge der Summanden.

Bei Typ (2) nehmen wir zur Vereinfachung der Bezeichnungen $i = 1$ und $j = 2$ an. Sei also

$$V := \text{Span}_K(v_1, v_2, v_3, \dots, v_m) \quad \text{und} \quad \tilde{V} := \text{Span}_K(v_1, v_2 + \lambda v_1, v_3, \dots, v_m).$$

Da $v_1, v_3, \dots, v_m \in V \cap \tilde{V}$, genügt es die zweite Stelle zu vergleichen:

$$V \subset \tilde{V}: \quad v_2 \in \tilde{V}, \text{ denn } v_2 = -\lambda v_1 + (v_2 + \lambda v_1).$$

$$\tilde{V} \subset V: \quad v_2 + \lambda v_1 \in V \text{ ist klar.} \quad \blacksquare$$

Nach dem in 0.5.4 beschriebenen Verfahren kann man jede Matrix A durch elementare Zeilenumformungen auf Zeilenstufenform \tilde{A} bringen. An \tilde{A} kann man wichtige Informationen ablesen:

Satz Aus $v_1, \dots, v_m \in K^n$ erhält man die Matrizen

$$A = \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix} \quad \text{und auf Zeilenstufenform gebracht} \quad \tilde{A} = \begin{pmatrix} w_1 \\ \vdots \\ w_m \end{pmatrix}.$$

Dabei sei r mit $0 \leq r \leq \max\{m, n\}$ die kritische Zahl so dass

$$w_1, \dots, w_r \neq \mathbf{0}, \quad w_{r+1} = \dots = w_m = \mathbf{0}.$$

Dann ist (w_1, \dots, w_r) eine Basis von $\text{Span}_K(v_1, \dots, v_m) \subset K^n$.

Insbesondere folgt, dass die Zahl $r = \dim \text{Span}_K(v_1, \dots, v_m)$ durch die Matrix A eindeutig bestimmt ist, d.h. unabhängig von den Wahlmöglichkeiten im Umformungsverfahren ist.

Weiter folgt: (v_1, \dots, v_m) linear unabhängig $\Leftrightarrow r = m$.

Beweis Es gilt $\text{Span}_K(v_1, \dots, v_m) = \text{Span}_K(w_1, \dots, w_m) = \text{Span}_K(w_1, \dots, w_r)$ nach dem obigen Lemma und da die Nullvektoren nichts beitragen. Wie wir in Beispiel 5 aus 2.1.4 gesehen hatten, ist (w_1, \dots, w_r) linear unabhängig; demnach ist (w_1, \dots, w_r) eine Basis.

Die beiden Folgerungen sind klar nach den in 2.2.2 bewiesenen Aussagen über die Dimension eines Vektorraums. ■

Beispiel 2 Mit Hilfe der letzten Folgerung aus dem obigen Satz kann man Beispiel 1 noch einmal behandeln:

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 3 & 5 \\ 2 & 4 & 6 \end{pmatrix}, \text{ auf Zeilenstufenform gebracht } \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 4 \\ 0 & 0 & 0 \end{pmatrix} = \tilde{A}.$$

Hier ist $m = 3$ und $r = 2$, also $r < m$; demnach ist (v_1, v_2, v_3) linear abhängig.

Eine Lösung von Problem 2 kann man nach der Methode des Basis-Auswahlsatzes aus 2.2.1 erhalten. Man prüft nach, ob v_1, \dots, v_m linear unabhängig sind; wenn nicht lässt man einen geeigneten Vektor weg. Nach höchstens m solchen Schritten hat man eine Basis erhalten.

Beispiel 3 Wir wählen die Vektoren $v_1, v_2, v_3 \in \mathbb{R}^3$ aus Beispiel 1. Dort hatten wir

$$v_1 + v_2 - v_3 = \mathbf{0}$$

erhalten. Also ist $v_1 = v_3 - v_2$, $v_2 = v_3 - v_1$ und $v_3 = v_1 + v_2$. Daher kann man v_1, v_2 oder v_3 weglassen, die beiden verbleibenden Vektoren bilden eine Basis.

Das Verfahren nach dem Basis-Auswahlsatz kann mehrere Schritte erfordern. Eine Basis (w_1, \dots, w_r) von $\text{Span}_K(v_1, \dots, v_m)$ kann man direkt mit Hilfe des obigen Satzes erhalten.

Beispiel 4 Wir wählen wieder die Vektoren $v_1, v_2, v_3 \in \mathbb{R}^3$ aus Beispiel 1. Dann ist

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 3 & 5 \\ 2 & 4 & 6 \end{pmatrix}, \text{ auf Zeilenstufenform gebracht zu } \tilde{A} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 4 \\ 0 & 0 & 0 \end{pmatrix}.$$

Dann bilden $w_1 = v_1$ und $w_2 = (0, 2, 4)$ eine Basis von $\text{Span}_K(v_1, v_2, v_3)$. Es gilt

$$v_1 = w_1, \quad v_2 = w_1 + w_2, \quad v_3 = 2w_1 + w_2.$$

Zur Lösung von Problem 3 gibt es das folgende

Rezept Gegeben linear unabhängige Vektoren $v_1, \dots, v_m \in K^n$. Trage sie als Zeilen in eine Matrix A ein, bringe A auf Zeilenstufenform B , und betrachte die Pivotpositionen

$$1 \leq j_1 < j_2 < \dots < j_m \leq n$$

in B . Es verbleiben $k = n - m$ Nicht-Pivotpositionen

$$1 \leq i_1 < i_2 < \dots < i_k \leq n.$$

Dann ist $\mathcal{A} := (v_1, \dots, v_m, e_{i_1}, \dots, e_{i_k})$ eine Basis von K^n .

Beweis Beschreiben wir die Matrizen durch ihre Zeilenvektoren, so ist

$$A = \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix} \quad \text{und} \quad B = \begin{pmatrix} w_1 \\ \vdots \\ w_m \end{pmatrix} = \begin{pmatrix} \boxed{b_{1j_1}} & & \\ & \ddots & \\ & & \boxed{b_{mj_m}} \end{pmatrix}.$$

Da B durch Zeilenumformungen entstanden ist, folgt

$$\text{Span}(w_1, \dots, w_m) = \text{Span}(v_1, \dots, v_m). \quad (*)$$

Fügt man zu B noch die Zeilen e_{i_1}, \dots, e_{i_k} an, so erhält man eine quadratische Matrix B' und daraus durch Zeilenvertauschungen eine Matrix B^* in Zeilenstufenform. Also ist

$$\mathcal{B} := (w_1, \dots, w_m, e_{i_1}, \dots, e_{i_k})$$

eine Basis von K^n . Aus $(*)$ folgt $K^n = \text{Span}(\mathcal{A})$, und etwa aus Korollar 3 in 2.2.2 folgt, dass \mathcal{A} auch Basis ist. ■

Beispiel 5 Gegeben $v_1 = (1, 2, 3)$ und $v_2 = (2, 4, 9) \in \mathbb{R}^3$. Sie sind Zeilen der Matrix

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 9 \end{pmatrix}, \text{ auf Zeilenstufenform gebracht } \begin{pmatrix} \boxed{1} & 2 & 3 \\ 0 & 0 & \boxed{3} \end{pmatrix} = B.$$

Die Pivotpositionen von B sind $j_1 = 1$ und $j_2 = 3$; $j = 2$ ist keine Pivotposition. Daher ergänzen wir mit $e_2 = (0, 1, 0)$ und erhalten:

$$B' = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 3 \\ 0 & 1 & 0 \end{pmatrix}, \quad B^* = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Dass (v_1, e_2, v_2) eine Basis von \mathbb{R}^3 ist, kann man auch noch einmal direkt durch Zeilenumformungen prüfen:

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 0 \\ 2 & 4 & 9 \end{pmatrix}, \text{ auf Zeilenstufenform gebracht } \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Der Leser möge zur Übung nachprüfen, dass in diesem Beispiel auch e_1 , nicht aber e_3 zur Ergänzung geeignet ist.

2.2.5 Summen und direkte Summen

Sind in einem Vektorraum V Untervektorräume $W_1, \dots, W_k \subset V$ gegeben, so ist der Durchschnitt $W_1 \cap \dots \cap W_k \subset V$ wieder ein Untervektorraum, die Vereinigung dagegen nur in trivialen Ausnahmefällen (vgl. Bemerkung 1 in 2.1.3). Ein Ersatz dafür ist die **Summe**

$$W_1 + \dots + W_k := \{v \in V : \text{es gibt } w_1 \in W_1, \dots, w_k \in W_k \text{ so dass } v = w_1 + \dots + w_k\}.$$

Wie man leicht sieht, ist $W_1 + \dots + W_k \subset V$ ein Untervektorraum, und da Basen der W_1, \dots, W_k zusammengenommen die Summe erzeugen, ist

$$\dim(W_1 + \dots + W_k) \leq \dim W_1 + \dots + \dim W_k.$$

Im Fall $k = 2$ kann man leicht sehen, wie weit diese Ungleichung von einer Gleichung abweicht.

Dimensionsformel für Untervektorräume Für endlich dimensionale Untervektorräume $W_1, W_2 \subset V$ gilt

$$\dim(W_1 + W_2) = \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2).$$

Beweis Wir starten mit einer Basis $\mathcal{B}_0 := (v_1, \dots, v_m)$ von $W_1 \cap W_2$ und ergänzen sie nach 2.2.2 zu Basen

$$\begin{aligned} \mathcal{B}_1 &:= (v_1, \dots, v_m, w_1, \dots, w_k) \text{ von } W_1 \text{ und} \\ \mathcal{B}_2 &:= (v_1, \dots, v_m, u_1, \dots, u_l) \text{ von } W_2. \end{aligned}$$

Dann genügt es zu zeigen, dass

$$\mathcal{B} := (v_1, \dots, v_m, w_1, \dots, w_k, u_1, \dots, u_l) \text{ Basis von } W_1 + W_2$$

ist. Der Beweis der Gleichung $W_1 + W_2 = \text{Span}_K(\mathcal{B})$ ist ganz einfach und wird dem Leser zur Übung empfohlen. Um die lineare Unabhängigkeit zu zeigen, nehmen wir an, dass

$$\lambda_1 v_1 + \dots + \lambda_m v_m + \mu_1 w_1 + \dots + \mu_k w_k + \rho_1 u_1 + \dots + \rho_l u_l = \mathbf{o}. \quad (*)$$

Setzt man $v := \lambda_1 v_1 + \dots + \lambda_m v_m + \mu_1 w_1 + \dots + \mu_k w_k \in W_1$, so folgt

$$-v = \rho_1 u_1 + \dots + \rho_l u_l \in W_2, \text{ also } v \in W_1 \cap W_2.$$

Da \mathcal{B}_0 bzw. \mathcal{B}_1 Basen von $W_1 \cap W_2$ bzw. W_1 sind, folgt $\mu_1 = \dots = \mu_k = 0$. Setzt man das in (*) ein, so folgt $\lambda_1 = \dots = \lambda_m = \rho_1 = \dots = \rho_l = 0$, denn \mathcal{B}_2 ist linear unabhängig. ■

Besonders ausgezeichnet ist der Fall $V = W_1 + W_2$ und $W_1 \cap W_2 = \{\mathbf{o}\}$. Dafür gibt es einen eigenen Namen.

Definition Gegeben sei ein Vektorraum V mit Untervektorräumen $W_1, W_2 \subset V$. Man sagt, V ist **direkte Summe** von W_1 und W_2 , in Zeichen

$$V = W_1 \oplus W_2,$$

wenn $V = W_1 + W_2$ und $W_1 \cap W_2 = \{\mathbf{o}\}$.

Vorsicht! Man beachte den Unterschied zu dem in Beispiel 6 aus 2.1.1 eingeführten direkten Produkt: Dort sind beliebige Vektorräume V_1, \dots, V_n vorgegeben, die auch gleich sein können. Die direkte Summe wird aus Untervektorräumen eines geeigneten Vektorraums gebildet!

Beispiel Sei $V = K^n$ mit der kanonischen Basis (e_1, \dots, e_n) und

$$W_1 := \text{Span}_K(e_1, \dots, e_k), \quad W_2 := \text{Span}_K(e_{k+1}, \dots, e_n).$$

Dann ist $K^n = W_1 \oplus W_2$ und es gilt $\dim K^n = \dim W_1 + \dim W_2$.

Im endlich-dimensionalen Fall kann man direkte Summen auch allgemeiner durch Basen und Dimensionen charakterisieren.

Lemma 1 Ist $\dim V < \infty$, so sind für Untervektorräume $W_1, W_2 \subset V$ folgende Bedingungen gleichwertig:

- i) $V = W_1 \oplus W_2$.
- ii) Sind Basen (w_1, \dots, w_k) von W_1 und (u_1, \dots, u_l) von W_2 gegeben, so ist

$$\mathcal{B} := (w_1, \dots, w_k, u_1, \dots, u_l) \text{ eine Basis von } V.$$

- iii) $V = W_1 + W_2$ und $\dim V = \dim W_1 + \dim W_2$.

Beweis i) \Rightarrow ii) ergibt sich sofort aus dem Beweis der Dimensionsformel, da die leere Menge eine Basis von $W_1 \cap W_2 = \{\mathbf{o}\}$ ist.

ii) \Rightarrow iii) Da \mathcal{B} Basis von V ist, folgt $V = W_1 + W_2$, und weiter $\dim V = k + l$.

iii) \Rightarrow i) Aus der Dimensionsformel folgt $\dim(W_1 \cap W_2) = 0$, also ist $W_1 \cap W_2 = \{\mathbf{o}\}$. ■

Wie man direkte Summen auch ohne Basen und Dimensionen charakterisieren kann, zeigt

Lemma 2 Für Untervektorräume $W_1, W_2 \subset V$ sind folgende Bedingungen gleichwertig:

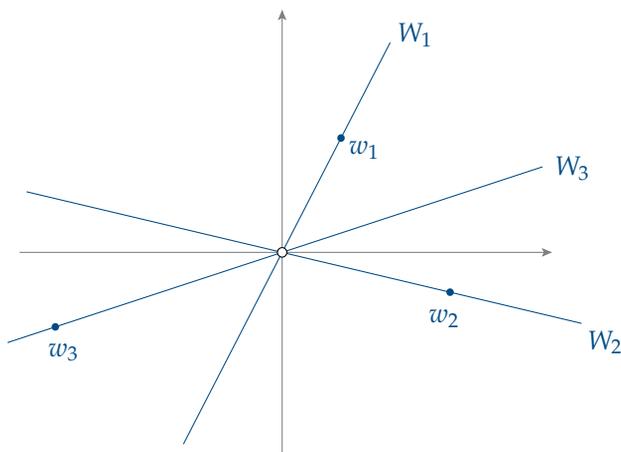
- i) $V = W_1 \oplus W_2$.
- ii) Jedes $v \in V$ ist eindeutig darstellbar als $v = w_1 + w_2$ mit $w_1 \in W_1$ und $w_2 \in W_2$.
- iii) $V = W_1 + W_2$ und aus $w_1 + w_2 = \mathbf{o}$ mit $w_1 \in W_1$ und $w_2 \in W_2$ folgt $w_1 = w_2 = \mathbf{o}$.

Beweis i) \Rightarrow ii): Ist $v = w_1 + w_2 = w'_1 + w'_2$, so folgt $w_1 - w'_1 = w'_2 - w_2 \in W_1 \cap W_2$, also $w_1 = w'_1$ und $w_2 = w'_2$.

ii) \Rightarrow iii): $w_1 + w_2 = \mathbf{o} = \mathbf{o} + \mathbf{o}$, also $w_1 = w_2 = \mathbf{o}$.

iii) \Rightarrow i): Angenommen, es gibt ein $\mathbf{o} \neq v \in W_1 \cap W_2$. Dann folgt $\mathbf{o} = v + (-v)$, im Widerspruch zu iii). ■

In der Eigenwert-Theorie in Kapitel 4 benötigen wir eine Verallgemeinerung der direkten Summen auf mehr als zwei Summanden $W_1, \dots, W_k \subset V$. Die Bedingung $W_1 \cap W_2 = \{\mathbf{o}\}$ vom Fall $k = 2$ kann man dabei nicht ersetzen durch $W_i \cap W_j = \{\mathbf{o}\}$ für $i \neq j$. Das sieht man schon am Beispiel von drei verschiedenen Geraden durch \mathbf{o} im \mathbb{R}^2 .



Hier gibt es Vektoren $\mathbf{o} \neq w_i \in W_i$ mit $w_1 + w_2 + w_3 = \mathbf{o}$. Die Bedingungen ii) und iii) aus Lemma 2 sind einfacher zu verallgemeinern.

Bemerkung Für Untervektorräume $W_1, \dots, W_k \subset V$ sind folgende Bedingungen gleichwertig:

i) Jedes $v \in V$ hat eine eindeutige Darstellung

$$v = w_1 + \dots + w_k \text{ mit } w_1 \in W_1, \dots, w_k \in W_k.$$

ii) $V = W_1 + \dots + W_k$ und aus $w_1 + \dots + w_k = \mathbf{o}$ mit $w_1 \in W_1, \dots, w_k \in W_k$ folgt

$$w_1 = \dots = w_k = \mathbf{o}.$$

Beweis i) \Rightarrow ii) ist offensichtlich. Zum Nachweis von ii) \Rightarrow i) sei

$$v = w_1 + \dots + w_k = w'_1 + \dots + w'_k \text{ mit } w_i, w'_i \in W_i.$$

Daraus folgt

$$\mathbf{o} = (w_1 - w'_1) + \dots + (w_k - w'_k), \text{ also } w_i - w'_i = \mathbf{o}. \quad \blacksquare$$

Definition Gegeben sei ein Vektorraum V mit Untervektorräumen $W_1, \dots, W_k \subset V$ derart, dass $V = W_1 + \dots + W_k$. Diese Summe heißt **direkt**, in Zeichen

$$V = W_1 \oplus \dots \oplus W_k,$$

wenn eine der äquivalenten Bedingungen der obigen Bemerkung erfüllt ist.

In diesem Fall nennt man V **direkte Summe** von W_1, \dots, W_k , die W_i heißen **direkte Summanden** von V . Einer solchen Zerlegung von V entspricht auch eine Zerlegung einer Basis. Genauer gilt eine Verallgemeinerung des obigen Lemma 1:

Satz Ist $\dim V < \infty$, so sind für Untervektorräume $W_1, \dots, W_k \subset V$ folgende Bedingungen gleichwertig:

i) $V = W_1 \oplus \dots \oplus W_k$.

ii) Ist für jedes $i \in \{1, \dots, k\}$ eine Basis $\mathcal{B}_i = (v_1^{(i)}, \dots, v_{d_i}^{(i)})$ von W_i gegeben, so ist

$$\mathcal{B} := (v_1^{(1)}, \dots, v_{d_1}^{(1)}, \dots, v_1^{(k)}, \dots, v_{d_k}^{(k)}) \text{ eine Basis von } V.$$

iii) $V = W_1 + \dots + W_k$ und $\dim V = \dim W_1 + \dots + \dim W_k$.

Beweis ii) \Leftrightarrow iii) folgt sofort aus den Eigenschaften von Basen.

i) \Rightarrow ii) : Da $V = W_1 + \dots + W_k$, ist \mathcal{B} ein Erzeugendensystem von V . Zum Beweis der linearen Unabhängigkeit nehmen wir an, es sei

$$\lambda_1^{(1)} v_1^{(1)} + \dots + \lambda_{d_1}^{(1)} v_{d_1}^{(1)} + \dots + \lambda_1^{(k)} v_1^{(k)} + \dots + \lambda_{d_k}^{(k)} v_{d_k}^{(k)} = \mathbf{o}, \quad (*)$$

wobei $\lambda_j^{(i)} \in K$. Setzen wir $w_i := \lambda_1^{(i)} v_1^{(i)} + \dots + \lambda_{d_i}^{(i)} v_{d_i}^{(i)} \in W_i$, so bedeutet (*), dass

$$w_1 + \dots + w_k = \mathbf{o}.$$

Nach Definition der direkten Summe folgt daraus $w_1 = \dots = w_k = \mathbf{o}$. Also ist für $i = 1, \dots, k$

$$\lambda_1^{(i)} v_1^{(i)} + \dots + \lambda_{d_i}^{(i)} v_{d_i}^{(i)} = \mathbf{o}.$$

Da \mathcal{B}_i eine Basis von W_i ist, folgt $\lambda_1^{(i)} = \dots = \lambda_{d_i}^{(i)} = 0$, und das gilt für alle i . Also sind alle $\lambda_j^{(i)} = 0$.

ii) \Rightarrow i) : Gegeben seien $w_i \in W_i$ mit

$$w_1 + \dots + w_k = \mathbf{o}. \quad (**)$$

Wählt man für jedes i eine Basis $\mathcal{B}_i = (v_1^{(i)}, \dots, v_{d_i}^{(i)})$ von W_i , so ist

$$w_i = \lambda_1^{(i)} v_1^{(i)} + \dots + \lambda_{d_i}^{(i)} v_{d_i}^{(i)}$$

mit $\lambda_j^{(i)} \in K$. Da \mathcal{B} eine Basis von V ist, folgt aus (**), dass alle Koeffizienten $\lambda_j^{(i)} = 0$ sind. Also gilt $w_1 = \dots = w_k = \mathbf{o}$. ■

Beim Beweis der Dimensionsformel für Untervektorräume zu Beginn dieses Abschnitts hatten wir die Existenz von passenden Basen benutzt. Für praktische Rechnungen hat man das folgende

Problem Im K^n seien Untervektorräume

$$V = \text{Span}(v_1, \dots, v_k) \quad \text{und} \quad W = \text{Span}(w_1, \dots, w_l)$$

gegeben. Gesucht sind Basen von $V + W$ und von $V \cap W$.

Eine Basis von $V + W$ ist leicht zu finden, für $V \cap W$ ist es schwieriger. Für eine gemeinsame Lösung gibt es ein geschicktes Rechenverfahren. Man schreibt die gegebenen Vektoren als Zeilen in eine Matrix der Form

$$A = (A_1, A_2) = \begin{pmatrix} v_1 & v_1 \\ \vdots & \vdots \\ v_k & v_k \\ w_1 & \mathbf{o} \\ \vdots & \vdots \\ w_l & \mathbf{o} \end{pmatrix} \in M((k+l) \times 2n; K).$$

Offensichtlich gilt für die in 2.2.6 erklärten Zeilenräume $\text{ZR}(A_1) = V + W$ und $\text{ZR}(A_2) = V$. Durch Zeilenumformungen bringt man A auf Zeilenstufenform

$$\tilde{A} = (\tilde{A}_1, \tilde{A}_2) = \begin{pmatrix} u_1 & u'_1 \\ \vdots & \vdots \\ u_r & u'_r \\ u_{r+1} & u'_{r+1} \\ \vdots & \vdots \\ u_{r+d} & u'_{r+d} \\ \mathbf{o} & \mathbf{o} \\ \mathbf{o} & \mathbf{o} \end{pmatrix}.$$

Dabei sind die Teilmatrizen

$$\begin{pmatrix} u_1 \\ \vdots \\ u_r \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} u'_{r+1} \\ \vdots \\ u'_{r+d} \end{pmatrix}$$

auf Zeilenstufenform mit $u_r \neq \mathbf{o}$, $u_{r+1} = \dots = u_{r+d} = \mathbf{o}$, $u'_{r+d} \neq \mathbf{o}$. Da $\text{ZR}(\tilde{A}_1) = \text{ZR}(A_1)$ folgt sofort, dass

$$\mathcal{B} := (u_1, \dots, u_r) \quad \text{Basis von } V + W$$

ist. Etwas Sorgfalt ist nötig um zu sehen, dass

$$\mathcal{B} := (u'_{r+1}, \dots, u'_{r+d}) \quad \text{Basis von } V \cap W$$

ist. Zunächst ist klar, dass $(u'_{r+1}, \dots, u'_{r+d})$ linear unabhängig ist, denn die entsprechende Matrix ist auf Zeilenstufenform. Im nächsten Schritt zeigen wir

$$u'_{r+1}, \dots, u'_{r+d} \in V \cap W.$$

Jede Zeile von \tilde{A} ist Linearkombination von Zeilen von A . Also hat man für jedes i die Darstellung

$$u_i = \lambda_{1i}v_1 + \dots + \lambda_{ki}v_k + \mu_{1i}w_1 + \dots + \mu_{li}w_l \quad \text{und} \quad u'_i = \lambda_{1i}v_1 + \dots + \lambda_{ki}v_k.$$

Für $i = r+1, \dots, r+d$ ist $u_i = \mathbf{o}$, also $u'_i \in V \cap W$. Es bleibt zu zeigen, dass

$$V \cap W = \text{Span}(u'_{r+1}, \dots, u'_{r+d}).$$

Sei also $u \in V \cap W$. Wir zeigen zunächst, dass $(\mathbf{o}, u) \in \text{ZR}(A)$. Da $u \in V$ und $u \in W$ gibt es Darstellungen

$$u = \sum_{i=1}^k \rho_i v_i = \sum_{j=1}^l \sigma_j w_j$$

mit $\rho_i, \sigma_j \in K$. Aus diesen beiden Darstellungen folgt

$$\left(\sum_{i=1}^k \rho_i v_i - \sum_{j=1}^l \sigma_j w_j, \sum_{i=1}^l \rho_i v_i\right) = (\mathbf{o}, u) \in \text{ZR}(A).$$

Da $\text{ZR}(\tilde{A}) = \text{ZR}(A)$, folgt $(\mathbf{o}, u) \in \text{ZR}(\tilde{A})$. Also gibt es eine Darstellung

$$(\mathbf{o}, u) = \left(\sum_{i=1}^n \alpha_i u_i, \sum_{i=1}^r \alpha_i u'_i + \sum_{j=1}^d \beta_j u'_{r+j}\right)$$

mit $\alpha_i, \beta_j \in K$. Aus $\sum \alpha_i u_i = \mathbf{o}$ folgt wegen der linearen Unabhängigkeit von (u_1, \dots, u_r) , dass $\alpha_1 = \dots = \alpha_r = 0$. Somit ist

$$u = \sum_{j=1}^d \beta_j u'_{r+j}. \quad \blacksquare$$

Beispiel

A_1		A_2	
1 2 3		1 2 3	
0 1 2		0 1 2	
2 3 1		0 0 0	
1 2 0		0 0 0	
1 2 3		1 2 3	
0 1 2		0 1 2	
0 -1 -5		-2 -4 -6	
0 0 -3		-1 -2 -3	
1 2 3		1 2 3	
0 1 2		0 1 2	
0 0 -3		-2 -3 -4	
0 0 0		1 1 1	
\tilde{A}_1		\tilde{A}_2	

Geometrisch gesehen schneiden sich in diesem Beispiel zwei Ebenen $V, W \subset \mathbb{R}^3$ in einer Gerade $V \cap W$. Die Zahlen sind so gewählt, dass das Ergebnis

$$V + W = \mathbb{R}^3 \quad V \cap W = \mathbb{R} \cdot (1, 1, 1)$$

schon ziemlich direkt zu sehen ist; dann kann man gespannt beobachten, wie es der Algorithmus schrittweise produziert.

Das eben beschriebene Verfahren wird manchmal **ZASSENHAUS-Algorithmus** genannt. Allerdings scheint keine Quelle in den Arbeiten von HANS ZASSENHAUS (1912-1991) bekannt zu sein. Es gibt aber eine nette Assoziation. Die Firma **Zassenhaus** baut seit langer Zeit klassische Kaffeemühlen und der Algorithmus ist eine Art von Kaffeemühle: Man wirft oben in den Trichter die Erzeugendensysteme ein, dreht genügend oft die Kurbel, und nimmt anschließend aus der kleinen Schublade unten die Basen heraus.



2.2.6 Der Rang einer Matrix

Beim Eliminationsverfahren in 0.5.4 hatten wir die Koeffizientenmatrix auf Zeilenstufenform gebracht. Von den anfänglichen m Zeilen waren dabei r von Null verschiedene Zeilen übrig geblieben, und diese Zahl r war entscheidend gewesen für die Anzahl der Lösungen. Es war dabei offen geblieben, ob die Zahl r von den verschiedenen Wahlmöglichkeiten bei der Elimination unabhängig ist. Mit den Ergebnissen der vorhergehenden Abschnitte über Basen ist das leicht zu zeigen.

Bei der theoretischen Behandlung von Gleichungssystemen in 2.3.5 wird sich überdies zeigen, dass man neben den Zeilen auch die Spalten der Matrix betrachten muss. Man könnte eine Spaltenstufenform berechnen und dabei eine analoge Zahl r' von verbleibenden nicht verschwindenden Spalten erhalten. Nicht nur auf den ersten Blick ist eine Beziehung zwischen r und r' wenig offensichtlich. In diesem Abschnitt wollen wir zeigen, dass stets $r = r'$ gilt, diese Zahl heißt dann „Rang“ der Matrix. So wie die Dimension eines Vektorraums ist der Rang ein Maß für die Reichhaltigkeit einer Matrix.

Zunächst ist es nützlich, einige Bezeichnungen und Begriffe einzuführen. Ist K ein Körper und $A = (a_{ij}) \in M(m \times n; K)$ eine Matrix, so bezeichnen wir mit

$v_1, \dots, v_m \in K^n$, $v_i = (a_{i1}, \dots, a_{in})$ die **Zeilenvektoren** und mit

$w_1, \dots, w_n \in K^m$, $w_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$ die **Spaltenvektoren** von A .

Die zu A **transponierte** Matrix tA ist erklärt durch ${}^tA = (a_{ji}) \in M(n \times m; K)$. Demnach sind die Zeilenvektoren von tA die Spaltenvektoren von A und umgekehrt. Eine weitere Transposition führt zurück zu A , in Zeichen ${}^t({}^tA) = A$. Man nennt eine Matrix $A \in M(n \times n; K)$ **symmetrisch**, wenn ${}^tA = A$.

Weiter sei

$ZR(A) := \text{Span}_K(v_1, \dots, v_m) \subset K^n$ den **Zeilenraum** von A und
 $SR(A) := \text{Span}_K(w_1, \dots, w_n) \subset K^m$ den **Spaltenraum** von A , und
 $zr(A) := \dim ZR(A)$ den **Zeilenrang** von A ,
 $sr(A) := \dim SR(A)$ den **Spaltenrang** von A .

Aus den Definitionen erhält man sofort die Abschätzungen

$$0 \leq zr(A) \leq \min\{m, n\} \quad \text{und} \quad 0 \leq sr(A) \leq \min\{m, n\}.$$

Außerdem ist offensichtlich

$$ZR({}^tA) = SR(A), \text{ also } zr({}^tA) = sr(A) \text{ und}$$

$$SR({}^tA) = ZR(A), \text{ also } sr({}^tA) = zr(A).$$

Zur Berechnung des Zeilenrangs (und mit Hilfe der Transposition auch des Spaltenrangs) kann man den Satz aus 2.2.4 benutzen: Man bringt die Matrix A auf Zeilenstufenform \tilde{A} mit r von \mathbf{o} verschiedenen Zeilen. Dann ist $zr(A) = r$.

Beispiel 1 Sei $m = 1$ und $n \geq 1$ beliebig. Dann ist

$$A = (a_1, \dots, a_n) \quad \text{und} \quad 0 \leq zr(A), sr(A) \leq 1.$$

Ist $a_1 = \dots = a_n = 0$, so folgt $zr(A) = 0 = sr(A)$.

Ist mindestens ein $a_i \neq 0$, so ist $ZR(A) \subset K^n$ eine Gerade und $SR(A) = K^1$, also

$$zr(A) = 1 = sr(A).$$

Man beachte dabei, dass $ZR(A)$ und $SR(A)$ ganz verschiedene Vektorräume sind. Dennoch haben sie in jedem der beiden möglichen Fälle die gleiche Dimension.

Beispiel 2 Sei $m = n = 2$. Durch Zeilenumformungen erhalten wir

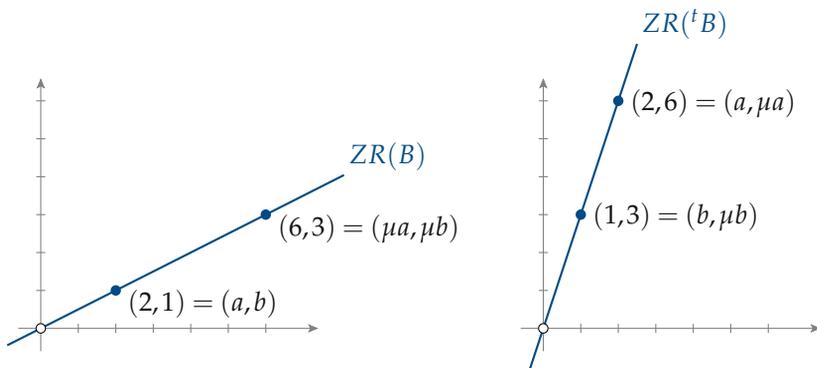
$$A = \begin{pmatrix} 2 & 1 \\ 6 & 2 \end{pmatrix} \sim \begin{pmatrix} \boxed{2} & 1 \\ 0 & \boxed{-1} \end{pmatrix} = \tilde{A}, \quad \text{also } zr(A) = 2,$$

$${}^tA = \begin{pmatrix} 2 & 6 \\ 1 & 2 \end{pmatrix} \sim \begin{pmatrix} \boxed{2} & 6 \\ 0 & \boxed{-1} \end{pmatrix} = {}^t\tilde{A}, \quad \text{also } zr({}^tA) = sr(A) = 2.$$

$$B = \begin{pmatrix} 2 & 1 \\ 6 & 3 \end{pmatrix} \sim \begin{pmatrix} \boxed{2} & 1 \\ 0 & 0 \end{pmatrix} = \tilde{B}, \quad \text{also } zr(B) = 1,$$

$${}^tB = \begin{pmatrix} 2 & 6 \\ 1 & 3 \end{pmatrix} \sim \begin{pmatrix} \boxed{2} & 6 \\ 0 & 0 \end{pmatrix} = {}^t\tilde{B}, \quad \text{also } zr({}^tB) = sr(B) = 1.$$

Bei A und B stimmen demnach Zeilenrang und Spaltenrang überein. Bei B ist zu bemerken, dass Zeilenraum und Spaltenraum im Fall $K = \mathbb{R}$ beide Geraden sind, allerdings sind sie verschieden.



Eine allgemeinere Form ist mit $a \neq 0$

$$B = \begin{pmatrix} a & b \\ \mu a & \mu b \end{pmatrix} \sim \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \tilde{B},$$

$${}^t B = \begin{pmatrix} a & \mu a \\ b & \mu b \end{pmatrix} \sim \begin{pmatrix} a & \mu a \\ 0 & 0 \end{pmatrix} = {}^t \tilde{B}, \quad \text{denn } (b, \mu b) = \frac{b}{a}(a, \mu a).$$

Auch in diesem Fall ist $\text{zr}(B) = 1 = \text{sr}(B)$.

Wir überlassen dem Leser den Rest des Beweises, dass auch im Fall $m = n = 2$ stets Zeilenrang gleich Spaltenrang ist.

Nach diesen beiden Beispielen ist das folgende allgemeine Ergebnis vielleicht nicht mehr ganz so verwunderlich.

Rang-Satz Für beliebige Zahlen $m, n \in \mathbb{N}^*$ und Matrizen $A \in M(m \times n; K)$ über einem Körper K gilt

$$\text{zr}(A) = \text{sr}(A).$$

Kurz ausgedrückt: Zeilenrang = Spaltenrang.

Benutzt man dieses anschließend bewiesene Ergebnis, so kann man den **Rang** einer Matrix A erklären als ihren Zeilenrang oder Spaltenrang, in Zeichen

$$\text{rang}(A) := \text{zr}(A) = \text{sr}(A).$$

Mit Hilfe der Sätze über Basis und Dimension erhält man

Bemerkung Für jedes $A \in M(m \times n; K)$ gilt:

$$\begin{aligned} \text{rang}(A) &= \text{Maximalzahl linear unabhängiger Zeilen von } A \\ &= \text{Maximalzahl linear unabhängiger Spalten von } A. \end{aligned}$$

Man hat die Abschätzung $0 \leq \text{rang}(A) \leq \min\{m, n\}$.

Will man den Rang einer gegebenen Matrix ausrechnen, so genügt es, sie auf Zeilenstufenform zu bringen. Dann ist der Rang bestimmt durch die Anzahl r der verbleibenden von Null verschiedenen Zeilen.

Der entscheidende Schritt im Beweis des Rangsatzes ist enthalten in folgendem

Lemma Für die Matrix $A \in M(m \times n; K)$ gebe es ein $i \in \{1, \dots, m\}$ derart, dass die i -te Zeile Linearkombination der restlichen Zeilen ist. $\bar{A} \in M((m-1) \times n; K)$ sei die Matrix, die aus A durch Streichen der i -ten Zeile entsteht. Dann gilt:

- a) $ZR(\bar{A}) = ZR(A)$, insbesondere $\text{zr}(\bar{A}) = \text{zr}(A)$.
 b) $\text{sr}(\bar{A}) = \text{sr}(A)$.

Beweis Wir bezeichnen mit $v_1, \dots, v_m \in K^n$ die Zeilenvektoren und mit $w_1, \dots, w_n \in K^m$ die Spaltenvektoren von A . Zur Vereinfachung der Bezeichnungen nehmen wir $i = m$ an. Dann besagt die Voraussetzung, dass

$$v_m \in \text{Span}_K(v_1, \dots, v_{m-1}) = ZR(\bar{A}) = \text{Span}_K(v_1, \dots, v_m) = ZR(A) \subset K^n;$$

daraus folgt sofort a). Dagegen wird der Spaltenraum verändert: Es ist

$$\text{SR}(A) \subset K^m \quad \text{aber} \quad \text{SR}(\bar{A}) \subset K^{m-1}.$$

Den Übergang von A nach \bar{A} kann man geometrisch sehen. Bezeichnet

$$\pi: K^m \rightarrow K^{m-1}, \quad x = (x_1, \dots, x_m) \mapsto \bar{x} = (x_1, \dots, x_{m-1}),$$

die „Projektion“, so ist $\text{SR}(\bar{A}) = \pi(\text{SR}(A))$. Wir wollen nun zeigen, dass auf Grund der gemachten Voraussetzung

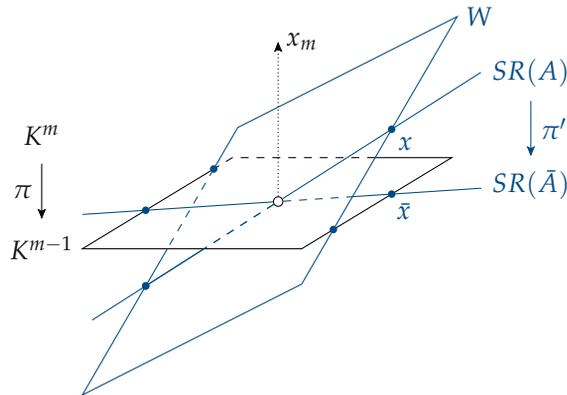
$$v_m = \mu_1 v_1 + \dots + \mu_{m-1} v_{m-1} \tag{+}$$

die Dimension von $\text{SR}(A)$ durch die Projektion nicht verändert wird, d.h.

$$\dim \pi(\text{SR}(A)) = \dim \text{SR}(A), \quad \text{also} \quad \text{sr}(\bar{A}) = \text{sr}(A).$$

Wegen (+) ist $\text{SR}(A)$ enthalten im Untervektorraum

$$W := \{(x_1, \dots, x_m) \in K^m : x_m = \mu_1 x_1 + \dots + \mu_{m-1} x_{m-1}\} \subset K^m.$$



Nach dem Basis-Auswahlsatz können wir annehmen, dass

(w_1, \dots, w_s) eine Basis von $\text{SR}(A)$ ist, wobei $0 \leq s = \text{sr}(A) \leq \min\{m, n\}$.

Nun genügt es zu zeigen, dass

$(\bar{w}_1, \dots, \bar{w}_s)$ eine Basis von $\text{SR}(\bar{A}) \subset K^{m-1}$

ist. Erzeugendensystem ist klar. Zum Nachweis der linearen Unabhängigkeit sei

$$\lambda_1 \bar{w}_1 + \dots + \lambda_s \bar{w}_s = \mathbf{o}, \quad \text{d.h.} \quad \sum_{j=1}^s \lambda_j a_{ij} = 0 \quad \text{für } i = 1, \dots, m-1. \quad (*)$$

Mit Hilfe von (+) zeigen wir nun, dass sich diese Relation (*) in die m -ten Komponenten a_{m1}, \dots, a_{ms} von w_1, \dots, w_s fortsetzt, d.h. $\sum_{j=1}^s \lambda_j a_{mj} = 0$. Das folgt mit Hilfe der Umordnung einer doppelten Summe von insgesamt $(m-1)s$ Summanden:

$$\begin{aligned} \lambda_1 a_{m1} + \dots + \lambda_s a_{ms} &= \lambda_1 \left(\sum_{i=1}^{m-1} \mu_i a_{i1} \right) + \dots + \lambda_s \left(\sum_{i=1}^{m-1} \mu_i a_{is} \right) \\ &= \mu_1 \left(\sum_{j=1}^s \lambda_j a_{1j} \right) + \dots + \mu_{m-1} \left(\sum_{j=1}^s \lambda_j a_{m-1,j} \right) \\ &= \mu_1 \cdot 0 + \dots + \mu_{m-1} \cdot 0 = 0. \end{aligned}$$

Also folgt $\lambda_1 w_1 + \dots + \lambda_s w_s = \mathbf{o}$ und $\lambda_1 = \dots = \lambda_s = 0$. ■

Wer von den vielen Summenzeichen verwirrt ist, möge den Beweis im Spezialfall $m-1 = s = 2$ mit den vier Summanden zum besseren Verständnis direkt aufschreiben.

Ein kundiger Leser wird sofort bemerken, dass dieser Beweis kürzer geführt werden kann, wenn man benutzt, dass die Projektion

$$\pi : W \rightarrow K^{m-1} \text{ und ihre Einschränkung } \pi' : \text{SR}(A) \rightarrow \text{SR}(\bar{A})$$

bijektive lineare Abbildungen sind.

Das folgt daraus, dass jedes $\bar{x} = (x_1, \dots, x_{m-1}) \in K^{m-1}$ genau ein Urbild

$$x = (x_1, \dots, x_{m-1}, \mu_1 x_1 + \dots + \mu_{m-1} x_{m-1})$$

in W hat. Also ist π' ein Isomorphismus und nach den anschließend in 2.3.2 bewiesenen Aussagen folgt, dass

$$\dim \text{SR}(\bar{A}) = \dim \text{SR}(A).$$

Beweis des Rang-Satzes Nach dem Basis-Auswahlsatz kann man so lange Zeilen streichen, bis die verbleibenden r Zeilen mit $0 \leq r \leq \min\{m, n\}$ eine Basis von $\text{ZR}(A)$ bilden. Wir bezeichnen mit

$$A' \in \text{M}(r \times n; K)$$

die verbleibende Matrix. Durch wiederholte Anwendung des Lemmas erhält man

$$\text{zr}(A) = \text{zr}(A') = r \quad \text{und} \quad \text{sr}(A) = \text{sr}(A').$$

Da $\text{SR}(A') \subset K^r$ folgt $\text{sr}(A') \leq r$. Damit ist also gezeigt, dass für jede Matrix A die Beziehung

$$\text{sr}(A) \leq \text{zr}(A), \quad \text{d.h. Spaltenrang} \leq \text{Zeilenrang}$$

gilt. Das kann man auch auf ${}^t A$ anwenden, daraus folgt

$$\text{zr}(A) = \text{sr}({}^t A) \leq \text{zr}({}^t A) = \text{sr}(A);$$

insgesamt ist also $\text{zr}(A) = \text{sr}(A)$. ■

Als unmittelbare Folgerung erhält man das

Korollar Für jede Matrix $A \in \text{M}(m \times n; K)$ gilt

$$\text{rang} {}^t A = \text{rang } A.$$
■

2.3 Lineare Abbildungen

2.3.1 Definitionen und Beispiele

Der Gesamtpreis einer Ware hängt ab vom Einzelpreis und der Menge. Ist im einfachsten Fall a der Preis pro kg und x das Gewicht in kg, so berechnet sich der Preis als $f(x) = ax$. Eine derartige Funktion f heißt „linear“ bezüglich x . Die Realität ist meist schon komplizierter: Es kann ein Grundpreis b dazukommen, dann ist $f(x) = ax + b$ und der Preis a pro kg kann für große Gewichte x niedriger werden. Aber immerhin ist eine lineare Funktion in vielen Fällen eine brauchbare erste Approximation für den genauen Wert. Das ist ein wesentlicher Grund für die Bedeutung der linearen Algebra.

Hat man statt einer einzigen Ware n verschiedene Waren mit Einzelpreisen a_1, \dots, a_n und Mengen x_1, \dots, x_n , so berechnet sich der Gesamtpreis als

$$f(x_1, \dots, x_n) = a_1x_1 + \dots + a_nx_n. \quad (*)$$

Die charakteristischen Eigenschaften einer derartigen Abbildung

$$f: \mathbb{R}^n \rightarrow \mathbb{R}, x = (x_1, \dots, x_n) \mapsto f(x),$$

sind folgende:

- 1) $f(x + x') = f(x) + f(x')$ für $x, x' \in \mathbb{R}^n$ und
- 2) $f(\lambda x) = \lambda f(x)$ für $x \in \mathbb{R}^n$ und $\lambda \in \mathbb{R}$.

Dass eine Abbildung f der Form (*) diese beiden Eigenschaften hat, rechnet man ganz leicht nach. Hat umgekehrt f die Eigenschaften 1) und 2), so definiert man

$$a_i := f(e_i),$$

wobei $e_i \in \mathbb{R}^n$ den kanonischen Basisvektor bezeichnet. Dann ist

$$x = (x_1, \dots, x_n) = x_1e_1 + \dots + x_n e_n$$

und nach 1) und 2) folgt

$$\begin{aligned} f(x) &= f(x_1e_1 + \dots + x_n e_n) = f(x_1e_1) + \dots + f(x_n e_n) \\ &= x_1f(e_1) + \dots + x_n f(e_n) = a_1x_1 + \dots + a_nx_n. \end{aligned}$$

Also ist f von der Form (*).

Diese Vorüberlegung motiviert die allgemeine

Definition Sind V, W Vektorräume über einem Körper K , so heißt eine Abbildung $F: V \rightarrow W$ **linear**, oder genauer **K -linear** wenn sie folgende Eigenschaften hat:

L1 Für $v, v' \in V$ gilt $F(v + v') = F(v) + F(v')$.

L2 Für $v \in V$ und $\lambda \in K$ gilt $F(\lambda v) = \lambda F(v)$.

Man sollte sich diese beiden Bedingungen näher ansehen: Die Summe $v + v'$ wird in V gebildet, die Summe $F(v) + F(v')$ dagegen in W ; genau genommen müsste man hier zwei verschiedene Zeichen $+$ verwenden. Aus dieser Sicht bedeutet Bedingung L1, dass F mit den beiden Additionen in V und W „verträglich“ ist; analog bedeutet L2 die Verträglichkeit von F mit den beiden Multiplikationen mit Skalaren. Aus diesem Grund wird eine lineare Abbildung zwischen Vektorräumen auch **Homomorphismus** genannt, das bedeutet allgemein „verträglich mit den gegebenen Strukturen“.

Beispiel 1 Im Fall $V = K^n$ und $W = K^m$ benutzen wir eine Matrix

$$A = (a_{ij}) \in M(m \times n; K)$$

und wir definieren mit der Konvention aus 0.5.2

$$F(x) = Ax.$$

Dabei sind $x = {}^t(x_1, \dots, x_n) \in K^n$ und $F(x) = {}^t(y_1, \dots, y_m) \in K^m$ als Spaltenvektoren geschrieben. Ganz explizit bedeutet das

$$y_i = \sum_{j=1}^n a_{ij}x_j \quad \text{für } i = 1, \dots, m. \quad (*)$$

Diese Summenschreibweise sollte man sich gut einprägen. Man kann sie auch so veranschaulichen:

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{i1} & \cdots & a_{in} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_i \\ \vdots \\ y_m \end{pmatrix}$$

Ist $x' = {}^t(x'_1, \dots, x'_n)$ und $F(x') = {}^t(y'_1, \dots, y'_m)$, so gilt

$$y'_i = \sum_{j=1}^n a_{ij}x'_j, \quad \text{also} \quad y_i + y'_i = \sum_{j=1}^n a_{ij}(x_j + x'_j).$$

Daraus folgt $F(x + x') = F(x) + F(x')$. Für $\lambda \in K$ hat man

$$\sum_{j=1}^n a_{ij}(\lambda x_j) = \lambda \sum_{j=1}^n a_{ij}x_j = \lambda y_i,$$

also gilt auch $F(\lambda x) = \lambda F(x)$; somit ist die aus der Matrix A erhaltene Abbildung F linear. In 2.4.2 werden wir sehen, dass jede lineare Abbildung $F : K^n \rightarrow K^m$ auf diese Weise entsteht.

Wir wollen noch die Bilder der kanonischen Basisvektoren $e_1, \dots, e_n \in K^n$ unter der durch A beschriebenen Abbildung F berechnen. Nach der oben angegebenen Regel (*) für die Berechnung von Ax erhält man

$$\begin{pmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1n} \\ & & \vdots & & \\ a_{m1} & \cdots & a_{mj} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}.$$

Bezeichnet $a^{(j)}$ den j -ten Spaltenvektor von A , so bedeutet das $F(e_j) = a^{(j)}$. Das kann man auch als Summe schreiben. Bezeichnen (e_1, \dots, e_n) und (e'_1, \dots, e'_m) die kanonischen Basen von K^n und K^m , so ist

$$F(e_j) = \sum_{i=1}^m a_{ij} e'_i \quad \text{für } j = 1, \dots, n. \quad (**)$$

Man beachte die verschiedenen Summationen in den Formeln (*) und (**). Eine einprägsame Merkregel in Worten ist:

Die Spaltenvektoren sind die Bilder der kanonischen Basisvektoren.

Diese Regel sollte man sich gut einprägen, sie wird immer wieder auftauchen!

Einen Spezialfall von solchen linearen Abbildungen hatten wir schon in Kapitel 0 bei der Parametrisierung von Geraden oder Ebenen durch $\mathbf{o} \in \mathbb{R}^n$ benutzt. Das waren lineare Abbildungen

$$F_1 : \mathbb{R} \rightarrow \mathbb{R}^n, \lambda \mapsto \lambda w \quad \text{und} \quad F_2 : \mathbb{R}^2 \rightarrow \mathbb{R}^n, \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} \mapsto \lambda_1 w_1 + \lambda_2 w_2,$$

wobei $w \neq \mathbf{o}$ und (w_1, w_2) linear unabhängig vorausgesetzt war. In diesem Fall ist F_1 gegeben durch die Matrix mit w als der einzigen Spalte, und F_2 durch die Matrix mit zwei Spalten w_1 und w_2 .

Sehr wichtig ist der Zusammenhang mit linearen Gleichungssystemen. Ist $A \in M(m \times n; K)$ und $b \in K^m$, so gilt offenbar

$$\text{Lös}(A, b) = F^{-1}(b) \subset K^n,$$

d.h. der Lösungsraum des linearen Gleichungssystems $Ax = b$ ist gleich dem Urbild von b bei der aus A wie oben erhaltenen Abbildung F . Weiter ist die in 0.5.3 konstruierte Abbildung

$$\varphi : \mathbb{R}^k \rightarrow \text{Lös}(A, \mathbf{o}), \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_k \end{pmatrix} \mapsto \lambda_1 w_1 + \dots + \lambda_k w_k,$$

linear und bijektiv. Diesen Zusammenhang werden wir in 2.3.5 wieder aufgreifen.

Beispiel 2 Sei \mathcal{D} der \mathbb{R} -Vektorraum aller beliebig oft differenzierbaren Funktionen $f : \mathbb{R} \rightarrow \mathbb{R}$. Dann ist die durch die Ableitung erklärte Abbildung

$$D : \mathcal{D} \rightarrow \mathcal{D}, f \mapsto D(f) := f',$$

linear, denn wie man in der Analysis lernt, ist

$$(f + g)' = f' + g' \quad \text{und} \quad (\lambda f)' = \lambda f'.$$

Beispiel 3 Ist \mathcal{I} der \mathbb{R} -Vektorraum aller auf einem Intervall $[a, b] \subset \mathbb{R}$ integrierbaren Funktionen, so ist die Abbildung

$$\mathcal{I} \rightarrow \mathbb{R}, f \mapsto \int_a^b f(x) dx,$$

linear. Das folgt aus den entsprechenden Rechenregeln für Integrale.

Beispiel 4 Wir geben drei verschiedene lineare Abbildungen des Vektorraums $K[X]$ der Polynome über einem Körper K der Charakteristik $\text{char}(K) = 0$ in sich an. Analog zu Beispiel 2 hat man die Differentiation

$$D : K[X] \rightarrow K[X], f = a_n X^n + \dots + a_1 X + a_0 \mapsto f' = n a_n X^{n-1} + \dots + a_1.$$

Die Integration von Polynomen ergibt

$$I : K[X] \rightarrow K[X], f = a_n X^n + \dots + a_1 X + a_0 \mapsto I(f) := \frac{a_n}{n+1} X^{n+1} + \dots + a_0 X.$$

$I(f)$ ist eine Stammfunktion von f .

Ist $g \in K[X]$ ein fest gewähltes Polynom, so hat man eine Multiplikation mit g

$$\mu_g : K[X] \rightarrow K[X], f \mapsto fg.$$

Nach den Rechenregeln im Polynomring (vgl. 1.4.2) gilt

$$(f_1 + f_2)g = f_1g + f_2g \quad \text{und} \quad (\lambda f)g = \lambda(fg).$$

Also ist die Abbildung μ_g linear.

Spezialfällen von Beispiel 1 mit $K = \mathbb{R}$ und kleinen Dimension n und m werden wir später wieder begegnen im Rahmen der „linearen Geometrie“. Die Vektorräume aus Beispiel 2, 3 und 4 haben unendliche Dimension; sie sind ein weiterer Hinweis auf die Bedeutung der linearen Algebra in der Analysis.

2.3.2 Elementare Eigenschaften linearer Abbildungen

Ist $F : V \rightarrow W$ eine lineare Abbildung, so betrachtet man neben dem **Bild** von F

$$F(V) := \{w \in W : \text{es gibt mindestens ein } v \in V \text{ mit } F(v) = w\}$$

auch den **Kern** von F

$$\text{Ker}(F) := \{v \in V : F(v) = \mathbf{o}\} = F^{-1}(\mathbf{o}) \subset V.$$

Zunächst stellen wir einige elementare Eigenschaften linearer Abbildungen zusammen:

Bemerkung Für eine lineare Abbildung $F : V \rightarrow W$ zwischen K -Vektorräumen V und W gilt:

- a) $F(\mathbf{o}) = \mathbf{o}$ und $F(v - v') = F(v) - F(v')$ für $v, v' \in V$.
 b) Für $v_1, \dots, v_n \in V$ und $\lambda_1, \dots, \lambda_n \in K$ gilt

$$F(\lambda_1 v_1 + \dots + \lambda_n v_n) = \lambda_1 F(v_1) + \dots + \lambda_n F(v_n).$$

Kurz ausgedrückt: F respektiert Linearkombinationen.

- c) $\text{Ker}(F) \subset V$ und $F(V) \subset W$ sind Untervektorräume.
 d) Ist $V = \text{Span}(v_1, \dots, v_n)$, so folgt $F(V) = \text{Span}(F(v_1), \dots, F(v_n))$.
 e) Sind (v_1, \dots, v_n) linear abhängig in V , so sind $(F(v_1), \dots, F(v_n))$ linear abhängig in W .
 f) Sind (w_1, \dots, w_n) linear unabhängig in $F(V)$ und $v_1, \dots, v_n \in V$ mit $F(v_i) = w_i$, so sind (v_1, \dots, v_n) linear unabhängig in V .
 g) Ist F injektiv und sind (v_1, \dots, v_n) linear unabhängig in V , so sind $(F(v_1), \dots, F(v_n))$ linear unabhängig in W .
 h) $\dim F(V) \leq \dim V$ und $\dim F(V) \leq \dim W$.

Beweis a) $F(\mathbf{o}) = F(0 \cdot \mathbf{o}) = 0 \cdot F(\mathbf{o}) = \mathbf{o}$ und
 $F(v - v') = F(v + (-1)v') = F(v) + (-1)F(v') = F(v) - F(v')$.

b) Folgt durch wiederholte Anwendung der Regeln L1 und L2 mit Hilfe der Assoziativität der Addition. Wer ganz präzise sein will, kann auch eine Induktion nach n laufen lassen.

c) Nach a) ist $\mathbf{o} \in \text{Ker}(F)$, also $\text{Ker}(F) \neq \emptyset$. Ist $F(v) = F(v') = \mathbf{o}$, so ist auch

$$F(v + v') = F(v) + F(v') = \mathbf{o} \quad \text{und} \quad F(\lambda v) = \lambda F(v) = \lambda \cdot \mathbf{o} = \mathbf{o}.$$

Ebenfalls nach a) ist $\mathbf{o} \in F(V)$. Ist $w = F(v)$ und $w' = F(v')$, so ist

$$w + w' = F(v) + F(v') = F(v + v') \quad \text{und} \quad \lambda w = \lambda F(v) = F(\lambda v).$$

d) und e) folgen sofort aus b).

f) folgt aus d), denn wären (v_1, \dots, v_n) linear abhängig, so wären auch (w_1, \dots, w_n) linear abhängig.

g) Angenommen $\lambda_1 F(v_1) + \dots + \lambda_n F(v_n) = \mathbf{o}$. Aus der Linearität von F folgt

$$F(\lambda_1 v_1 + \dots + \lambda_n v_n) = \mathbf{o} \in W \quad \text{folgt} \quad \lambda_1 v_1 + \dots + \lambda_n v_n = \mathbf{o} \in V,$$

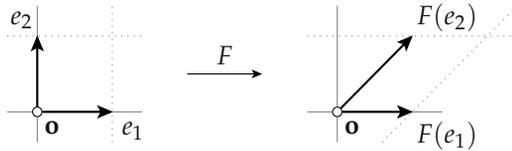
da F injektiv ist. Also ist $\lambda_1 = \dots = \lambda_n = 0$.

h) folgt sofort aus f), zusammen mit dem Basisaustauschsatz aus 2.2.2, sowie dem Korollar aus 2.2.3. ■

Nach Aussage h) kann die Dimension bei einer linearen Abbildung nicht erhöht werden. Für stetige Abbildungen ist das falsch, Gegenbeispiele sind etwa die PEANO-Kurven! Das sind stetige surjektive Abbildungen des Intervalls $I = [0, 1] \subset \mathbb{R}$ auf ein Quadrat $I \times I \subset \mathbb{R}^2$ (vgl. etwa [PE₃] und [HI₁]).

Beispiel 1 Sei $F : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ gegeben durch die Matrix $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Dann ist $F \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ x_2 \end{pmatrix}$, also $F(e_1) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ und $F(e_2) = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.



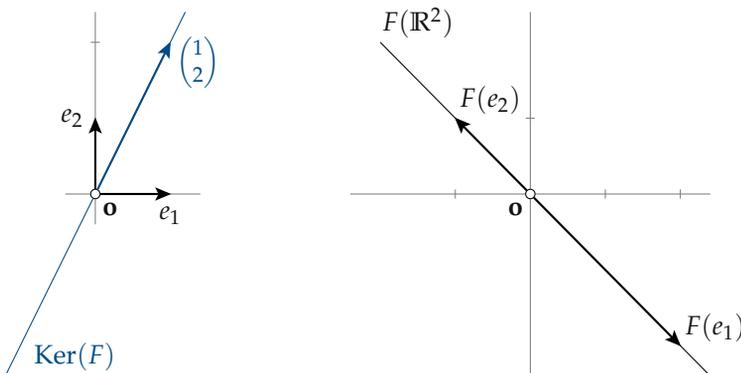
Offensichtlich sind $F(e_1)$ und $F(e_2)$ linear unabhängig, also ist

$$F(V) = \text{Span}(F(e_1), F(e_2)) = \mathbb{R}^2.$$

Für $x \in \text{Ker}(F)$ muss $x_1 + x_2 = 0$ und $x_2 = 0$ sein, also ist $\text{Ker}(F) = \{\mathbf{o}\}$.

Beispiel 2 Sei $F : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ gegeben durch die Matrix $A = \begin{pmatrix} 2 & -1 \\ -2 & 1 \end{pmatrix}$.

Dann ist $F \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 2x_1 - x_2 \\ -2x_1 + x_2 \end{pmatrix}$, also $F(e_1) = \begin{pmatrix} 2 \\ -2 \end{pmatrix}$ und $F(e_2) = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$.



Da $F(e_1) = -2F(e_2)$, sind $F(e_1)$ und $F(e_2)$ linear abhängig, also ist $F(V) = \text{Span} F(e_1)$ eine Gerade.

Für $x \in \text{Ker}(F)$ muss $2x_1 - x_2 = 0$ und $-2x_1 + x_2 = 0$ sein. Also ist auch

$$\text{Ker}(F) = \text{Span} \begin{pmatrix} 1 \\ 2 \end{pmatrix} \text{ eine Gerade.}$$

Beispiel 3 Im Vektorraum $K[X]$ aller Polynome mit Koeffizienten aus einem Körper der Charakteristik $\text{char}(K) = 0$ betrachten wir für jedes $n \in \mathbb{N}$ den Untervektorraum

$$K[X]_n := \{f \in K[X] : \deg f \leq n\}.$$

Eine Basis von $K[X]_n$ ist $(1, X, \dots, X^n)$ also ist $\dim_K K[X]_n = n + 1$. Die in Beispiel 4 aus 2.3.1 betrachtete Ableitung D können wir auf $K[X]_n$ einschränken, das ergibt

$$D : K[X]_n \rightarrow K[X]_n, a_n X^n + \dots + a_1 X + a_0 \mapsto n a_n X^{n-1} + \dots + a_1.$$

Da $D(X^k) = kX^{k-1}$ für $k \geq 1$ ist

$$D(K[X]_n) = \text{Span}(nX^{n-1}, \dots, 1) = K[X]_{n-1}.$$

Weiter ist $\text{Ker}(D) = \text{Span}(X^0)$. Für die Dimensionen gilt

$$\dim D(K[X]_n) = n \quad \text{und} \quad \dim \text{Ker}(D) = 1.$$

Der Leser möge zur Übung Bild und Kern der beiden anderen Abbildungen I und μ_g von Beispiel 4 in 2.3.1 bestimmen.

Beispiel 4 Sei \mathcal{I} der \mathbb{R} -Vektorraum aller stetigen Funktionen

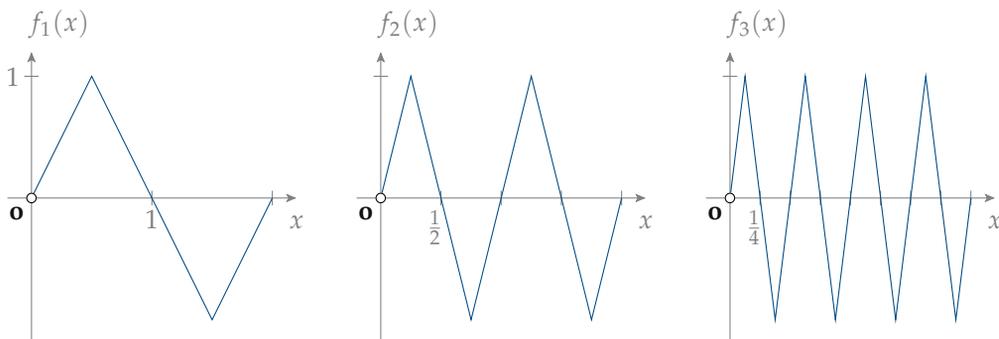
$$f : [a, b] \rightarrow \mathbb{R}$$

und $I : \mathcal{I} \rightarrow \mathbb{R}$ gegeben durch $I(f) := \int_a^b f(x) dx$.

Die Abbildung I ist linear; da konstante Funktionen integrierbar sind, ist $I(\mathcal{I}) = \mathbb{R}$. Wir behaupten nun, dass

$$\dim \text{Ker}(I) = \infty.$$

Dazu genügt es, eine Folge f_1, f_2, \dots von Funktionen $f_k \in \text{Ker}(I)$ zu konstruieren, so dass für jedes $n \in \mathbb{N}^*$ die Funktionen f_1, \dots, f_n linear unabhängig sind. Wir skizzieren eine von vielen Möglichkeiten, wobei $[a, b] = [0, 2]$.



Entscheidend sind die positiven Nullstellen dieser Funktionen. Nach Konstruktion ist

$$f_1(1) = 0, f_2(1) = f_2\left(\frac{1}{2}\right) = 0, f_3(1) = f_3\left(\frac{1}{2}\right) = f_3\left(\frac{1}{4}\right) = 0.$$

Allgemeiner gilt

$$f_k\left(\frac{1}{2^l}\right) = 0 \text{ für } l < k \quad \text{und} \quad f_k\left(\frac{1}{2^l}\right) \neq 0 \text{ für } l \geq k.$$

Zum Nachweis der linearen Unabhängigkeit von (f_1, \dots, f_n) sei

$$\lambda_1 f_1 + \dots + \lambda_n f_n = \mathbf{0}, \text{ d.h. } \lambda_1 f_1(x) + \dots + \lambda_n f_n(x) = 0 \text{ für alle } x \in [0, 2].$$

In diese Beziehung werden nun geeignete Werte von x eingesetzt. Für $x = \frac{1}{2}$ hat man

$$f_1\left(\frac{1}{2}\right) \neq 0 \quad \text{und} \quad f_2\left(\frac{1}{2}\right) = \dots = f_n\left(\frac{1}{2}\right) = 0;$$

daraus folgt $\lambda_1 = 0$. Für $x = \frac{1}{4}$ hat man

$$f_2\left(\frac{1}{4}\right) \neq 0 \quad \text{und} \quad f_3\left(\frac{1}{4}\right) = \dots = f_n\left(\frac{1}{4}\right) = 0;$$

daraus folgt $\lambda_2 = 0$. Durch Fortsetzung dieses Verfahrens erhält man schließlich

$$\lambda_1 = \lambda_2 = \dots = \lambda_n = 0. \quad \blacksquare$$

Ganz analog kann man beweisen, dass die Funktionen

$$\sin x, \sin 2x, \sin 4x, \dots, \sin 2^n x$$

für jedes $n \in \mathbb{N}$ linear unabhängig sind.

Allgemein gilt, dass für jedes $n \in \mathbb{N}^*$ die Funktionen

$$1, \cos x, \dots, \cos nx, \sin x, \dots, \sin nx$$

linear unabhängig sind. Das ist eine Grundlage der Theorie der FOURIER-Reihen (vgl. etwa [FO₁, §23]). Der ganz einfache Spezialfall $n = 1$ wird in Beispiel 9 aus 2.1.4 behandelt.

2.3.3 Spezielle lineare Abbildungen

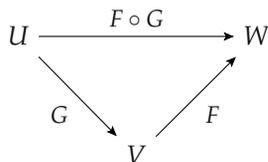
In 1.1.3 hatten wir die Komposition (oder Hintereinanderschaltung) von Abbildungen erklärt. Im Fall linearer Abbildungen benötigt man die elementare

Bemerkung 1 Sind U, V, W Vektorräume über dem selben Körper K , und sind

$$F: V \rightarrow W \quad \text{und} \quad G: U \rightarrow V$$

lineare Abbildungen, so ist auch $F \circ G: U \rightarrow W$ linear.

Die drei beteiligten Abbildungen kann man in ein kleines Diagramm einzeichnen:



Beweis Für $u, u' \in U$ und $\lambda \in K$ gilt

$$\begin{aligned}
 (F \circ G)(u + u') &= F(G(u + u')) = F(G(u) + G(u')) = F(G(u)) + F(G(u')) \\
 &= (F \circ G)(u) + (F \circ G)(u') \text{ und} \\
 (F \circ G)(\lambda u) &= F(G(\lambda u)) = F(\lambda G(u)) = \lambda F(G(u)) \\
 &= \lambda (F \circ G)(u).
 \end{aligned}$$

■

Für spezielle Eigenschaften linearer Abbildungen sind besondere Namen üblich. Eine lineare Abbildung $F : V \rightarrow W$ die auch **Homomorphismus** genannt wird, heißt

Monomorphismus, wenn sie injektiv ist,

Epimorphismus, wenn sie surjektiv ist,

Isomorphismus, wenn sie bijektiv ist,

Endomorphismus, wenn $V = W$ ist und

Automorphismus, wenn sie im Fall $V = W$ bijektiv ist.

Der Leser sollte nicht erschrecken vor dieser Ansammlung von Fremdworten, wir werden sparsam davon Gebrauch machen. Oft benutzt wird der Begriff Isomorphismus. Zwei Vektorräume V und W heißen *isomorph* (das kann man etwa mit „strukturgleich“ übersetzen), wenn es einen Isomorphismus $F : V \rightarrow W$ gibt. Dieser Begriff erfordert noch etwas Erläuterung.

Eine lineare Abbildung

$$f : \mathbb{R} \rightarrow \mathbb{R}, x \mapsto ax,$$

ist genau dann bijektiv, wenn $a \neq 0$; in diesem Fall ist die Umkehrabbildung

$$f^{-1} : \mathbb{R} \rightarrow \mathbb{R} \text{ gegeben durch } y \mapsto x = \frac{1}{a}y,$$

also auch wieder linear. Dass dies ganz allgemein für Isomorphismen zutrifft, zeigt das folgende

Lemma 1 Ist $F : V \rightarrow W$ eine bijektive lineare Abbildung, so ist auch die Umkehrabbildung

$$F^{-1} : W \rightarrow V$$

linear.

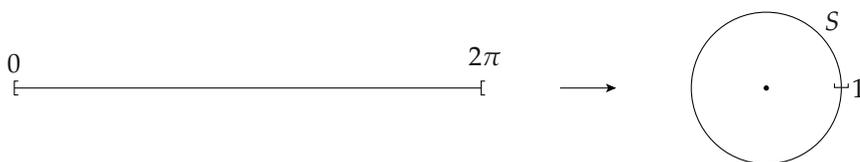
Beweis Seien $w, w' \in W$ und $\lambda \in K$. Da F bijektiv ist, gibt es eindeutig bestimmte $v, v' \in V$ mit $F(v) = w$ und $F(v') = w'$, also ist $F^{-1}(w) = v$ und $F^{-1}(w') = v'$. Da F linear ist, und da $F^{-1} \circ F = \text{id}_V$, folgt

$$\begin{aligned} F^{-1}(w + w') &= F^{-1}(F(v) + F(v')) = F^{-1}(F(v + v')) = v + v' \\ &= F^{-1}(w) + F^{-1}(w') \quad \text{und} \\ F^{-1}(\lambda w) &= F^{-1}(\lambda F(v)) = F^{-1}(F(\lambda v)) = \lambda v \\ &= \lambda F^{-1}(w). \end{aligned}$$

■

Es sei bemerkt, dass diese Aussage nicht selbstverständlich ist, ein Analogon für stetige Abbildungen gilt nicht. Als Beispiel betrachte man die Abbildung

$$f : [0, 2\pi[\rightarrow S := \{z \in \mathbb{C} : |z| = 1\}, \quad t \mapsto e^{it}.$$



f ist stetig und bijektiv, aber die Umkehrabbildung

$$f^{-1} : S \rightarrow [0, 2\pi[$$

ist an der Stelle $1 \in S$ nicht stetig! Um das zu sehen betrachte man die Bilder unter f^{-1} von einer Punktfolge, die in S „von unten“ gegen 1 konvergiert.

Unter den linearen Abbildungen sind auch diejenigen ausgezeichnet, die zwar nicht bijektiv aber immerhin injektiv sind. Ist nämlich $F : V \rightarrow W$ injektiv, so kann man W verkleinern zum Untervektorraum $W' = F(V)$, und die so durch Einschränkung des Bildes erhaltene Abbildung

$$F' : V \rightarrow W' = F(V) \subset W$$

ist bijektiv, also ein Isomorphismus. Also ist V isomorph zu einem Untervektorraum von W .

Die Injektivität einer Abbildung $F : V \rightarrow W$ bedeutet nach Definition, dass jedes $w \in F(V)$ genau ein Urbild hat. Ist F linear, so gilt $F(\mathbf{o}) = \mathbf{o}$, also ist bei einer injektiven linearen Abbildung $\text{Ker}(F) = \{\mathbf{o}\}$. Diese Bedingung ist auch hinreichend, das ist sehr nützlich beim Nachweis der Injektivität:

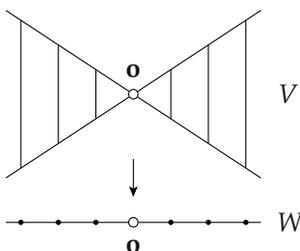
Lemma 2 Eine lineare Abbildung $F : V \rightarrow W$ mit $\text{Ker}(F) = \{\mathbf{o}\}$ ist injektiv.

Beweis Ist $F(v) = F(v')$ für $v, v' \in V$, so folgt

$$F(v - v') = F(v) - F(v') = \mathbf{o}, \text{ also } v - v' \in \text{Ker}(F).$$

Die Voraussetzung ergibt $v - v' = \mathbf{o}$, also $v = v'$. ■

Geometrisch kann man sich vorstellen, dass eine lineare Abbildung nicht so aussehen kann, wie die gezeichnete Projektion, bei der V kein Vektorraum ist.



Nach diesen allgemeinen Vorbereitungen liegt es nahe zu fragen, „wie viele“ lineare Abbildungen es zwischen zwei Vektorräumen V und W gibt. Dazu betrachtet man die Menge

$$\text{Hom}(V, W) := \{F : V \rightarrow W : F \text{ ist linear}\}.$$

Das ist offenbar eine Teilmenge des Vektorraums $\text{Abb}(V, W)$ aller Abbildungen von V nach W (Beispiel 2 in 2.1.1). Nun ist es einfach zu sehen, dass

$$\text{Hom}(V, W) \subset \text{Abb}(V, W)$$

ein Untervektorraum ist. Dazu betrachten wir $F, G \in \text{Hom}(V, W)$ und $\lambda \in K$. Dass $F + G$ wieder linear ist, folgt nach der Definition von $F + G$ aus

$$\begin{aligned} (F + G)(v + v') &= F(v + v') + G(v + v') = F(v) + F(v') + G(v) + G(v') \\ &= F(v) + G(v) + F(v') + G(v') = (F + G)(v) + (F + G)(v') \quad \text{und} \\ (F + G)(\lambda v) &= F(\lambda v) + G(\lambda v) = \lambda F(v) + \lambda G(v) \\ &= \lambda(F(v) + G(v)) = \lambda(F + G)(v). \end{aligned}$$

Analog zeigt man, dass λF wieder linear ist.

Die Frage „wie viele“ Homomorphismen es gibt, kann man nun präzisieren zur Frage nach der Dimension des Vektorraums $\text{Hom}(V, W)$. In 2.4.2, Bemerkung 2, werden wir sehen, dass

$$\dim \text{Hom}(V, W) = (\dim V) \cdot (\dim W).$$

Im Spezialfall $W = V$ hat man den Vektorraum

$$\text{End}(V) := \text{Hom}(V, V)$$

der Endomorphismen von V . Hier hat man eine weitere Verknüpfung, denn nach Bemerkung 1 gilt

$$F, G \in \text{End}(V) \Rightarrow F \circ G \in \text{End}(V).$$

Diese Komposition von Abbildungen kann man als eine Art von „Multiplikation“ ansehen. Wieder reine Rechenarbeit ist der Beweis von folgender

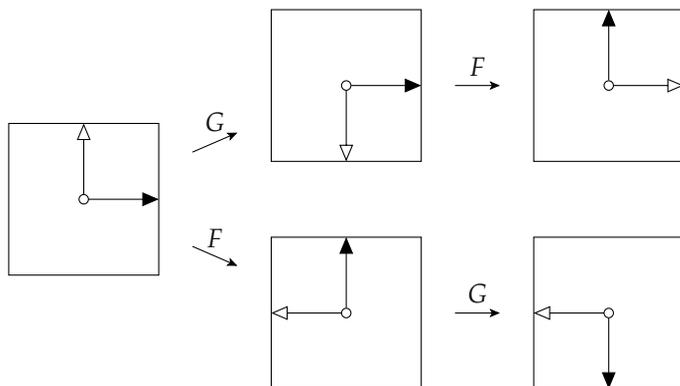
Bemerkung 2 Für jeden Vektorraum V ist die Menge $\text{End}(V)$ der Endomorphismen zusammen mit der oben erklärten Addition von Abbildungen und der Komposition ein Ring mit der Nullabbildung als Nullelement und der identischen Abbildung id_V als Einselement. ■

Im einfachsten Fall $V = K$ ist jeder Endomorphismus von der Form

$$F(x) = ax \quad \text{mit } a \in K.$$

Also ist der Ring $\text{End}(K)$ isomorph zum Körper K .

Im Allgemeinen ist der Ring $\text{End}(V)$ nicht kommutativ, das sieht man schon im Fall $V = \mathbb{R}^2$. Ist etwa F eine Drehung um 90° und G eine Spiegelung an der x -Achse, so erhält man folgendes Bild:



Offensichtlich ist in diesem Fall $G \circ F = -F \circ G$. Das kann man auch durch Rechnung mit Matrizen beweisen, darauf kommen wir in 2.4.5 zurück.

2.3.4 Eine Dimensionsformel für lineare Abbildungen

Bei linearen Abbildungen werden im allgemeinen die Dimensionen der beteiligten Vektorräume verändert. In diesem Abschnitt wird bewiesen, dass es dafür eine präzise Regel gibt. Diese hat zahlreiche Folgerungen, insbesondere für das grundlegende Problem

der Dimensionen des Lösungsraumes eines linearen Gleichungssystems. In Teil h) der Bemerkung aus 2.3.2 hatten wir gesehen, dass stets $\dim F(V) \leq \dim V$ gilt. Diese Aussage kann präzisiert werden:

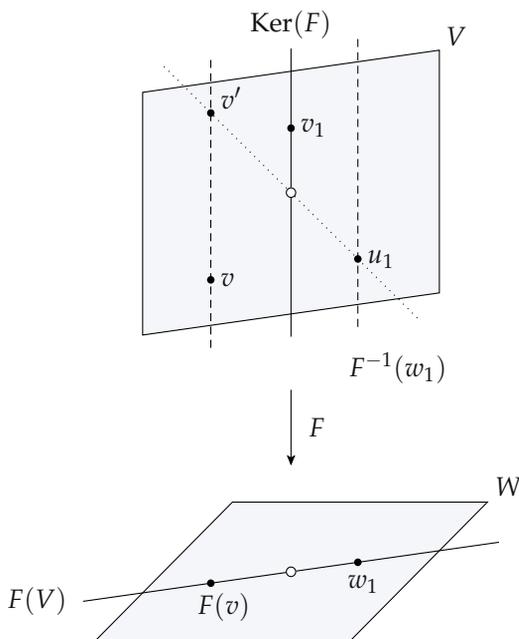
Dimensionsformel für lineare Abbildungen Ist $F : V \rightarrow W$ eine lineare Abbildung zwischen K -Vektorräumen V und W , sei $\dim V < \infty$. Dann ist $\dim F(V) < \infty$ und es ist

$$\dim V = \dim F(V) + \dim \text{Ker}(F).$$

Genauer gilt: Ist (w_1, \dots, w_r) eine Basis von $F(V)$, (v_1, \dots, v_k) eine Basis von $\text{Ker}(F)$ und seien $u_1 \in F^{-1}(w_1), \dots, u_r \in F^{-1}(w_r)$ beliebig, so ist $\mathcal{B} = (u_1, \dots, u_r, v_1, \dots, v_k)$ eine Basis von V .

Man beachte, dass die Dimension von W in dieser Formel nicht vorkommt. Sie kann beliebig viel größer sein, als die Dimension von $F(V)$.

Im Spezialfall $k = r = 1$ kann man sich F als senkrechte Projektion zwischen zwei Ebenen vorstellen.



Von den zahlreichen Folgerungen vermerken wir zunächst ein Analogon zum „Apfel-Lemma“ für endliche Mengen aus 1.1.3.

Korollar Für eine lineare Abbildung $F : V \rightarrow W$ sind im Fall $\dim V = \dim W < \infty$ folgende Bedingungen äquivalent:

i) F ist injektiv,

ii) F ist surjektiv,

iii) F ist bijektiv.

Beweis des Korollars i) \Rightarrow ii) Aus $\dim \text{Ker}(F) = 0$ folgt $\dim V = \dim F(V)$, also $F(V) = W$ nach Korollar 3 aus 2.2.2.

ii) \Rightarrow iii) Aus $\dim F(V) = \dim W$ folgt $\dim \text{Ker}(F) = 0$. Also ist F auch injektiv nach Lemma 2 aus 2.3.3.

iii) \Rightarrow i) ist klar. ■

Beweis der Dimensionsformel Zunächst zeigen wir, dass $V = \text{Span}(\mathcal{B})$. Zu $v \in V$ gibt es $\mu_1, \dots, \mu_r \in K$, so dass

$$F(v) = \mu_1 w_1 + \dots + \mu_r w_r. \quad \text{Sei } v' := \mu_1 u_1 + \dots + \mu_r u_r.$$

Dann ist $F(v') = F(v)$, also $v - v' \in \text{Ker}(F)$ und es gibt $\lambda_1, \dots, \lambda_k \in K$ so dass

$$v - v' = \lambda_1 v_1 + \dots + \lambda_k v_k.$$

Daraus folgt $v = v' + (v - v') = \mu_1 u_1 + \dots + \mu_r u_r + \lambda_1 v_1 + \dots + \lambda_k v_k$.

Zum Nachweis der linearen Unabhängigkeit von \mathcal{B} sei

$$\mu_1 u_1 + \dots + \mu_r u_r + \lambda_1 v_1 + \dots + \lambda_k v_k = \mathbf{0}. \quad (*)$$

Anwendung von F auf diese Relation ergibt

$$\mathbf{0} = \mu_1 F(u_1) + \dots + \mu_r F(u_r) + \mathbf{0} = \mu_1 w_1 + \dots + \mu_r w_r,$$

also folgt $\mu_1 = \dots = \mu_r = 0$. Setzt man das in (*) ein, so folgt $\lambda_1 = \dots = \lambda_k = \mathbf{0}$. ■

2.3.5 Lineare Gleichungssysteme

Mit Hilfe der bisherigen Ergebnisse dieses Kapitels über Basis, Dimension und lineare Abbildungen können wir nun das Problem der Lösung linearer Gleichungssysteme noch einmal von einem höheren Standpunkt betrachten und dabei die in 0.5.4 offen gebliebenen Fragen beantworten. Entscheidend ist folgender offensichtlicher Zusammenhang.

Zu einem linearen Gleichungssystem

$$Ax = b \quad \text{mit } A \in M(m \times n; K) \quad \text{und } b \in K^m$$

gehört eine durch A bestimmte lineare Abbildung (Beispiel 1 in 2.3.1)

$$F_A : K^n \rightarrow K^m, x \mapsto Ax,$$

und für den Lösungsraum von $Ax = b$ gilt offensichtlich

$$\text{Lös}(A, b) = \{x \in K^n : Ax = b\} = F_A^{-1}(b),$$

d.h. er ist das Urbild von b unter der linearen Abbildung F_A . Insbesondere gilt für ein homogenes System

$$\text{Lös}(A, \mathbf{0}) = \text{Ker}(F_A).$$

Bevor wir diese Spur weiter verfolgen, ein ganz einfaches

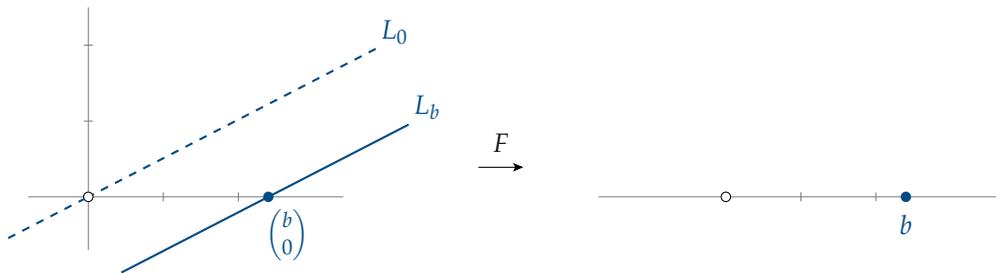
Beispiel 1 Im Fall $K = \mathbb{R}$ und $n = 2, m = 1$ hat man eine einzige Gleichung

$$a_1x_1 + a_2x_2 = b,$$

die Lösungsmenge ist eine Gerade in \mathbb{R}^2 . Die zugehörige lineare Abbildung ist

$$F : \mathbb{R}^2 \rightarrow \mathbb{R}, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto a_1x_1 + a_2x_2.$$

Ist etwa $a_1 = 1$ und $a_2 = 2$, so ist $F(\mathbb{R}^2) = \mathbb{R}$ und $\text{Ker}(F)$ ist eine Gerade $L_0 \subset \mathbb{R}^2$ durch $\mathbf{0}$.



Für ein beliebiges $b \in \mathbb{R}$ ist $\begin{pmatrix} b \\ 0 \end{pmatrix} \in F^{-1}(b)$, also ist

$$L_b := F^{-1}(b) = \begin{pmatrix} b \\ 0 \end{pmatrix} + L_0$$

die zu L_0 parallele Gerade durch $\begin{pmatrix} b \\ 0 \end{pmatrix}$. Insbesondere gilt für die Dimensionen der beteiligten Räume und die Koeffizientenmatrix $A = (1, 2)$, dass

$$1 = \dim L_0 = n - \text{rang } A = 2 - 1.$$

Dass diese Beziehung allgemein gilt, besagt das zentrale

Lemma Ist $A \in M(m \times n; K)$ die Koeffizientenmatrix eines homogenen linearen Gleichungssystems, so ist der Lösungsraum

$$\text{Lös}(A, \mathbf{o}) = \{x \in K^n : Ax = \mathbf{o}\} \subset K^n$$

ein Untervektorraum, und für seine Dimension gilt

$$\dim \text{Lös}(A, \mathbf{o}) = n - \text{rang } A.$$

Beweis Wie schon zu Beginn dieses Abschnitts ausgeführt, ist

$$\text{Lös}(A, \mathbf{o}) = \text{Ker}(F_A), \quad \text{also} \quad \dim \text{Lös}(A, \mathbf{o}) = n - \dim F_A(K^n)$$

nach der Dimensionsformel aus 2.3.4. Es bleibt also nur noch zu zeigen, dass

$$\dim F_A(K^n) = \text{rang } A. \quad (*)$$

Nach Teil d) der Bemerkung aus 2.3.2 wird das Bild $F_A(K^n)$ erzeugt von den Bildern $F_A(e_1), \dots, F_A(e_n)$ der kanonischen Basisvektoren des K^n . Wie in Beispiel 1 aus 2.3.1 ausgeführt wird, sind das die Spaltenvektoren von A , also ist

$$\dim F_A(K^n) = \text{Spaltenrang}(A) = \text{rang } A.$$

An dieser Stelle ist die in 2.2.6 bewiesene Gleichheit von Zeilenrang und Spaltenrang entscheidend. Bei der Elimination in 0.5.4 wird der Zeilenrang bestimmt, in der verwendeten Dimensionsformel für lineare Abbildungen tritt der Spaltenrang auf! ■

Ist ein lineares Gleichungssystem $Ax = b$ inhomogen, d.h. ist $b \neq \mathbf{o}$, so kann $x = \mathbf{o}$ keine Lösung sein, also ist auch $\text{Lös}(A, b) \subset K^n$ kein Untervektorraum. Wie wir schon in den Beispielen gesehen haben, steht er aber in enger Beziehung zum Untervektorraum $\text{Lös}(A, \mathbf{o})$: der wird einfach in passender Weise parallel verschoben. Dafür ist ein eigener Name üblich.

Definition Ist V ein Vektorraum, so heißt eine Teilmenge $L \subset V$ ein **affiner Unterraum**, wenn es einen Untervektorraum $L_0 \subset V$ und ein $v \in V$ gibt, so dass

$$L = v + L_0 = \{v + u : u \in L_0\}.$$

Um Fallunterscheidungen zu vermeiden, darf sich auch die leere Menge als affiner Unterraum bezeichnen.

Beispiele für affine Unterräume hatten wir schon in Kapitel 0 kennengelernt: Geraden und Ebenen im \mathbb{R}^n . Wie in diesen Spezialfällen beweist man, dass $v \in L$ beliebig gewählt

werden kann, L_0 dagegen eindeutig bestimmt ist als Menge der Differenzen aus L (vgl. die Bemerkung in 0.4.1). Daher kann man die *Dimension* von $L = v + L_0$ erklären als

$$\dim L := \dim L_0.$$

Affine Unterräume stehen in engem Zusammenhang mit linearen Abbildungen:

Bemerkung Ist $F : V \rightarrow W$ linear und $w \in W$, so ist das Urbild $F^{-1}(w) \subset V$ ein affiner Unterraum. Ist $w \in F(V)$ und $v \in F^{-1}(w)$ beliebig, so gilt

$$F^{-1}(w) = v + \text{Ker } F.$$

Beweis Ist $w \notin F(V)$, so ist $F^{-1}(w) = \emptyset$, also affiner Unterraum. Andernfalls gilt für jedes $v' \in F^{-1}(w)$, dass $F(v') = F(v)$, also

$$v' - v \in \text{Ker } F \quad \text{und} \quad v' = v + (v' - v) \in v + \text{Ker } F.$$

Ist umgekehrt $u \in \text{Ker } F$, so gilt

$$F(v + u) = F(v) = w, \quad \text{also} \quad v + u \in F^{-1}(w). \quad \blacksquare$$

Schließlich ist es von Vorteil, eine einfach zu formulierende Bedingung dafür zu haben, dass der Lösungsraum $\text{Lös}(A, b)$ eines inhomogenen Systems nicht leer ist. Bringt man die erweiterte Koeffizientenmatrix (A, b) durch Zeilenumformungen auf Zeilenstufenform (\tilde{A}, \tilde{b}) , so folgt durch Betrachtung der Zeilenränge, dass

$$\text{rang } \tilde{A} = \text{rang } A \quad \text{und} \quad \text{rang}(\tilde{A}, \tilde{b}) = \text{rang}(A, b). \quad (*)$$

Betrachtet man nun die Einträge $\tilde{b}_{r+1}, \dots, \tilde{b}_m$ von \tilde{b} , so gilt wie in 0.5 gezeigt, dass

$$\text{Lös}(A, b) = \text{Lös}(\tilde{A}, \tilde{b}) \neq \emptyset \Leftrightarrow \tilde{b}_{r+1} = \dots = \tilde{b}_m = 0. \quad (**)$$

Durch Betrachtung der Spaltenränge sieht man sofort, dass

$$\tilde{b}_{r+1} = \dots = \tilde{b}_m = 0 \Leftrightarrow \text{rang}(\tilde{A}, \tilde{b}) = \text{rang } \tilde{A}.$$

Zusammen mit (*) und (**) ergibt sich daraus die Bedingung

$$\text{Lös}(A, b) \neq \emptyset \Leftrightarrow \text{rang}(A, b) = \text{rang } A.$$

Dabei ist zu bedenken, dass ganz allgemein $\text{rang } A \leq \text{rang}(A, b) \leq \text{rang } A + 1$ gilt.

Insgesamt erhalten wir für lineare Gleichungssysteme das folgende abschließende Ergebnis:

Theorem Gegeben sei ein lineares Gleichungssystem $Ax = b$, wobei $A \in M(m \times n; K)$ über einem beliebigen Körper K und $b \in K^m$. Dann ist der Lösungsraum

$$\text{Lös}(A, b) = \{x \in K^n : Ax = b\} \subset K^n$$

ein affiner Unterraum. Es gilt

$$\text{Lös}(A, b) \neq \emptyset \Leftrightarrow \text{rang}(A, b) = \text{rang } A.$$

Ist dies der Fall, so folgt

$$\text{Lös}(A, b) = v + \text{Lös}(A, \mathbf{o}),$$

wobei $v \in \text{Lös}(A, b)$ beliebig gewählt werden kann. Insbesondere gilt

$$\dim \text{Lös}(A, b) = n - \text{rang } A.$$

Das ist das wichtigste Ergebnis der elementaren linearen Algebra. Es zeigt insbesondere, dass die bei dem in 0.5.3 angegebenen Verfahren erhaltene Zahl r als Rang von A und $k = n - r$ als Dimension des Lösungsraums eindeutig bestimmt sind und eine präzise geometrische Bedeutung haben. In 0.5.3 war stets $K = \mathbb{R}$ vorausgesetzt gewesen, aber alle benutzten Argumente bleiben in einem beliebigen Körper gültig. Wir wollen die Ergebnisse aus 0.5.3 noch einmal vom Standpunkt linearer Abbildungen beleuchten.

Die Matrix $A \in M(m \times n; K)$ beschreibt eine lineare Abbildung, die wir zur Vereinfachung mit dem gleichen Buchstaben bezeichnen:

$$A : K^n \rightarrow K^m, x \mapsto Ax.$$

Da $A(K^n) \subset K^m$ nach 2.3.1 von den Spaltenvektoren von A aufgespannt wird, ist

$$A(K^n) = K^r = \{^t(y_1, \dots, y_r, y_{r+1}, \dots, y_m) \in K^m : y_{r+1} = \dots = y_m = 0\},$$

falls A in Zeilenstufenform mit den Pivotpositionen $j_1 = 1, \dots, j_r = r$ ist. In diesem Falle kann man wie für $K = \mathbb{R}$ in 0.5.3 eine Matrix

$$D = \begin{pmatrix} d_{11} & \cdots & d_{1k} \\ \vdots & & \vdots \\ d_{r1} & \cdots & d_{rk} \\ 1 & 0 & \cdots & 0 \\ \vdots & \ddots & & \vdots \\ 0 & \cdots & 0 & 1 \end{pmatrix} \in M(n \times k; K)$$

berechnen, so dass für die durch D erklärte lineare Abbildung

$$D : K^k \rightarrow K^n, \lambda \mapsto D\lambda,$$

das Bild in $\text{Ker}(A)$ enthalten ist. Wie man D sofort ansieht, ist $\text{rang } D = k$, also gilt

$$\dim D(K^k) = k = n - r = \dim \text{Ker}(A).$$

Somit ist $D(K^k) = \text{Ker}(A) = \text{Lös}(A, \mathbf{o})$. Daraus folgt, dass der Lösungsraum des homogenen Systems $Ax = \mathbf{o}$ aufgespannt wird von den linear unabhängigen Spaltenvektoren w_1, \dots, w_k von D . Somit ist

$$(w_1, \dots, w_k) \text{ eine Basis von } \text{Lös}(A, \mathbf{o}).$$

Insgesamt erhalten wir zu einer Matrix A in Zeilenstufenform eine Folge linearer Abbildungen

$$K^k \xrightarrow{D} K^n \xrightarrow{A} K^r,$$

mit folgenden Eigenschaften: D ist injektiv, A ist surjektiv und $D(K^k) = \text{Ker}(A)$.

Zur Lösung eines inhomogenen Systems $Ax = b$ mit

$$b = {}^t(b_1, \dots, b_r, b_{r+1}, \dots, b_m) \neq \mathbf{o} \in K^m$$

genügt eine einfache Zusatzüberlegung. Ist – wie schon oben vorausgesetzt – A in Zeilenstufenform, so liegt b genau dann im Bild $A(K^n) \subset K^m$, wenn

$$b_{r+1} = \dots = b_m = 0,$$

und genau dann ist $\text{Lös}(A, b) \neq \emptyset$. Ist das der Fall, so kann man wie in 0.5.3 eine spezielle Lösung

$$v = {}^t(c_1, \dots, c_r, 0, \dots, 0) \in \text{Lös}(A, b) \subset K^n$$

erhalten, indem man $\lambda_1 = \dots = \lambda_k = 0$ setzt, und $\text{Lös}(A, b) \subset K^n$ ist das Bild der Abbildung

$$\varphi : K^k \rightarrow K^n, \lambda \mapsto v + D\lambda.$$

Wie man die Transformation der Koeffizientenmatrix auf Zeilenstufenform als lineare Abbildung interpretieren kann, werden wir in 2.4.7 erläutern.

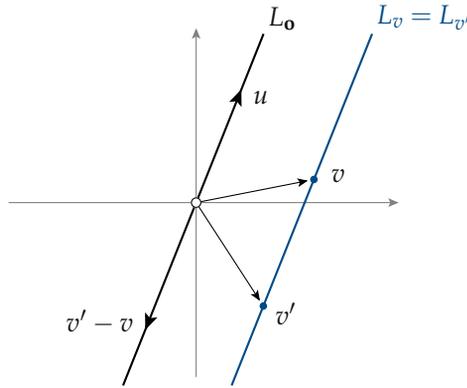
2.3.6 Quotientenvektorräume*

Ist in der Ebene \mathbb{R}^2 ein Vektor $u \neq \mathbf{o}$ gegeben, so ist $L_{\mathbf{o}} := \mathbb{R} \cdot u$ eine Gerade durch \mathbf{o} und für jedes beliebige $v \in \mathbb{R}^2$ ist

$$L_v := v + L_{\mathbf{o}}$$

eine zu $L_{\mathbf{o}}$ parallele Gerade. Wie man sich leicht überzeugt, gilt für beliebige $v, v' \in \mathbb{R}^2$

$$L_v = L_{v'} \Leftrightarrow v' - v \in L_{\mathbf{o}}.$$



Nun bezeichnen wir mit M die Menge aller zu L_0 parallelen Geraden. Man beachte, dass ein Element $L_v \in M$ eine Teilmenge $L_v \subset \mathbb{R}^2$ ist. Mit Hilfe der Vektorraumstruktur von \mathbb{R}^2 kann man nun auch M zu einem \mathbb{R} -Vektorraum machen. Die Summen von zwei Geraden und das Vielfache einer Geraden sollen dazu erklärt werden durch

$$L_v + L_w := L_{v+w} \quad \text{und} \quad \lambda \cdot L_v := L_{\lambda \cdot v},$$

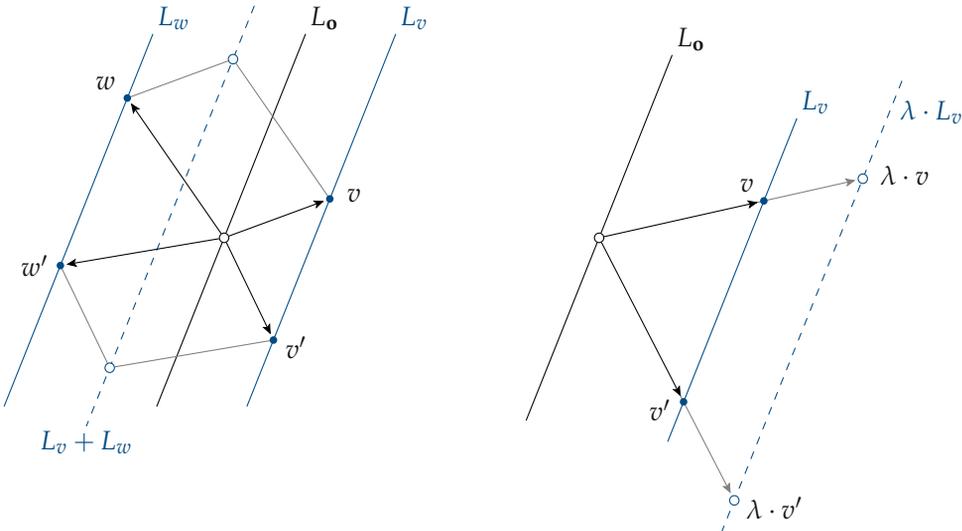
wobei $v, w \in \mathbb{R}^2$ und $\lambda \in \mathbb{R}$. Da der Aufhängepunkt v einer Geraden L_v nicht eindeutig bestimmt ist, muss man zeigen, dass diese Definitionen unabhängig von den Repräsentanten sind. Seien also

$$L_v = L_{v'} \quad \text{und} \quad L_w = L_{w'}, \quad \text{also} \quad v' - v, w' - w \in L_0.$$

Da $L_0 \subset \mathbb{R}^2$ ein Untervektorraum ist, folgt

$$(v' + w') - (v + w) = (v' - v) + (w' - w) \in L_0 \quad \text{und} \quad \lambda \cdot v' - \lambda \cdot v = \lambda \cdot (v' - v) \in L_0,$$

also ist $L_{v'+w'} = L_{v+w}$ und $L_{\lambda \cdot v'} = L_{\lambda \cdot v}$. Damit ist gezeigt, dass Addition und Multiplikation mit Skalaren in M wohldefiniert sind.



Die gerade im \mathbb{R}^2 beschriebene Konstruktion kann man allgemeiner ausführen, wenn in einem beliebigen K -Vektorraum V ein Untervektorraum $U \subset V$ gegeben ist. Dann kann man in V eine Äquivalenz modulo U erklären durch

$$v \sim_U v' \quad :\Leftrightarrow \quad v' - v \in U.$$

Dass dadurch eine Äquivalenzrelation erklärt ist, folgt sofort aus den Eigenschaften eines Untervektorraums. Außerdem sieht man leicht, dass die Äquivalenzklasse eines $v \in V$ der affine Unterraum

$$L_v := v + U \subset V$$

ist. Nun bezeichnen wir mit V/U (sprich V modulo U) die Menge dieser Äquivalenzklassen und mit

$$\varrho : V \rightarrow V/U, \quad v \mapsto L_v,$$

die kanonische Abbildung. Ergebnis dieses Abschnitts ist der

Satz über den Quotientenvektorraum *Ist V ein K -Vektorraum und $U \subset V$ ein Untervektorraum, so kann man die Menge V/U der Äquivalenzklassen modulo U auf genau eine Weise so zu einem K -Vektorraum machen, dass die kanonische Abbildung*

$$\varrho : V \rightarrow V/U, \quad v \mapsto v + U,$$

linear wird. Dann ist $\text{Ker } \varrho = U$. Ist $\dim V < \infty$, so gilt

$$\dim V/U = \dim V - \dim U.$$

Man nennt V/U den **Quotientenvektorraum** von V modulo U , oder V nach U . Im Fall $U = \{\mathbf{o}\}$ ist $\varrho : V \rightarrow V/\{\mathbf{o}\}$ ein Isomorphismus

Beweis Wir können uns ganz an dem obigen Beispiel der parallelen Geraden in \mathbb{R}^2 orientieren. Wenn ϱ ein Homomorphismus werden soll, so bedeutet das

$$\begin{aligned} \varrho(v+w) &\stackrel{!}{=} \varrho(v) + \varrho(w), & \text{also} & \quad (v+w) + U \stackrel{!}{=} (v+U) + (w+U) \quad \text{und} \\ \varrho(\lambda \cdot v) &\stackrel{!}{=} \lambda \cdot \varrho(v), & \text{also} & \quad \lambda \cdot v + U \stackrel{!}{=} \lambda \cdot (v+U). \end{aligned}$$

Die einzig mögliche Definition unter der vorgegebenen Bedingung ist also

$$(v+U) + (w+U) := (v+w) + U \quad \text{und} \quad \lambda \cdot (v+U) := \lambda \cdot v + U.$$

Wie im Beispiel der Geraden sieht man, dass dadurch Addition und Multiplikation wohldefiniert sind. Der Nachweis der Vektorraumaxiome ist ganz einfach, denn die Regeln übertragen sich mühelos von V nach V/U . Nullelement in V/U ist der Untervektorraum $U \subset V$, denn

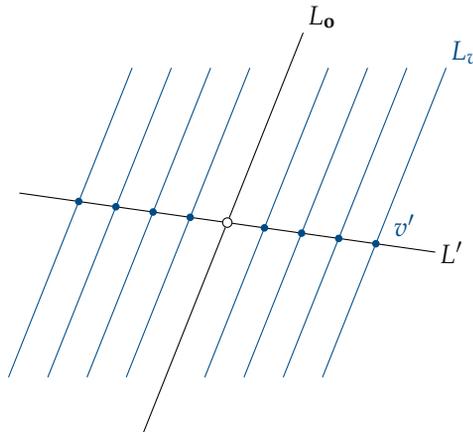
$$U = \mathbf{o} + U, \quad \text{also} \quad U + (v+U) = (\mathbf{o} + U) + (v+U) = v + U.$$

Da $v + U = U \Leftrightarrow v \in U$ ist $\text{Ker } \varrho = U$. Aus der Dimensionsformel in 2.3.4 folgt im Fall $\dim V < \infty$

$$\dim V = \dim \varrho(V) + \dim \text{Ker } \varrho = \dim V/U + \dim U. \quad \blacksquare$$

Da diese allgemeine Konstruktion sehr abstrakt aussieht, wollen wir zunächst einmal den Quotientenvektorraum \mathbb{R}^2/L_0 mit $L_0 = \mathbb{R} \cdot u$ aus obigem Beispiel noch einmal genauer ansehen. Dazu wählen wir einen von u linear unabhängigen Vektor $u' \in \mathbb{R}^2$ und betrachten die Gerade

$$L' = \mathbb{R} \cdot u' \quad \text{mit} \quad L' \cap L_0 = \{0\}.$$

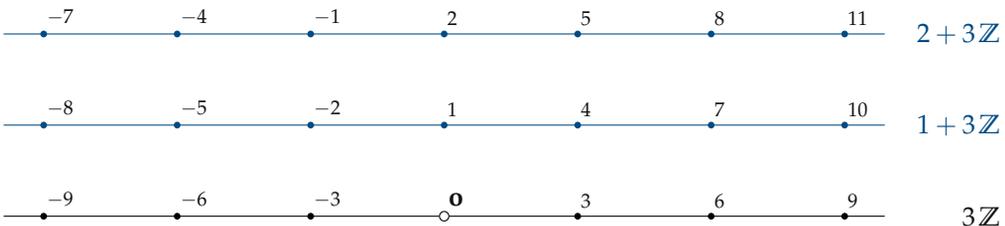


Jede Gerade $L_v \in \mathbb{R}^2/L_0$ hat mit L' genau einen Schnittpunkt $v' \in L'$; das ergibt eine Abbildung

$$\sigma : \mathbb{R}^2/L_0 \rightarrow L', \quad L_v \mapsto v' = L_v \cap L'.$$

Offensichtlich ist σ bijektiv, und da $L_v = L_{v'}$ für alle $v \in \mathbb{R}^2$, ist σ nach der Definition der Vektorraumstruktur in \mathbb{R}^2/L_0 sogar ein Homomorphismus, insgesamt also ein Isomorphismus. Unser mit etwas Mühe konstruierter Vektorraum ist also isomorph zu einer anderen Geraden $L' \subset \mathbb{R}^2$; allerdings ist L' nicht eindeutig bestimmt, weil es viele Möglichkeiten für die Wahl von u' gibt.

Da Quotientenstrukturen mit Äquivalenzklassen als Elementen erfahrungsgemäß gewöhnungsbedürftig sind, wollen wir den Zusammenhang zwischen der Menge paralleler Geraden und den Restklassen von \mathbb{Z} modulo m aus 1.1.5 auch geometrisch illustrieren. Dazu genügt es, die ganzen Zahlen nicht in einer Geraden, sondern auf m parallelen Geraden anzuordnen. Im Fall $m = 3$ sieht das so aus:



Man beachte, dass es in diesem Fall mit Ausnahme von $m = 1$ keine Untergruppe $G \subset \mathbb{Z}$ und einen Isomorphismus $\mathbb{Z}/m\mathbb{Z} \rightarrow G$ gibt. Das folgt sofort aus dem Lemma über die Untergruppen von \mathbb{Z} in 1.2.5. Quotientenvektorräume sind wichtig in der Analysis beim Studium von Funktionenräumen. Dafür geben wir ein einfaches

Beispiel Im Vektorraum \mathbb{R}^n hatten wir in 0.3.1 als Maß für die Länge eines Vektors $v = (x_1, \dots, x_n)$ die Norm

$$\|v\| = \sqrt{x_1^2 + \dots + x_n^2}$$

eingeführt. In den unendlich-dimensionalen Vektorräumen von Funktionen ist eine solche einfache Definition einer Norm nicht möglich. Als Beispiel betrachten wir ein Intervall $[a, b] \subset \mathbb{R}$ und den Vektorraum

$$\mathcal{F}([a, b]; \mathbb{R}) = \{f : [a, b] \rightarrow \mathbb{R}\}$$

aller auf $[a, b]$ definierten reell-wertigen Funktionen. Auf dem Untervektorraum

$$\mathcal{C} \subset \mathcal{F}([a, b]; \mathbb{R})$$

der stetigen Funktionen kann man für $f \in \mathcal{C}$ eine **Maximums-Norm**

$$\|f\| := \max\{|f(x)| : x \in [a, b]\}$$

erklären. Wie man leicht sieht, hat diese **Norm** die Eigenschaften

$$\|f\| \geq 0 \text{ und } \|f\| = 0 \Leftrightarrow f = \mathbf{o}, \quad \|\lambda \cdot f\| = |\lambda| \cdot \|f\|, \quad \|f + g\| \leq \|f\| + \|g\| \quad (\text{N})$$

für $f, g \in \mathcal{C}$ und $\lambda \in \mathbb{R}$.

Ein größerer Unterraum als \mathcal{C} ist

$$\mathcal{L} := \{f : [a, b] \rightarrow \mathbb{R} : f \text{ ist integrierbar}\},$$

wobei die Größe von \mathcal{L} davon abhängt, ob man das Integral im Sinn von RIEMANN oder LEBESGUE zugrunde legt. Dann kann man als Maß für die Größe von f das Integral

$$I(f) := \int_a^b |f(t)| dt$$

ansehen. Die Abbildung $I : \mathcal{L} \rightarrow \mathbb{R}_+$ kann nicht linear sein, denn \mathbb{R}_+ ist kein \mathbb{R} -Vektorraum. Nach den Rechenregeln für Integrale gilt jedoch

$$I(\lambda \cdot f) = |\lambda| \cdot I(f) \quad \text{und} \quad I(f + g) \leq I(f) + I(g) \quad \text{für } f, g \in \mathcal{L} \text{ und } \lambda \in \mathbb{R}.$$

Es kann aber $I(f) = 0$ sein, ohne dass $f = \mathbf{o}$ ist. Das sind die Funktionen, die „fast überall“ verschwinden, etwa die **Sprungfunktion** von DIRICHLET

$$D(x) = \begin{cases} 0 & \text{falls } x \text{ irrational,} \\ 1 & \text{falls } x \text{ rational.} \end{cases}$$

Sie ist LEBESGUE-integrierbar und $\int_a^b D(t)dt = 0$ für alle Intervalle $[a, b]$.

Um aus der Funktion $I : \mathcal{L} \rightarrow \mathbb{R}_+$ eine Norm zu machen, betrachtet man den Untervektorraum

$$\mathcal{N} := \{f \in \mathcal{L} : I(f) = 0\} \subset \mathcal{L}$$

der fast überall verschwindenden Funktionen. Nun gehen wir zum Quotientenvektorraum

$$L := \mathcal{L}/\mathcal{N}$$

über. Dabei kommen zwei Funktionen $f, g \in \mathcal{L}$ in die gleiche Äquivalenzklasse, wenn $f - g \in \mathcal{N}$, d.h. $f = g$ fast überall.

Nun können wir eine Norm auf L erklären. Ist

$$q : \mathcal{L} \rightarrow \mathcal{L}/\mathcal{N} = L, f \mapsto q(f) = f + \mathcal{N},$$

der kanonische Homomorphismus, so definieren wir

$$\|q(f)\| := I(f).$$

Diese Abbildung ist wohldefiniert, denn ist $q(f) = q(g)$ für $f, g \in \mathcal{L}$, so weiß man aus der Analysis (vgl. etwa [FO₃, §4, Satz 10 c]), dass $I(f) = I(g)$. Die Norm einer Äquivalenzklasse ist also das Integral über den Betrag eines Repräsentanten. Die Null in L ist die Restklasse \mathcal{N} , also gilt

$$\|q(f)\| = 0 \Leftrightarrow I(f) = 0 \Leftrightarrow f \in \mathcal{N} \Leftrightarrow q(f) = \mathcal{N}.$$

Zusammenfassend hat die Abbildung

$$\| \cdot \| : L \rightarrow \mathbb{R}_+, f + \mathcal{N} \mapsto I(f),$$

die oben angegebenen Eigenschaften (N) einer Norm. Diese kann man benutzen um die Güte einer Approximation von Funktionen zu messen. In diesem Fall gibt es keinen für die Analysis brauchbaren Untervektorraum $L' \subset \mathcal{L}$ derart, dass die Beschränkung $q' : L' \rightarrow L$ von q ein Isomorphismus ist.

2.4 Lineare Abbildungen und Matrizen

Zwischen Matrizen und linearen Abbildungen besteht ein enges Wechselspiel. In Beispiel 1 aus 2.3.1 hatten wir jeder Matrix $A \in M(m \times n; K)$ eine lineare Abbildung $F: K^n \rightarrow K^m$ zugeordnet, und in 2.3.5 hatten wir gesehen, wie nützlich diese Interpretation einer Matrix bei der Lösung linearer Gleichungssysteme sein kann. In den folgenden Abschnitten wird der Zusammenhang zwischen Matrizen und linearen Abbildungen bei endlich-dimensionalen Vektorräumen im allgemeineren Rahmen studiert.

Allgemein kann man die Matrizen in der linearen Algebra als eine Art von „Buchhaltern“ betrachten. Das Wechselspiel mit der allgemeinen Theorie ist nützlich für beide: Mit Matrizen kann man Vieles übersichtlich ausrechnen, und die Operationen mit Matrizen erhalten durch die Theorie eine klare Interpretation.

2.4.1 Erzeugung linearer Abbildungen

Zur Definition einer Abbildung $f: M \rightarrow N$ zwischen Mengen muss man eine Vorschrift angeben, wie zu jedem $x \in M$ ein Bild $f(x) \in N$ erhalten wird. Solch eine Vorschrift kann ziemlich kompliziert sein. Lineare Abbildungen zwischen Vektorräumen sind dagegen durch relativ wenige Vorgaben zu erklären.

Beispiel Um eine lineare Abbildung $F: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ festzulegen kann man zunächst die Bilder einiger Punkte vorgeben. Für $\mathbf{o} \in \mathbb{R}^2$ gibt es keine Wahl, es muss $F(\mathbf{o}) = \mathbf{o}$ sein. Für ein $v_1 \neq \mathbf{o}$ dagegen kann man $F(v_1)$ ganz beliebig wählen. Kommt ein v_2 dazu, entsteht das erste Problem:

- Ist $v_2 = \lambda v_1$, so muss $F(v_2) = \lambda F(v_1)$ sein, eine andere Wahl gibt es nicht.
- Ist $v_2 \notin \mathbb{R} \cdot v_1$, so kann man auch noch $F(v_2)$ beliebig wählen.

Hat man schließlich v_1, v_2, v_3 mit $v_1 \neq \mathbf{o}$ und $v_2 \notin \mathbb{R} \cdot v_1$, so sind (v_1, v_2) eine Basis von \mathbb{R}^2 , also muss

$$v_3 = \lambda_1 v_1 + \lambda_2 v_2 \quad \text{und} \quad F(v_3) = \lambda_1 F(v_1) + \lambda_2 F(v_2)$$

sein. Also ist F auf ganz \mathbb{R}^2 durch die Werte $F(v_1)$ und $F(v_2)$ festgelegt. Eine präzise Begründung dafür liefert der folgende

Satz über die Erzeugung linearer Abbildungen Gegeben seien K -Vektorräume V und W , sowie Vektoren $v_1, \dots, v_n \in V$ und $w_1, \dots, w_n \in W$. Dann gilt:

1) Sind (v_1, \dots, v_n) linear unabhängig, so gibt es mindestens eine lineare Abbildung

$$F: V \rightarrow W \quad \text{mit} \quad F(v_i) = w_i \quad \text{für} \quad i = 1, \dots, n.$$

2) Ist $\mathcal{B} = (v_1, \dots, v_n)$ eine Basis von V , so gibt es genau eine lineare Abbildung

$$F: V \rightarrow W \quad \text{mit} \quad F(v_i) = w_i \quad \text{für} \quad i = 1, \dots, n.$$

Für dieses F gilt:

- a) $F(V) = \text{Span}_K(w_1, \dots, w_n)$.
- b) F injektiv $\Leftrightarrow (w_1, \dots, w_n)$ linear unabhängig.
- c) F Isomorphismus $\Leftrightarrow (w_1, \dots, w_n)$ Basis von W .

Beweis Teil 1) folgt aus Teil 2): Man kann (v_1, \dots, v_n) nach 2.2.2 zu einer Basis

$$(v_1, \dots, v_n, v_{n+1}, \dots, v_N) \quad \text{von} \quad V$$

ergänzen. Zu den vorgegebenen w_1, \dots, w_n kann man noch beliebige $w_{n+1}, \dots, w_N \in W$ dazunehmen und nach 2) gibt es genau ein lineares

$$F: V \rightarrow W \quad \text{mit} \quad F(v_i) = w_i \quad \text{für} \quad i = 1, \dots, N.$$

Daran kann man auch erkennen, wie weit das gesuchte F von der Eindeutigkeit entfernt ist: ein Maß dafür ist die Zahl $\dim V - n$.

Ad 2) Zunächst zeigt man, dass es höchstens ein solches F gibt. Da \mathcal{B} eine Basis von V ist, hat jedes $v \in V$ eine eindeutige Darstellung

$$v = \lambda_1 v_1 + \dots + \lambda_n v_n.$$

Da F linear sein soll, muss wegen $F(v_i) = w_i$

$$F(v) = \lambda_1 F(v_1) + \dots + \lambda_n F(v_n) = \lambda_1 w_1 + \dots + \lambda_n w_n$$

sein. Zum Beweis der Existenz von F benutzt man die so erhaltene Bedingung als Definition:

$$F(v) := \lambda_1 w_1 + \dots + \lambda_n w_n. \quad (*)$$

Dadurch ist F „wohldefiniert“, weil die $\lambda_1, \dots, \lambda_n$ durch v eindeutig bestimmt sind. Als kleine Fleißaufgabe muss man noch nachrechnen, dass die durch (*) definierte Abbildung F linear ist. Für

$$v' = \lambda'_1 v_1 + \dots + \lambda'_n v_n \quad \text{ist}$$

$$\begin{aligned} F(v + v') &= F((\lambda_1 + \lambda'_1)v_1 + \dots + (\lambda_n + \lambda'_n)v_n) = (\lambda_1 + \lambda'_1)w_1 + \dots + (\lambda_n + \lambda'_n)w_n \\ &= \lambda_1 w_1 + \dots + \lambda_n w_n + \lambda'_1 w_1 + \dots + \lambda'_n w_n = F(v) + F(v'). \end{aligned}$$

$$\begin{aligned} F(\lambda v) &= F((\lambda \lambda_1)v_1 + \dots + (\lambda \lambda_n)v_n) = (\lambda \lambda_1)w_1 + \dots + (\lambda \lambda_n)w_n \\ &= \lambda(\lambda_1 w_1 + \dots + \lambda_n w_n) = \lambda F(v). \end{aligned}$$

Zusatz a) folgt aus Teil d) der Bemerkung in 2.3.2. Aus Teil g) der selben Bemerkung folgt „ \Rightarrow “ in Beweis b). Zum Nachweis von „ \Leftarrow “ sei $F(v) = \mathbf{o}$. Ist

$$v = \lambda_1 v_1 + \dots + \lambda_n v_n, \quad \text{so folgt} \quad \mathbf{o} = F(v) = \lambda_1 w_1 + \dots + \lambda_n w_n,$$

also $\lambda_1 = \dots = \lambda_n = 0$. Somit ist $\text{Ker}(F) = \{\mathbf{o}\}$ und F injektiv.

Zusatz c) folgt aus a) und b). ■

Grundlage für die Beziehung zwischen linearen Abbildungen und Matrizen ist das

Korollar *Ist V ein K -Vektorraum mit einer Basis $\mathcal{B} = (v_1, \dots, v_n)$, so gibt es dazu genau einen Isomorphismus*

$$\Phi_{\mathcal{B}} : K^n \rightarrow V \quad \text{mit} \quad \Phi_{\mathcal{B}}(e_j) = v_j \quad \text{für} \quad j = 1, \dots, n.$$

Man nennt $\Phi_{\mathcal{B}}$ **Koordinatensystem** von V bezüglich \mathcal{B} . Ist

$$v = x_1 v_1 + \dots + x_n v_n, \quad \text{so gilt} \quad \Phi_{\mathcal{B}}(x_1, \dots, x_n) = v.$$

Die Skalare $x_1, \dots, x_n \in K$ heißen entsprechend **Koordinaten** von v bezüglich \mathcal{B} .

Dass die x_1, \dots, x_n bezüglich \mathcal{B} durch v eindeutig bestimmt sind, folgt schon aus der Definition einer Basis. Der Fortschritt ist nun die Einsicht, dass die bijektive Abbildung $\Phi_{\mathcal{B}}$ sogar ein Isomorphismus von Vektorräumen ist. Somit ist gezeigt, dass V „strukturgleich“ ist mit dem einfacher zu handhabenden Vektorraum K^n .

2.4.2 Die darstellende Matrix einer linearen Abbildung

Von dem Wechselspiel zwischen Matrizen und linearen Abbildungen hatten wir schon einige Eindrücke bekommen: Eine Matrix $A \in M(m \times n; K)$ definiert eine lineare Abbildung

$$F_A : K^n \rightarrow K^m, \quad x \mapsto A \cdot x,$$

(Beispiel 1 in 2.3.1), damit kann man die Lösungsräume linearer Gleichungssysteme beschreiben (2.3.5).

Um den Zusammenhang zwischen linearen Abbildungen und Matrizen besser zu verstehen behandeln wir zunächst den Fall der Standardräume.

Bemerkung 1 *Zu jeder linearen Abbildung $F : K^n \rightarrow K^m$ existiert genau eine Matrix $A \in M(m \times n; K)$, so dass $F = F_A$, d.h.*

$$F(x) = A \cdot x \quad \text{für alle} \quad x \in K^n.$$

Beweis Ist $F := F_A$, so haben wir in Beispiel 1 aus 2.3.1 gesehen, dass $F(e_1), \dots, F(e_n)$ die Spaltenvektoren von A sind. Also gibt es höchstens ein solches A . Damit erhält man auch die Existenz einer Matrix A zu gegebenem F : Trage die Bilder

$$F(e_j) = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} \quad \text{für } j = 1, \dots, n$$

in eine Matrix $A = (a_{ij})$ ein. Da dann $F(e_j) = A \cdot e_j$ ist $F = F_A$ nach Teil 2) des Satzes aus 2.4.1. ■

Damit hat man die linearen Abbildungen zwischen Standardräumen mit Hilfe der kanonischen Basen beschrieben. Im Prinzip geht das analog für beliebige Vektorräume mit beliebigen Basen. Da sind nur etwas mehr Buchstaben nötig.

Darstellungssatz für lineare Abbildungen Gegeben seien K -Vektorräume V und W mit einer linearen Abbildung $F : V \rightarrow W$. Zu beliebigen Basen

$$\mathcal{A} = (v_1, \dots, v_n) \text{ von } V \quad \text{und} \quad \mathcal{B} = (w_1, \dots, w_m) \text{ von } W$$

gibt es genau eine Matrix $A = (a_{ij}) \in M(m \times n; K)$ so dass

$$F(v_j) = a_{1j}w_1 + \dots + a_{mj}w_m \quad \text{für } j = 1, \dots, n. \quad (*)$$

Das ergibt ein Diagramm linearer Abbildungen

$$\begin{array}{ccc} V & \xrightarrow{F} & W \\ \Phi_{\mathcal{A}} \uparrow & & \uparrow \Phi_{\mathcal{B}} \\ K^n & \xrightarrow{A} & K^m \end{array}$$

mit $F \circ \Phi_{\mathcal{A}} = \Phi_{\mathcal{B}} \circ A$. Dabei bezeichnen $\Phi_{\mathcal{A}}$ und $\Phi_{\mathcal{B}}$ die durch \mathcal{A} und \mathcal{B} gegebenen Koordinatensysteme, die Matrix A wird als lineare Abbildung betrachtet.

Man nennt dieses A die **darstellende Matrix** von F bezüglich der Basen \mathcal{A} und \mathcal{B} und schreibt dafür

$$M_{\mathcal{B}}^{\mathcal{A}}(F) := A = (a_{ij}) \in M(m \times n; K).$$

Das obige Diagramm linearer Abbildungen heißt **kommutativ**, weil auf allen verschiedenen Wegen mit gleichem Start und Ziel (in diesem Fall nur K^n und W) die gleiche Abbildung entsteht. Solche Diagramme können Sachverhalte übersichtlicher darstellen, als Rechnungen mit vielen Indizes.

Beweis des Darstellungssatzes Da \mathcal{B} eine Basis von W ist, sind für jeden Basisvektor v_j die Skalare $a_{ij} \in K$ der Linearkombinationen

$$F(v_j) = a_{1j}w_1 + \dots + a_{mj}w_m$$

eindeutig bestimmt. Also ist die Matrix A eindeutig bestimmt, und sie definiert eine lineare Abbildung. Nach Teil 2) des Satzes aus 2.4.1 genügt es, die Beziehung

$$F \circ \Phi_{\mathcal{A}} = \Phi_{\mathcal{B}} \circ A$$

auf den Basisvektoren e_j von K^n zu überprüfen:

$$\begin{aligned} (F \circ \Phi_{\mathcal{A}})(e_j) &= F(\Phi_{\mathcal{A}}(e_j)) = F(v_j) = \sum_{i=1}^m a_{ij}w_i, \\ (\Phi_{\mathcal{B}} \circ A)(e_j) &= \Phi_{\mathcal{B}}({}^t(a_{1j}, \dots, a_{mj})) = \sum_{i=1}^m a_{ij}w_i. \end{aligned}$$

Das kann man noch einmal durch ein Diagramm deutlich machen:

$$\begin{array}{ccc} v_j & \xrightarrow{\quad} & \sum a_{ij}w_i \\ \uparrow & & \uparrow \\ e_j & \xrightarrow{\quad} & {}^t(a_{1j}, \dots, a_{mj}) \end{array}$$

Den gerade bewiesenen Darstellungssatz kann man analog zur Regel aus 2.3.1 auch kurz so formulieren:

Die Spaltenvektoren der darstellenden Matrix sind die Koordinaten der Bilder der Basisvektoren.

Für die Rechnung mit der darstellenden Matrix A einer linearen Abbildung F sollte man sich zwei verschiedene Summenformeln merken. Zunächst gilt für die Beziehung zwischen den Basisvektoren

$$F(v_j) = \sum_{i=1}^m a_{ij}w_i \quad \text{für } j = 1, \dots, n.$$

Betrachtet man dagegen die Koordinatenvektoren

$$x = {}^t(x_1, \dots, x_n) \in K^n \text{ von } v \quad \text{und} \quad y = {}^t(y_1, \dots, y_m) \in K^m \text{ von } F(v),$$

d.h.

$$v = \Phi_{\mathcal{A}}(x) = \sum_{j=1}^n x_j v_j \quad \text{und} \quad F(v) = \Phi_{\mathcal{B}}(y) = \sum_{i=1}^m y_i w_i,$$

so gilt

$$y_i = \sum_{j=1}^n a_{ij}x_j \quad \text{für } i = 1, \dots, m.$$

Als Eselsbrücke kann man sich merken, dass rechts immer über den Index summiert wird, der links nicht steht.

Beispiel 1 Im K^n und K^m hat man die Standardbasen \mathcal{K} und \mathcal{K}' , in diesem Fall sind die Koordinatensysteme $\Phi_{\mathcal{K}}$ und $\Phi_{\mathcal{K}'}$ die identischen Abbildungen. Ist $F: K^n \rightarrow K^m$ eine lineare Abbildung, so gibt es nach der Bemerkung aus 2.4.2 genau eine Matrix

$$A \in M(m \times n; K) \quad \text{so dass} \quad F(x) = A \cdot x$$

für alle $x \in K^n$. In diesem Fall ist offensichtlich

$$M_{\mathcal{K}'}^{\mathcal{K}}(F) = A,$$

d.h. die darstellende Matrix bezüglich der kanonischen Basen ist gleich der Matrix mit der F beschrieben wurde.

Der Fall von linearen Abbildungen $F: K^n \rightarrow K^m$ wird erst interessanter, wenn man andere als die kanonischen Basen verwendet. Darauf kommen wir in 2.5.2 zurück.

Beispiel 2 Im \mathbb{R} -Vektorraum $\text{Abb}(\mathbb{R}, \mathbb{R})$ betrachten wir den Untervektorraum

$$V := \text{Span}_{\mathbb{R}}(1, \cos, \sin).$$

Nach Beispiel 9 aus 2.1.4 ist $\mathcal{B} := (1, \cos, \sin)$ eine Basis von V . Wir betrachten nun die durch Differentiation erklärte Abbildung

$$D: V \rightarrow V, f \mapsto f'.$$

Differenziert man die Basisvektoren, so erhält man

$$D(1) = 0, \quad D(\cos) = -\sin \quad \text{und} \quad D(\sin) = \cos.$$

Daraus erhält man die Spalten von

$$M_{\mathcal{B}}^{\mathcal{B}}(D) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}.$$

Rechnet man in Koordinaten, so folgt aus

$$f = x_1 + x_2 \cos + x_3 \sin, \quad \text{dass} \quad D(f) = x_3 \cos - x_2 \sin, \quad \text{d.h.} \quad M_{\mathcal{B}}^{\mathcal{B}}(D) \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ x_3 \\ -x_2 \end{pmatrix}.$$

Man kann den Darstellungssatz für lineare Abbildungen noch von einem abstrakteren Standpunkt betrachten. Zu Vektorräumen V und W hat man den Vektorraum $\text{Hom}(V, W)$ aller linearen Abbildungen F von V nach W (vgl. 2.3.4). Haben V und W endliche Basen \mathcal{A} und \mathcal{B} , so ist die darstellende Matrix $M_{\mathcal{B}}^{\mathcal{A}}(F)$ ein Element des Vektorraums $M(m \times n; K)$ der Matrizen (Beispiel 7 aus 2.1.1).

Bemerkung 2 Sind \mathcal{A} und \mathcal{B} Basen der Längen n und m der Vektorräume V und W , so ist die Abbildung

$$M_{\mathcal{B}}^{\mathcal{A}} : \text{Hom}(V, W) \rightarrow M(m \times n; K), F \mapsto M_{\mathcal{B}}^{\mathcal{A}}(F),$$

ein Isomorphismus von Vektorräumen. Insbesondere gilt

$$\dim \text{Hom}(V, W) = (\dim V) \cdot (\dim W).$$

Beweis Sei $\mathcal{A} = (v_1, \dots, v_n)$ und $\mathcal{B} = (w_1, \dots, w_m)$. Um die Linearität von $M_{\mathcal{B}}^{\mathcal{A}}$ zu zeigen, betrachten wir $F, G \in \text{Hom}(V, W)$ und $\lambda \in K$. Ist

$$M_{\mathcal{B}}^{\mathcal{A}}(F) = A = (a_{ij}) \quad \text{und} \quad M_{\mathcal{B}}^{\mathcal{A}}(G) = B = (b_{ij}),$$

so folgt

$$(F + G)(v_j) = F(v_j) + G(v_j) = \sum_{i=1}^m a_{ij} w_i + \sum_{i=1}^m b_{ij} w_i = \sum_{i=1}^m (a_{ij} + b_{ij}) w_i.$$

Also folgt $M_{\mathcal{B}}^{\mathcal{A}}(F + G) = A + B = M_{\mathcal{B}}^{\mathcal{A}}(F) + M_{\mathcal{B}}^{\mathcal{A}}(G)$. Aus

$$(\lambda F)(v_j) = \lambda F(v_j) = \lambda \cdot \sum_{i=1}^m a_{ij} w_i = \sum_{i=1}^m (\lambda a_{ij}) w_i \quad \text{folgt}$$

$M_{\mathcal{B}}^{\mathcal{A}}(\lambda F) = \lambda A = \lambda M_{\mathcal{B}}^{\mathcal{A}}(F)$. Dass $M_{\mathcal{B}}^{\mathcal{A}}$ bijektiv ist, folgt mit Hilfe des Satzes über die Erzeugung linearer Abbildungen aus 2.4.1. Ist $F \in \text{Ker } M_{\mathcal{B}}^{\mathcal{A}}$, so folgt

$$F(v_j) = \sum_{i=1}^m 0 \cdot w_i = \mathbf{o}$$

für alle j , also ist $F = \mathbf{o}$. Ist $A = (a_{ij}) \in M(m \times n; K)$, so ist durch

$$F(v_j) := \sum_{i=1}^m a_{ij} w_i$$

ein $F \in \text{Hom}(V, W)$ erklärt und nach Definition von F ist $A = M_{\mathcal{B}}^{\mathcal{A}}(F)$. ■

2.4.3 Multiplikation von Matrizen

Wie wir in 2.4.2 gesehen haben, ist jede lineare Abbildung $F: K^n \rightarrow K^m$ durch eine Matrix $A \in M(m \times n; K)$ beschrieben, d.h.

$$F(x) = A \cdot x = {}^t(y_1, \dots, y_m) \in K^m \quad \text{für} \quad x = {}^t(x_1, \dots, x_n) \in K^n.$$

Daher ist die Bezeichnung $F = F_A$ nützlich. Wir betrachten nun die Komposition von zwei linearen Abbildungen zwischen Standardräumen:

$$\begin{array}{ccc} K^r & \xrightarrow{F_B} & K^n & \xrightarrow{F_A} & K^m, \\ \begin{pmatrix} z_1 \\ \vdots \\ z_r \end{pmatrix} & \longmapsto & \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} & \longmapsto & \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}. \end{array}$$

Dabei ist $B \in M(n \times r; K)$ und $F_B(z) = B \cdot z$. Die Abbildung

$$F_A \circ F_B: K^r \rightarrow K^m$$

wird durch eine Matrix $C \in M(m \times r; K)$ beschrieben, d.h. $F_A \circ F_B = F_C$, und es gibt das offensichtliche Problem, wie man C aus A und B berechnen kann. Das wollen wir zunächst in ganz einfachen Spezialfällen explizit ausführen.

Im Fall $r = n = m = 1$ ist $A = (a)$, $B = (b)$, also $C = (a \cdot b)$.

Im Fall $r = n = m = 2$ ist

$$\begin{array}{l} A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad \text{also} \quad \begin{array}{l} y_1 = a_{11}x_1 + a_{12}x_2 \\ y_2 = a_{21}x_1 + a_{22}x_2, \end{array} \\ B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}, \quad \text{also} \quad \begin{array}{l} x_1 = b_{11}z_1 + b_{12}z_2 \\ x_2 = b_{21}z_1 + b_{22}z_2. \end{array} \end{array}$$

Durch Einsetzen erhält man

$$\begin{aligned} y_1 &= a_{11}(b_{11}z_1 + b_{12}z_2) + a_{12}(b_{21}z_1 + b_{22}z_2) \\ &= (a_{11}b_{11} + a_{12}b_{21})z_1 + (a_{11}b_{12} + a_{12}b_{22})z_2, \\ y_2 &= a_{21}(b_{11}z_1 + b_{12}z_2) + a_{22}(b_{21}z_1 + b_{22}z_2) \\ &= (a_{21}b_{11} + a_{22}b_{21})z_1 + (a_{21}b_{12} + a_{22}b_{22})z_2. \end{aligned}$$

Für $C = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$ folgt

$$\begin{array}{ll} c_{11} = a_{11}b_{11} + a_{12}b_{21}, & c_{12} = a_{11}b_{12} + a_{12}b_{22}, \\ c_{21} = a_{21}b_{11} + a_{22}b_{21}, & c_{22} = a_{21}b_{12} + a_{22}b_{22}. \end{array}$$

Man bezeichnet $C = A \cdot B$ als Produkt von A und B .

Ganz allgemein hat man

$$y_i = \sum_{j=1}^n a_{ij}x_j \text{ für } i = 1, \dots, m \quad \text{und} \quad x_j = \sum_{k=1}^r b_{jk}z_k \text{ für } j = 1, \dots, n.$$

Durch Einsetzen und Umordnen der Summe ergibt sich

$$y_i = \sum_{j=1}^n a_{ij} \cdot \left(\sum_{k=1}^r b_{jk}z_k \right) = \sum_{k=1}^r \left(\sum_{j=1}^n a_{ij}b_{jk} \right) \cdot z_k.$$

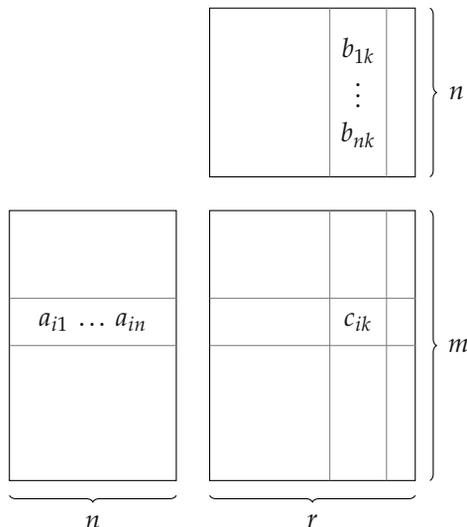
Daraus folgt für die Matrix $C = (c_{ik}) \in M(m \times r; K)$, dass

$$c_{ik} = \sum_{j=1}^n a_{ij}b_{jk} \quad \text{für } i = 1, \dots, m \text{ und } k = 1, \dots, r.$$

Anders aufgeschrieben ist c_{ik} das Skalarprodukt der i -ten Zeile von A mit der k -ten Spalte von B , also

$$c_{ik} = (a_{i1}, \dots, a_{in}) \cdot \begin{pmatrix} b_{1k} \\ \vdots \\ b_{nk} \end{pmatrix}.$$

Entscheidend dabei ist, dass die Zahl der Spalten von A mit der Zahl der Zeilen von B übereinstimmt. Schematisch kann man die Situation so illustrieren:



Damit haben wir genug Motivation für die folgende

Definition Ist K ein beliebiger Körper, so ist für Matrizen $A \in M(m \times n; K)$ und $B \in M(n \times r; K)$ das **Produkt**

$$A \cdot B = (c_{ik}) \in M(m \times r; K) \quad \text{definiert durch} \quad c_{ik} := \sum_{j=1}^n a_{ij} b_{jk}.$$

Im wichtigen Spezialfall quadratischer Matrizen A, B gleicher Größe (d.h. $m = r = n$) ist $A \cdot B$ wieder quadratisch. Eine unmittelbare Folgerung aus unserer Konstruktion der Produktmatrix ist der

Satz Sind $F_A : K^n \rightarrow K^m$ und $F_B : K^r \rightarrow K^n$ beschrieben durch

$$A \in M(m \times n; K) \quad \text{und} \quad B \in M(n \times r; K),$$

so ist die Komposition $F_A \circ F_B : K^r \rightarrow K^m$ beschrieben durch $A \cdot B \in M(m \times r; K)$. Kurz ausgedrückt $F_A \circ F_B = F_{A \cdot B}$, oder als kommutatives Diagramm

$$\begin{array}{ccc} K^r & \xrightarrow{F_{A \cdot B}} & K^m \\ & \searrow F_B & \nearrow F_A \\ & K^n & \end{array}$$

Aus dieser Beziehung erhält man ganz einfach eine Abschätzung für den Rang der Produktmatrix. ■

Korollar 1 Ist $A \in M(m \times n; K)$ und $B \in M(n \times r; K)$, so gilt

$$\text{rang}(A \cdot B) \leq \min\{\text{rang } A, \text{rang } B\}.$$

Beweis Zunächst ist $\text{rang}(A \cdot B) = \dim F_{A \cdot B}(K^r)$. Es ist $F_B(K^r) \subset K^n$ und nach dem obigen Satz gilt

$$F_{A \cdot B}(K^r) = F_A(F_B(K^r)) \subset F_A(K^n).$$

Also folgt

$$\text{rang}(A \cdot B) \leq \dim F_A(K^n) = \text{rang } A.$$

Mit Hilfe von Teil h) der Bemerkung aus 2.3.2 folgt

$$\text{rang}(A \cdot B) = \dim F_A(F_B(K^r)) \leq \dim F_B(K^r) = \text{rang } B. \quad \blacksquare$$

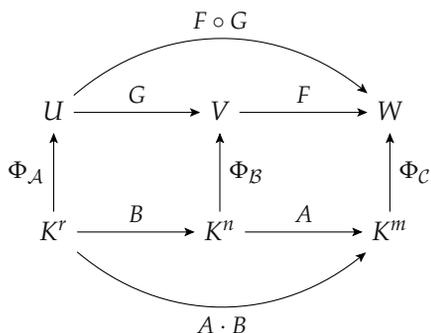
Eine Produktregel wie in obigem Satz gilt nicht nur für lineare Abbildungen zwischen den Standardräumen, sondern allgemeiner.

Korollar 2 Gegeben seien Vektorräume U, V, W mit endlichen Basen $\mathcal{A}, \mathcal{B}, \mathcal{C}$, sowie lineare Abbildungen

$$F : V \rightarrow W \quad \text{und} \quad G : U \rightarrow V.$$

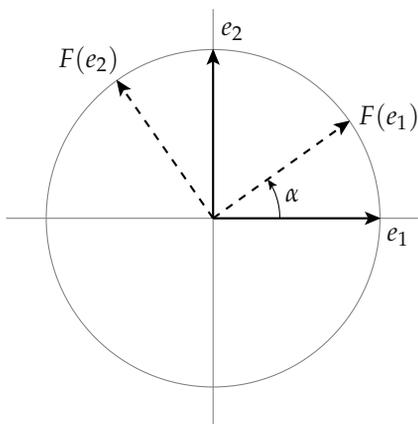
Dann gilt für die darstellenden Matrizen $M_{\mathcal{C}}^{\mathcal{A}}(F \circ G) = M_{\mathcal{C}}^{\mathcal{B}}(F) \cdot M_{\mathcal{B}}^{\mathcal{A}}(G)$. ■

Setzt man $A := M_{\mathcal{C}}^{\mathcal{B}}(F), B := M_{\mathcal{B}}^{\mathcal{A}}(G)$ und betrachtet man Matrizen ohne Unterscheidung der Bezeichnung auch als Abbildungen zwischen Standardräumen, so erhält man das folgende kommutative Diagramm:



Beispiel Bei einer *Drehung* F des \mathbb{R}^2 um den Winkel α ist

$$F(e_1) = \begin{pmatrix} \cos \alpha \\ \sin \alpha \end{pmatrix} \quad \text{und} \quad F(e_2) = \begin{pmatrix} -\sin \alpha \\ \cos \alpha \end{pmatrix}.$$



Also wird F beschrieben durch die Matrix

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

Eine weitere Drehung G um den Winkel β ist beschrieben durch

$$B = \begin{pmatrix} \cos \beta & -\sin \beta \\ \sin \beta & \cos \beta \end{pmatrix}.$$

Offensichtlich ist $F \circ G$ eine Drehung um den Winkel $\alpha + \beta$ und da $\alpha + \beta = \beta + \alpha$, ist auch $F \circ G = G \circ F$. Für die beschriebenen Matrizen bedeutet das

$$A \cdot B = \begin{pmatrix} \cos \alpha \cos \beta - \sin \alpha \sin \beta & -(\sin \alpha \cos \beta + \cos \alpha \sin \beta) \\ \sin \alpha \cos \beta + \cos \alpha \sin \beta & \cos \alpha \cos \beta - \sin \alpha \sin \beta \end{pmatrix} = B \cdot A$$

In dieser Beziehung sind die **Additionstheoreme** der trigonometrischen Funktionen enthalten:

$$\begin{aligned} \cos(\alpha + \beta) &= \cos \alpha \cos \beta - \sin \alpha \sin \beta, \\ \sin(\alpha + \beta) &= \sin \alpha \cos \beta + \cos \alpha \sin \beta. \end{aligned}$$

2.4.4 Rechenregeln für Matrizen

Bei der Multiplikation von Matrizen gibt es manche Überraschungen. So ist etwa im Fall quadratischer Matrizen gleicher Größe

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \text{aber} \\ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}. \end{aligned}$$

Daran sieht man sofort, dass die Multiplikation in $M(2 \times 2; K)$ für jeden Körper K nicht kommutativ ist, und dass es Nullteiler gibt! Indem man die obigen Matrizen durch Nullen vergrößert, erhält man analoge Beispiele in $M(n \times n; K)$ für $n \geq 2$. Der Leser möge sich zur Übung überlegen, was dieses Beispiel für die entsprechenden linearen Abbildungen des K^2 bedeutet.

Entscheidend für das Rechnen mit Matrizen ist das

Lemma Die Multiplikation von Matrizen ist für jeden Körper K assoziativ. Genauer: Ist mit $m, n, r, s \in \mathbb{N}^*$

$$A \in M(m \times n; K), \quad B \in M(n \times r; K) \quad \text{und} \quad C \in M(r \times s; K),$$

so folgt

$$(A \cdot B) \cdot C = A \cdot (B \cdot C) \quad \text{in} \quad M(m \times s; K).$$

Beweis Man kann diese Gleichung direkt nachrechnen, das ist allerdings etwas mühsam und erfordert große Präzision im Umgang mit den Indizes. Viel einfacher geht es, wenn man den Zusammenhang von Matrizen und linearen Abbildungen ausnutzt; schließlich war der Definition der Multiplikation in 2.4.3 schon etwas Rechnung vorausgegangen.

Wir betrachten die zu den gegebenen Matrizen gehörigen linearen Abbildungen

$$K^s \xrightarrow{F_C} K^r \xrightarrow{F_B} K^n \xrightarrow{F_A} K^m.$$

Wie wir in 1.2.2 gesehen hatten, gilt das Assoziativgesetz für Abbildungen, also ist

$$(F_A \circ F_B) \circ F_C = F_A \circ (F_B \circ F_C).$$

Nach dem Satz aus 2.4.3 werden die Abbildungen auf beiden Seiten der Gleichung beschrieben durch

$$(A \cdot B) \cdot C \quad \text{und} \quad A \cdot (B \cdot C).$$

Da die Abbildungen gleich sind, müssen auch die beschreibenden Matrizen gleich sein. ■

In der Sprache der Matrizenprodukte kann man den Satz aus 2.4.3 so formulieren: Für jede Spalte $z = {}^t(z_1, \dots, z_r)$ ist

$$A \cdot (B \cdot z) = (A \cdot B) \cdot z.$$

Das ist gerade die Aussage des Assoziativgesetzes für den Spezialfall $s = 1$, also $C = z \in M(r \times 1; K)$. Der obige Beweis zeigt, wie man den allgemeinen Fall auf diesen Spezialfall zurückführen kann.

Besondere Bedeutung für die Multiplikation haben die **Einheitsmatrizen**:

Für jedes $n \in \mathbb{N}^*$ ist

$$E_n := \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in M(n \times n; K)$$

die Matrix mit Einsen in der Diagonale und sonst lauter Nullen.

Wir notieren einige für Matrizen laufend benutzte

Rechenregeln Ist K ein Körper, so gilt für alle $A, A' \in M(m \times n; K)$, $B, B' \in M(n \times r; K)$ und $\lambda \in K$

$$1) \quad A \cdot (B + B') = A \cdot B + A \cdot B', \quad (A + A') \cdot B = A \cdot B + A' \cdot B. \quad \text{Distributivgesetze}$$

$$2) \quad A \cdot (\lambda B) = (\lambda A) \cdot B = \lambda(A \cdot B).$$

$$3) \quad E_m \cdot A = A \cdot E_n = A.$$

Neutralität der Einheitsmatrizen

$$4) \quad {}^t(A \cdot B) = {}^tB \cdot {}^tA.$$

Beweis 1) Ist $A = (a_{ij})$, $B = (b_{jk})$ und $B' = (b'_{jk})$, so folgt die erste Behauptung sofort aus

$$\sum_j a_{ij}(b_{jk} + b'_{jk}) = \sum_j a_{ij}b_{jk} + \sum_j a_{ij}b'_{jk}.$$

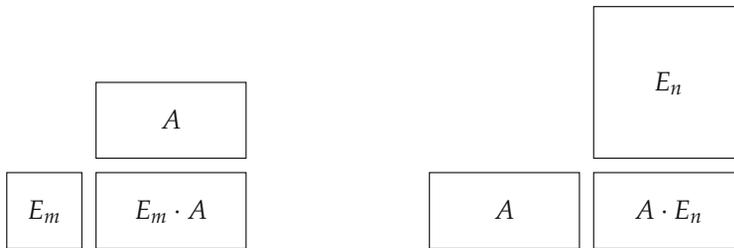
Analog prüft man die zweite Behauptung.

2) Folgt aus $\sum_j a_{ij}(\lambda b_{jk}) = \sum_j (\lambda a_{ij})b_{jk} = \lambda \sum_j a_{ij}b_{jk}$.

3) Hier hat man die Größen der Einheitsmatrizen zu beachten: Der Eintrag an der Stelle i, j von $E_m \cdot A$ ist

$$(0, \dots, 0, \underset{\substack{\uparrow \\ \text{Position } i}}{1}, 0, \dots, 0) \cdot \begin{pmatrix} a_{1j} \\ \vdots \\ a_{ij} \\ \vdots \\ a_{mj} \end{pmatrix} = a_{ij},$$

also ist $E_m \cdot A = A$. Analog sieht man $A \cdot E_n = A$. Schematisch kann man das im Fall $m < n$ so skizzieren:



4) Zunächst muss man überlegen, wie sich die transponierten Matrizen multiplizieren lassen. Da

$$A \in M(m \times n; K) \quad \text{und} \quad B \in M(n \times r; K), \quad \text{folgt} \\ {}^tA \in M(n \times m; K) \quad \text{und} \quad {}^tB \in M(r \times n; K).$$

Also ist ${}^tB \cdot {}^tA$ definiert (${}^tA \cdot {}^tB$ im Allgemeinen nicht). Um die behauptete Gleichheit zu zeigen, muss man geeignete Bezeichnungen wählen.

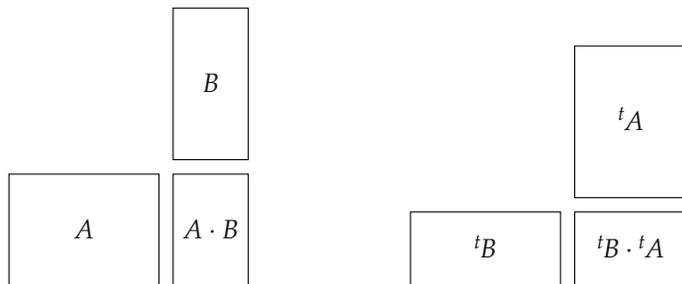
Ist $A = (a_{ij})$ und $B = (b_{jk})$, so wird

$${}^tA = (a'_{ji}) \quad \text{mit} \quad a'_{ji} = a_{ij} \quad \text{und} \quad {}^tB = (b'_{kj}) \quad \text{mit} \quad b'_{kj} = b_{jk}.$$

Weiter ist $A \cdot B = (c_{ik})$ mit $c_{ik} = \sum_j a_{ij}b_{jk}$, also ${}^t(A \cdot B) = (c'_{ki})$ mit $c'_{ki} = c_{ik}$. Nach der Formel für das Produkt gilt

$${}^tB \cdot {}^tA = (d_{ki}) \quad \text{mit} \quad d_{ki} = \sum_j b'_{kj}a'_{ji} = \sum_j b_{jk}a_{ij} = \sum_j a_{ij}b_{jk} = c_{ik} = c'_{ki}.$$

Daraus folgt die Behauptung. Schematisch kann man die Größen der beteiligten Matrizen wieder skizzieren:



Aus den gerade bewiesenen Rechenregeln folgt im Fall quadratischer Matrizen der

Satz Für jeden Körper K und jedes $n \in \mathbb{N}^*$ ist die Menge $M(n \times n; K)$ zusammen mit der Addition und der in 2.4.2 erklärten Multiplikation ein Ring. Nullelement ist die Nullmatrix, Einselement die Einheitsmatrix E_n .

Für $n \geq 2$ und jeden Körper K ist $M(n \times n; K)$ nicht kommutativ.

Beweis Nach den Regeln für die Multiplikation von Matrizen ist für $A, B \in M(n \times n; K)$ auch $A \cdot B \in M(n \times n; K)$. Die Ringaxiome folgen aus den oben bewiesenen Rechenregeln. Man beachte, dass dabei nur die Assoziativität der Multiplikation nicht offensichtlich ist. Ein Beispiel für $A \cdot B \neq B \cdot A$ in $M(2 \times 2; K)$ hatten wir schon zu Beginn von 2.4.4 gegeben.

In Bemerkung 2 aus 2.3.3 hatten wir gesehen, dass für jeden Vektorraum V die Menge $\text{End}(V)$ aller Endomorphismen zusammen mit der Addition und der Komposition ein Ring ist. Aus dem Satz in 2.4.3 folgt sofort das

Korollar 1 Für jeden Körper K und jedes $n \in \mathbb{N}^*$ ist die Abbildung

$$M(n \times n; K) \rightarrow \text{End}(K^n), A \mapsto F_A,$$

ein Isomorphismus von Ringen.

Benutzt man die Bemerkung 2 aus 2.4.2 und Korollar 2 aus 2.4.3, so erhält man

Korollar 2 Ist V ein K -Vektorraum mit $\dim V = n < \infty$, so ist für je zwei Basen \mathcal{A} und \mathcal{B} von V die Abbildung

$$\text{End}(V) \rightarrow M(n \times n; K), F \mapsto M_{\mathcal{B}}^{\mathcal{A}}(F),$$

ein Isomorphismus von Ringen.

2.4.5 Die allgemeine lineare Gruppe

Im Satz aus 2.4.4 hatten wir gesehen, dass quadratische Matrizen die Struktur eines Ringes haben. In der allgemeinen Theorie der Ringe sind diejenigen Elemente besonders ausgezeichnet, die ein multiplikatives Inverses besitzen. Im Spezialfall des Ringes von Matrizen führt das zu folgender

Definition Eine Matrix $A \in M(n \times n; K)$ heißt **invertierbar**, wenn es ein $B \in M(n \times n; K)$ gibt, so dass

$$A \cdot B = B \cdot A = E_n.$$

Diese Bedingung an A kann man auch anders fassen, dabei ist Korollar 1 aus 2.4.4 sehr hilfreich:

Lemma Für eine Matrix $A \in M(n \times n; K)$ sind folgende Bedingungen gleichwertig:

- i) A ist invertierbar,
- ii) $\text{rang } A = n$,
- iii) Die durch A erklärte lineare Abbildung $F_A : K^n \rightarrow K^n$ ist ein Isomorphismus.

Beweis i) \Rightarrow ii) Mit den durch A und B erklärten linearen Abbildungen F_A und F_B erhalten wir

$$K^n \xrightarrow{F_B} K^n \xrightarrow{F_A} K^n.$$

Da $F_A \circ F_B = F_{A \cdot B} = F_{E_n} = \text{id}_{K^n}$ folgt, dass F_A surjektiv sein muss, also ist $\text{rang } A = n$.

ii) \Rightarrow iii) folgt sofort aus dem Korollar in 2.3.5.

iii) \Rightarrow i) Die Umkehrabbildung F_A^{-1} wird beschrieben durch eine Matrix B , d.h. $F_A^{-1} = F_B$.

Aus $F_{A \cdot B} = F_A \circ F_B = \text{id}_{K^n}$ folgt $A \cdot B = E_n$, aus $F_{B \cdot A} = F_B \circ F_A = \text{id}_{K^n}$ folgt $B \cdot A = E_n$. ■

Dem aufmerksamen Leser wird nicht entgangen sein, dass wir beim Beweis von i) \Rightarrow ii) nur die Bedingung $A \cdot B = E_n$ benutzt haben; somit kann $B \cdot A = E_n$ daraus gefolgert werden. Das ist nicht in allen Ringen der Fall (vgl. [FI₃, Beispiel 5 in II 1.4]).

Der Beweis des Lemmas zeigt auch, dass die Matrix B zu einer invertierbaren Matrix A durch die Bedingung $A \cdot B = E_n$ eindeutig bestimmt ist, denn B beschreibt die Abbildung F_A^{-1} . Statt B kann man daher A^{-1} schreiben, das nennt man die zu A **inverse Matrix**; sie ist charakterisiert durch

$$A \cdot A^{-1} = A^{-1} \cdot A = E_n.$$

Zunächst ist es angebracht, die Gesamtheit aller invertierbaren Matrizen in $M(n \times n; K)$ zu betrachten. Grundlegend ist der folgende

Satz Für jeden Körper K und jedes $n \in \mathbb{N}^*$ ist

$$GL(n; K) := \{A \in M(n \times n; K) : A \text{ ist invertierbar}\}$$

mit der Multiplikation von Matrizen als Verknüpfung eine Gruppe.

Für jeden Körper K und jedes $n \geq 2$ ist $GL(n; K)$ nicht abelsch.

Man bezeichnet $GL(n; K)$ als **allgemeine lineare Gruppe** (GL steht für „general linear“).

Beweis Zunächst ist zu zeigen, dass für $A, B \in GL(n; K)$ auch $A \cdot B \in GL(n; K)$ ist. Am einfachsten sieht man das mit Hilfe der linearen Abbildungen F_A und F_B : Sind F_A und F_B Isomorphismen, so ist auch $F_{A \cdot B} = F_A \circ F_B$ ein Isomorphismus.

Man beachte, dass $GL(n; K)$ nicht abgeschlossen ist unter der Addition:

$$E_n, -E_n \in GL(n; K), \quad \text{aber} \quad E_n + (-E_n) = \mathbf{0} \notin GL(n; K).$$

Die Multiplikation von Matrizen ist assoziativ im Ring $M(n \times n; K)$, also auch in $GL(n; K)$. Einselement ist E_n , das Inverse zu A ist A^{-1} .

Dass $GL(n; K)$ für $n \geq 2$ nicht abelsch ist, sieht man mit Hilfe von invertierbaren Matrizen, die nur 0 und 1 enthalten:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}. \quad \blacksquare$$

Wir notieren noch zwei einfache und oft benutzte

Rechenregeln Für $A, B \in GL(n; K)$ gilt

$$(A \cdot B)^{-1} = B^{-1} \cdot A^{-1} \quad \text{und} \quad ({}^t A)^{-1} = {}^t(A^{-1}).$$

Insbesondere ist damit die Bezeichnung ${}^t A^{-1}$ gerechtfertigt.

Beweis Die erste Regel gilt allgemein in Gruppen, denn

$$\begin{aligned} (B^{-1}A^{-1})(AB) &= B^{-1}(A^{-1}A)B = B^{-1}B = E_n \quad \text{und} \\ (AB)(B^{-1}A^{-1}) &= A(BB^{-1})A^{-1} = AA^{-1} = E_n. \end{aligned}$$

Für die transponierte Matrix gilt nach der Rechenregel 4) aus 2.4.4

$${}^t A {}^t (A^{-1}) = {}^t (A^{-1} A) = {}^t E_n = E_n \quad \text{und} \quad {}^t (A^{-1}) {}^t A = {}^t (A A^{-1}) = {}^t E_n = E_n. \quad \blacksquare$$

Nach der allgemeinen Theorie stellt sich natürlich die Frage, wie man die Einträge von A^{-1} aus denen von A berechnen kann. Ein Verfahren, das auch für große n relativ wenig Rechenaufwand erfordert, beschreiben wir in 2.4.6. Man kann auch Determinanten verwenden, das ist von mehr theoretischem Interesse (vgl. 3.3.1). Vorweg behandeln wir die ganz einfachen Fälle $n = 1, 2$.

Beispiele Im Fall $n = 1$ ist $A = (a)$ und $\text{rang } A = 1$ bedeutet $a \neq 0$. Dann ist

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

Im Fall $n = 2$ sei

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{und} \quad A^{-1} = \begin{pmatrix} x_1 & x_3 \\ x_2 & x_4 \end{pmatrix},$$

wobei die Einträge x_1, \dots, x_4 von A^{-1} noch unbekannt sind. Die Gleichung $AA^{-1} = E_2$ ergibt für die beiden Spalten von A^{-1} die getrennten linearen Gleichungssysteme

$$\begin{array}{lcl} ax_1 + bx_2 = 1 & \text{und} & ax_3 + bx_4 = 0 \\ cx_1 + dx_2 = 0 & & cx_3 + dx_4 = 1. \end{array}$$

Die zugehörigen homogenen Systeme haben beide die Koeffizientenmatrix A und man weiß (etwa mit Hilfe des Lemmas aus 0.3.6, das offenbar für einen beliebigen Körper richtig bleibt), dass

$$\text{rang } A = 2 \Leftrightarrow ad - bc \neq 0.$$

Mit etwas Rechnung oder mit Hilfe der in 3.1.1 erläuterten CRAMERSchen Regel erhält man durch Lösen der beiden Gleichungssysteme

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Zur Kontrolle sollte man noch einmal nachprüfen, dass $AA^{-1} = A^{-1}A = E_2$ gilt.

Eine Verallgemeinerung dieser Methode folgt in 2.4.7.

2.4.6 Elementarmatrizen

In der linearen Algebra kann man viele Rechnungen iterativ durchführen, d.h. durch viele kleine und einfache Einzelschritte. Ein wichtiges Hilfsmittel dabei sind Umformungen von Matrizen, das wurde schon bei der Lösung von linearen Gleichungssystemen und zur Bestimmung von Basen in 2.2.4 benutzt. Dabei hatten wir für eine Matrix A folgende Umformungen betrachtet:

Typ (1)

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \end{pmatrix} = \begin{pmatrix} a_{21} & \dots & a_{2n} \\ a_{11} & \dots & a_{1n} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} \\ \vdots & \vdots \\ a_{m1} & a_{m2} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_{12} & a_{11} \\ \vdots & \vdots \\ a_{m2} & a_{m1} \end{pmatrix}$$

Typ (2)

$$\begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} \cdot \begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \lambda a_{11} + a_{21} & \dots & \lambda a_{1n} + a_{2n} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} \\ \vdots & \vdots \\ a_{m1} & a_{m2} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} = \begin{pmatrix} a_{11} + \lambda a_{12} & a_{12} \\ \vdots & \vdots \\ a_{m1} + \lambda a_{m2} & a_{m2} \end{pmatrix}$$

Typ (3)

$$\begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \end{pmatrix} = \begin{pmatrix} \lambda a_{11} & \dots & \lambda a_{1n} \\ a_{21} & \dots & a_{2n} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} \\ \vdots & \vdots \\ a_{m1} & a_{m2} \end{pmatrix} \cdot \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \lambda a_{11} & a_{12} \\ \vdots & \vdots \\ \lambda a_{m1} & a_{m2} \end{pmatrix}$$

Ganz analog sieht man die Wirkung auf eine beliebige Matrix $A \in M(m \times n); K$:

Typ(1) $P_m(i, j) \cdot A$: Zeilen i und j vertauscht.
 $A \cdot P_n(i, j)$: Spalten i und j vertauscht.

Typ(2) $Q_{\lambda, m}(i, j) \cdot A$: Zeile $j + \lambda \cdot$ Zeile i
 $A \cdot Q_{\lambda, n}(i, j)$: Spalte $i + \lambda \cdot$ Spalte j

Typ(3) $S_{\lambda, m}(i) \cdot A$: $\lambda \cdot$ Zeile i
 $A \cdot S_{\lambda, n}(i)$: $\lambda \cdot$ Spalte i

Die bisherigen Überlegungen waren scheinbar nur Spielereien; nun zum Nutzen der Elementarmatrizen.

Hilfssatz Die Elementarmatrizen sind invertierbar und ihre Inversen sind wieder Elementarmatrizen.

Beweis Die Invertierbarkeit ist klar, da die Elementarmatrizen durch Umformungen der Einheitsmatrix entstanden waren, dabei bleibt der Rang erhalten. Man beachte hierzu, dass bei Typ (2) $i \neq j$ und bei Typ (3) $\lambda \neq 0$ vorausgesetzt war. Im Fall $i = j$ könnte man sonst $\lambda = -1$ wählen!

Für die Berechnung der Inversen betrachten wir zunächst wieder den besonders einfachen aber charakteristischen Fall $n = 2$, $i = 1$ und $j = 2$. Die folgenden drei Produkte ergeben jeweils E_2 :

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{\lambda} & 0 \\ 0 & 1 \end{pmatrix}.$$

Allgemein gilt:

$$P(i,j)^{-1} = P(i,j), \quad Q_\lambda(i,j)^{-1} = Q_{-\lambda}(i,j) \quad \text{und} \quad S_\lambda(i)^{-1} = S_{\lambda^{-1}}(i).$$

■

Satz Sei K ein Körper und $n \in \mathbb{N}^*$. Zu jeder Matrix $A \in \text{GL}(n; K)$ gibt es Elementarmatrizen B_1, \dots, B_k so dass

$$A = B_1 \cdot \dots \cdot B_k.$$

Kurz ausgedrückt: Die Gruppe $\text{GL}(n; K)$ wird erzeugt von den Elementarmatrizen.

Beweis Da $\text{rang } A = n$ kann man A durch elementare Zeilenumformungen „von oben nach unten“ zunächst auf die Form

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

bringen. Diese Zeilenumformungen werden durch Elementarmatrizen C_1, \dots, C_l bewirkt, also ist

$$A' = C_l \cdot \dots \cdot C_1 \cdot A.$$

Durch weitere Zeilenumformungen „von unten nach oben“ kann man A' zu E_n machen; es gibt also Elementarmatrizen C_{l+1}, \dots, C_k so dass

$$E_n = C_k \cdot \dots \cdot C_{l+1} \cdot A' = C_k \cdot \dots \cdot C_1 \cdot A, \quad \text{also} \quad A = C_1^{-1} \cdot \dots \cdot C_k^{-1}.$$

Nach dem Hilfssatz sind auch die Inversen wieder Elementarmatrizen, also ist der Satz bewiesen. ■

Dieses Ergebnis hat nützliche Anwendungen, etwa beim Beweis der Eigenschaften von Determinanten in Kapitel 3. Außerdem erhält man mit Hilfe der Elementarmatrizen eine elegante Begründung für ein klassisches Verfahren einer schrittweisen Berechnung der inversen Matrix. Es wird oft **GAUSS-JORDAN-Verfahren** genannt. Dazu ist zu bemerken, dass der Name JORDAN an den schwäbischen Geometer und Landvermesser Wilhelm Jordan (1842-1899) erinnert, der die schon von GAUSS angewandte Elimination zur Lösung von linearen Gleichungssystemen ausgiebig benutzte und weiter entwickelte.

Nun zur **Inversion einer Matrix** $A \in M(n \times n; K)$. Man schreibt A und E_n nebeneinander. Durch elementare Zeilenumformungen versucht man A auf E_n umzuformen. Ist $\text{rang } A = n$, so gelingt das; andernfalls stellt man fest, dass A nicht invertierbar ist. Die gleichen Umformungen führt man an E_n durch. Das ergibt folgendes Schema:

$$\begin{array}{ccc}
 A & & E_n \\
 C_1 \cdot A & & C_1 \cdot E_n \\
 \vdots & & \vdots \\
 E_n = C_k \cdot \dots \cdot C_1 \cdot A & & C_k \cdot \dots \cdot C_1 \cdot E_n = A^{-1}
 \end{array}$$

Die elementaren Zeilenumformungen werden bewirkt durch Multiplikation von links mit Elementarmatrizen. Aus $(C_k \cdot \dots \cdot C_1) \cdot A = E_n$ folgt $C_k \cdot \dots \cdot C_1 = A^{-1}$.

Beispiel:

$$\begin{array}{cc}
 A & E_2 \\
 \parallel & \parallel \\
 \begin{array}{|cc|cc|}
 \hline
 1 & 2 & 1 & 0 \\
 1 & 1 & 0 & 1 \\
 \hline
 1 & 2 & 1 & 0 \\
 0 & -1 & -1 & 1 \\
 \hline
 1 & 2 & 1 & 0 \\
 0 & 1 & 1 & -1 \\
 \hline
 1 & 0 & -1 & 2 \\
 0 & 1 & 1 & -1 \\
 \hline
 \end{array} & \\
 \parallel & \parallel \\
 E_2 & A^{-1}
 \end{array}$$

Die Elementarmatrix, die den Schritt bewirkt, steht links daneben.

Das Ergebnis stimmt mit dem im Beispiel aus 2.4.5 erhaltenen überein, denn $\det A = -1$.

Um die dreireihige Hilbert-Matrix zu invertieren, rechnen wir nach den Erfahrungen aus 0.5.5 rational.

	A 	E_3 				
$Q_{-\frac{1}{3}}(1,3) \cdot Q_{-\frac{1}{2}}(1,2)$	1	$\frac{1}{2}$	$\frac{1}{3}$	1	0	0
	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	0	1	0
	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{5}$	0	0	1
$Q_{-1}(2,3)$	1	$\frac{1}{2}$	$\frac{1}{3}$	1	0	0
	0	$\frac{1}{12}$	$\frac{1}{12}$	$-\frac{1}{2}$	1	0
	0	$\frac{1}{12}$	$\frac{4}{45}$	$-\frac{1}{3}$	0	1
$S_{180}(3) \cdot S_{12}(2)$	1	$\frac{1}{2}$	$\frac{1}{3}$	1	0	0
	0	$\frac{1}{12}$	$\frac{1}{12}$	$-\frac{1}{2}$	1	0
	0	0	$\frac{1}{180}$	$\frac{1}{6}$	-1	1
$Q_{-\frac{1}{3}}(3,1) \cdot Q_{-1}(3,2)$	1	$\frac{1}{2}$	$\frac{1}{3}$	1	0	0
	0	1	1	-6	12	0
	0	0	1	30	-180	180
$Q_{-\frac{1}{2}}(2,1)$	1	$\frac{1}{2}$	0	-9	60	-60
	0	1	0	-36	192	-180
	0	0	1	30	-180	180
	1	0	0	-9	-36	30
	0	1	0	-36	192	-180
	0	0	1	30	-180	180

2.4.7 Lineare Gleichungssysteme und Elementarmatrizen*

Bei der Lösung von linearen Gleichungssystemen war es hilfreich gewesen, diese mit linearen Abbildungen in Verbindung zu bringen (vgl. 2.3.5). Wer gerne verstehen möchte, wie die in 0.5.4 durchgeführten Umformungen der Koeffizientenmatrix aus der Sicht linearer Abbildungen interpretiert werden können, kann das mit Hilfe der Elementarmatrizen leicht einsehen.

Gegeben sei also das lineare Gleichungssystem $A \cdot x = b$ mit

$$A \in M(m \times n; K) \quad \text{und} \quad b \in K^m.$$

Man betrachtet die Matrix A als lineare Abbildung

$$F_A : K^n \rightarrow K^m, \quad x \mapsto A \cdot x,$$

die Lösungsmenge $\text{Lös}(A, b) \subset K^n$ ist dann das Urbild von b unter F_A , in Zeichen

$$\text{Lös}(A, b) = F_A^{-1}(b).$$

Beim Eliminationsverfahren nach 0.5.4 wird die erweiterte Koeffizientenmatrix (A, b) durch elementare Zeilenumformungen auf Zeilenstufenform (\tilde{A}, \tilde{b}) gebracht. Hat man insgesamt l Umformungen vorgenommen, dann gehören dazu Elementarmatrizen

$$C_1, \dots, C_l \in \text{GL}(m; K) \quad \text{mit} \quad \tilde{A} = C_l \cdot \dots \cdot C_1 \cdot A \quad \text{und} \quad \tilde{b} = C_l \cdot \dots \cdot C_1 \cdot b.$$

Fasst man die Elementarmatrizen zusammen zu $S := C_l \cdot \dots \cdot C_1 \in \text{GL}(m; K)$ so ist also

$$\tilde{A} = S \cdot A \in M(m \times n; K) \quad \text{und} \quad \tilde{b} = S \cdot b \in K^m.$$

Zu den Matrizen A, \tilde{A} und S gehört ein Diagramm

$$\begin{array}{ccc} K^n & \xrightarrow{F_A} & K^m \\ & \searrow F_{\tilde{A}} & \downarrow F_S \\ & & K^m \end{array}$$

linearer Abbildungen, wobei F_S ein Isomorphismus ist. Insbesondere gilt

$$\text{Lös}(A, b) = F_A^{-1}(b) = F_{\tilde{A}}^{-1}(\tilde{b}) = \text{Lös}(\tilde{A}, \tilde{b}).$$

Ist $r := \text{rang } A = \text{rang } \tilde{A}$, so sind die ersten r Zeilen von \tilde{A} linear unabhängig, die restlichen $m - r$ Zeilen sind Null. Daraus folgt für das Bild von $F_{\tilde{A}}$ im K^m

$$F_{\tilde{A}}(K^n) = \{ {}^t(y_1, \dots, y_m) \in K^m : y_{r+1} = \dots = y_m = 0 \}.$$

Daraus folgt das Kriterium für die Existenz einer Lösung zu gegebenem b und $\tilde{b} = {}^t(\tilde{b}_1, \dots, \tilde{b}_m)$:

$$\text{Lös}(A, b) \neq \emptyset \Leftrightarrow \tilde{b} \in F_{\tilde{A}}(K^n) \Leftrightarrow \tilde{b}_{r+1} = \dots = \tilde{b}_m = 0.$$

Das hatten wir durch direkte Rechnung schon in 0.5.3 bemerkt.

Von diesem Standpunkt aus kann man das GAUSS-JORDAN-Verfahren interpretieren als simultane Lösung von linearen Gleichungssystemen. Für eine gegebene Matrix $A \in M(n \times n; K)$ betrachtet man, wie schon in 2.4.5 in einem Spezialfall, die Einträge von A^{-1} als Unbekannte, also

$$A^{-1} = \begin{pmatrix} x_{11} & \dots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \dots & x_{nn} \end{pmatrix}$$

Die Bedingung $A \cdot A^{-1} = E_n$ bedeutet dann für jede Spalte $x_j = {}^t(x_{1j}, \dots, x_{nj})$, dass

$$A \cdot x_j = e_j. \tag{j}$$

Nun formt man A nicht nur um auf Zeilenstufenform, sondern weiter bis auf E_n . Also gibt es ein $S \in GL(n; K)$ derart, dass $\tilde{A} = S \cdot A = E_n$. Die ursprünglichen „rechten Seiten“ e_1, \dots, e_n als Spalten von E_n werden dabei umgeformt zu $S \cdot E_n = S$. Die umgeformte Gleichung (j) lautet dann

$$E_n \cdot \begin{pmatrix} x_{1j} \\ \vdots \\ x_{nj} \end{pmatrix} = \begin{pmatrix} s_{1j} \\ \vdots \\ s_{nj} \end{pmatrix}, \quad \text{d.h.} \quad x_{ij} = s_{ij}.$$

Also gilt $A^{-1} = S$.

2.4.8 Die LR-Zerlegung*

Wir betrachten den Spezialfall eines linearen Gleichungssystems

$$A \cdot x = b, \quad \text{wobei} \quad A \in GL(n; K) \quad \text{und} \quad b \in K^n.$$

In diesem Fall hat man für jedes beliebige b die eindeutige Lösung

$$x = A^{-1} \cdot b.$$

Um den Aufwand für die Berechnung von A^{-1} und die damit verbundenen numerischen Instabilitäten zu reduzieren, kann man ein einfacheres Verfahren anwenden. Wie

in 2.4.7 erläutert, gibt es Elementarmatrizen C_1, \dots, C_l derart, dass das Gleichungssystem

$$A \cdot x = b \quad \text{äquivalent ist zu} \quad \tilde{A} \cdot x = \tilde{b}, \quad \text{wobei} \quad \tilde{A} = S \cdot A \quad \text{und} \quad \tilde{b} = S \cdot b$$

mit $S := C_l \cdot \dots \cdot C_1$. Diese Beschreibung der elementaren Zeilenumformungen an der Koeffizientenmatrix gestattet es, A aus \tilde{A} durch $A = S^{-1} \cdot \tilde{A}$ zu rekonstruieren, und aus beliebigen rechten Seiten b die Ergebnisse $\tilde{b} = S \cdot b$ zu berechnen. Auf diese Weise erhält man eine gute Dokumentation der Umformungen.

Beispiel Sei

$$A := \begin{pmatrix} 1 & 2 & -1 \\ 0 & 1 & -4 \\ 1 & 1 & 2 \end{pmatrix}.$$

Durch elementare Zeilenumformungen erhält man

$$\tilde{A} = Q_1(2,3) \cdot Q_{-1}(1,3) \cdot A = \begin{pmatrix} 1 & 2 & -1 \\ 0 & 1 & -4 \\ 0 & 0 & -1 \end{pmatrix}.$$

Daraus folgt

$$S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 1 & 1 \end{pmatrix} \quad \text{und} \quad S^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & -1 & 1 \end{pmatrix}.$$

Ist nun etwa $b := {}^t(1,2,1)$ gewählt, so erhält man

$$\tilde{b} = S \cdot b = {}^t(1,2,2).$$

Alternativ kann man \tilde{b} wegen $b = S^{-1} \cdot \tilde{b}$ auch mit Hilfe von S^{-1} als Lösung des Gleichungssystems

$$\begin{array}{rcl} y_1 & & = 1 \\ & y_2 & = 2 \\ y_1 - y_2 + y_3 & & = 1 \end{array}$$

„von oben nach unten“ berechnen.

Das Gleichungssystem $\tilde{A} \cdot x = \tilde{b}$ lautet ausgeschrieben

$$\begin{array}{rcl} x_1 + 2x_2 - x_3 & = & 1 \\ & x_2 - 4x_3 & = 2 \\ & & -x_3 & = 2, \end{array}$$

es hat „von unten nach oben“ berechnet die Lösung $x = {}^t(11, -6, -2)$.

Alternativ kann man natürlich in diesem einfachen Fall

$$A^{-1} = \begin{pmatrix} -6 & 5 & 7 \\ 4 & -3 & -4 \\ 1 & -1 & -1 \end{pmatrix}$$

berechnen. Dann ist $x = A^{-1} \cdot b$.

Für die ursprüngliche Matrix A hat man die Zerlegung

$$A = S^{-1} \cdot \tilde{A}.$$

Um eine solche Zerlegung allgemein zu untersuchen, zunächst übliche Namen:

Eine Matrix $D = (d_{ij}) \in M(n \times n; K)$ heißt

obere Dreiecksmatrix, wenn $d_{ij} = 0$ für $i > j$ und
untere Dreiecksmatrix, wenn $d_{ij} = 0$ für $i < j$.

Es ist leicht zu sehen, dass ein Produkt von oberen bzw. unteren Dreiecksmatrizen wieder eine obere bzw. untere Dreiecksmatrix ist, und dass diese Eigenschaften bei der Bildung von Inversen erhalten bleiben. Somit bilden die invertierbaren oberen bzw. unteren Dreiecksmatrizen Untergruppen von $GL(n; K)$.

Wir betrachten nun eine Matrix $A \in GL(n; K)$ und machen die zusätzliche Voraussetzung, dass, wie in obigem Beispiel, bei der Elimination **keine Zeilenvertauschungen** nötig sind. Die zugehörigen Elementarmatrizen sind dann von der Form

$$C = Q_\lambda(i, j) \quad \text{mit} \quad i < j,$$

also untere Dreiecksmatrizen mit Einträgen 1 in der Diagonalen. Das Ergebnis der Elimination

$$R := C_1 \cdot \dots \cdot C_1 \cdot A = S \cdot A = \tilde{A}$$

ist eine obere Dreiecksmatrix mit den Pivots in der Diagonalen. Mit S ist auch $L := S^{-1}$ eine untere Dreiecksmatrix mit Einsen in der Diagonale, das ergibt schließlich die Zerlegung

$$A = L \cdot R.$$

Dabei stehen die Buchstaben L für „links“ und R für „rechts“.

Im allgemeinen sind bei der Elimination Zeilenvertauschungen nötig und oft auch nützlich. Man kann beweisen (vgl. etwa [L-M, 5.2]), dass diese schon vorweg an A vorgenommen werden können, d.h. es gibt eine Permutationsmatrix P (vgl. 3.2.3) derart, dass $P \cdot A$ eine **LR-Zerlegung** gestattet, also

$$P \cdot A = L \cdot R.$$

Damit kann ein lineares Gleichungssystem

$$(P \cdot A) \cdot x = b$$

in zwei besonders einfachen Schritten gelöst werden:

$$(P \cdot A) \cdot x = b \quad \text{bedeutet} \quad (L \cdot R) \cdot x = L \cdot (R \cdot x) = b.$$

Man löst im ersten Schritt $L \cdot y = b$ von oben nach unten, die Lösung y ergibt das umgeformte \tilde{b} . Im zweiten Schritt löst man von unten nach oben das System $R \cdot x = y$.

2.4.9 Dualität*

Bei der Lösung eines homogenen linearen Gleichungssystems wird zu einer vorgegebenen Matrix $A \in M(m \times n; K)$ eine Basis des Vektorraums

$$W := \{x \in K^n : A \cdot x = \mathbf{o}\} = \text{Lös}(A; \mathbf{o})$$

berechnet. Schon in 0.2.3 und 0.4.2 hatten wir umgekehrt für Geraden im \mathbb{R}^2 und Ebenen im \mathbb{R}^3 passende Gleichungen bestimmt. Das waren ganz einfache Spezialfälle von dem allgemeinen

Problem Zu einem durch ein Erzeugendensystem gegebenen Untervektorraum $W \subset K^n$ ist eine Matrix $A \in M(m \times n; K)$ gesucht, derart dass $W = \text{Lös}(A; \mathbf{o})$.

Das kann man auffassen als ein „inverses Problem“: *Zu gegebener Lösung ist das passende Problem gesucht.* So etwas gibt es auch bei der Besetzung von Stellen, die öffentlich ausgeschrieben werden. Will man eine bestimmte Person darauf bekommen, muss man den Ausschreibungstext maßgeschneidert formulieren.

Um dieses inverse (oder „duale“) Problem zu lösen, benutzen wir einen formal sehr einfach zu beschreibenden Spezialfall der allgemeinen Theorie von *Dualität* in Vektorräumen. Bisher hatten wir Vektoren des K^n als Zeilen oder Spalten geschrieben, je nachdem, was einfacher aufzuschreiben war. In diesem Abschnitt sind Vektoren des K^n Spalten, d.h. wir identifizieren

$$K^n = M(n \times 1; K).$$

Zu diesem Vektorraum gehört der Vektorraum

$$(K^n)^* := M(1 \times n; K),$$

seine Elemente sind Zeilen. Ist nun

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n \quad \text{und} \quad a = (a_1, \dots, a_n) \in (K^n)^*,$$

so ist das Matrizenprodukt ein Skalar,

$$a \cdot x = \sum_{i=1}^n a_i x_i \in M(1 \times 1; K) = K.$$

Jedes $a \in (K^n)^*$ erklärt also eine lineare Abbildung

$$a : K^n \rightarrow K, \quad x \mapsto a \cdot x,$$

und alle derartigen linearen Abbildungen entstehen so.

Ist V ein beliebiger K -Vektorraum, so nennt man eine lineare Abbildung $\varphi: V \rightarrow K$ eine **Linearform**, der Vektorraum

$$V^* := \text{Hom}_K(V, K)$$

der Linearformen heißt der **duale Vektorraum**. In diesem Sinn ist $(K^n)^*$ der duale Vektorraum zu K^n . Die Abbildung

$$K^n \rightarrow (K^n)^*, v \mapsto {}^t v,$$

ist ein Isomorphismus. Diese etwas abstrakte Betrachtungsweise hilft nun, zu gegebenen Vektoren x die gesuchten durch Linearformen a beschriebenen Gleichungen zu finden. Somit ist es angebracht, zu dem gegebenen $W \subset K^n$ all die Kandidaten für die Zeilen von A d.h. all die $a \in (K^n)^*$ zu betrachten, die auf ganz W verschwinden, das ist der Untervektorraum

$$W^0 := \{a \in (K^n)^* : a \cdot x = 0 \text{ für alle } x \in W\} \subset (K^n)^*,$$

er heißt **Annulator** von W . Nun gilt es, einen Basis von W^0 zu finden!

Ist $W = \text{Span}(w_1, \dots, w_k)$ mit $k \geq r := \dim W$, so betrachten wir die Matrix

$$B := (w_1, \dots, w_k) \in M(n \times k; K) \text{ mit } \text{rang } B = r.$$

Dann ist die Bedingung $a \cdot x = 0$ für alle $x \in W$ gleichwertig mit

$$a \cdot B = \mathbf{0} \in M(1 \times k; K) \Leftrightarrow {}^t B \cdot {}^t a = \mathbf{0} \in M(k \times 1; K). \quad (*)$$

Diese Form der Bedingung ermöglicht es, die gesuchte Basis von W^0 durch Lösung eines linearen Gleichungssystems zu bestimmen. Ist

$$V := \text{Lös}({}^t B, \mathbf{0}) = \{{}^t a \in K^n : {}^t B \cdot {}^t a = \mathbf{0}\} \subset K^n,$$

so folgt aus den äquivalenten Bedingungen (*), dass

$$W^0 = {}^t V \subset (K^n)^*.$$

Da die Transposition $K^n \rightarrow (K^n)^*$ ein Isomorphismus ist, gilt

$$\dim W^0 = \dim V = n - \text{rang } {}^t B = n - \text{rang } B = n - r =: m.$$

Durch Lösung des Systems ${}^t B \cdot {}^t a = 0$ erhält man eine Basis (v_1, \dots, v_m) von V und daraus eine Basis $({}^t v_1, \dots, {}^t v_m)$ von W^0 . Als Zeilen eingetragen ergibt das die Matrix

$$A := \begin{pmatrix} {}^t v_1 \\ \vdots \\ {}^t v_m \end{pmatrix} \in M(m \times n; K) \text{ mit } \text{rang } A = m.$$

Um zu zeigen, dass A das gegebene Problem löst, vergleichen wir den gegebenen Vektorraum W mit

$$W' := \{x \in K^n : A \cdot x = \mathbf{0}\}.$$

Es gilt $\dim W' = n - \text{rang } A = n - m = r = \dim W$. Ist $x \in W$, so ist $v_i \cdot x = 0$ für $i = 1, \dots, m$, also $x \in W'$. Also ist $W \subset W'$ und somit $W = W'$. Damit ist das gestellte Problem gelöst.

Man beachte, dass die Gleichung $\text{rang } {}^t B = \text{rang } B$ eine entscheidende Stelle im Beweis ist. ■

Beispiel Ist $w_1 = {}^t(1, 0, 2)$ und $w_2 := {}^t(1, -1, -1)$, so ist $W = \text{Span}(w_1, w_2) \subset \mathbb{R}^3$ eine Ebene. Schon in 0.4.2 hatten wir eine Gleichung von W bestimmt durch das Vektorprodukt

$$w_1 \times w_2 = (2, 3, -1) =: (a_1, a_2, a_3) = a.$$

Nach der oben beschriebenen Methode ist

$$A = \begin{pmatrix} 1 & 0 & 2 \\ 1 & -1 & -1 \end{pmatrix}, \quad \text{also } v = (-2, -3, 1) = -a.$$

In diesem Fall ist $W^0 = \mathbb{R} \cdot (2, 3, -1)$, also ist die Gleichung für W bis auf einen Faktor $\neq 0$ eindeutig bestimmt.

Die Lösung dieses Problems im K^n ist nur ein Startpunkt für die Theorie der dualen Vektorräume. Etwas mehr darüber findet man etwa in [FI₁, 6.1]. Im Fall $K = \mathbb{R}$ kann man $W^0 \subset (\mathbb{R}^n)^*$ durch das orthogonale Komplement $W^\perp \subset \mathbb{R}^n$ ersetzen. Das wird in 5.3.3 erklärt.

2.5 Transformationen

2.5.1 Basistransformationen und Koordinatentransformationen

Hat man in einem Vektorraum V eine Basis $\mathcal{A} = (v_1, \dots, v_n)$ so erhält man daraus ein Koordinatensystem

$$\Phi_{\mathcal{A}} : K^n \rightarrow V, e_i \mapsto v_i, (x_1, \dots, x_n) \mapsto \sum_{i=1}^n x_i v_i.$$

Diese Abbildung ist ein Isomorphismus und sie ist sehr nützlich, denn man kann einen Vektor $u \in V$ durch seine Koordinaten

$$x = \Phi_{\mathcal{A}}^{-1}(u) = (x_1, \dots, x_n) \in K^n$$

ersetzen, was für viele Rechnungen von Vorteil ist. Die Behandlung von geometrischen Fragen kann oft stark vereinfacht werden, wenn eine Basis gewählt wird, die der Situation angepasst ist. Daher ist zu klären, wie der Übergang von einer alten Basis \mathcal{A} zu einer neuen Basis

$$\mathcal{B} = (w_1, \dots, w_n) \quad \text{und} \quad \Phi_{\mathcal{B}} : K^n \rightarrow V, (y_1, \dots, y_n) \mapsto \sum_{i=1}^n y_i w_i$$

beschrieben werden kann. Insbesondere stellt sich die Frage, wie man die „neuen“ Koordinaten y aus den „alten“ Koordinaten x berechnen kann. Wir geben zunächst zwei ganz elementare Beispiele.

Beispiel 1 Im Fall $\dim V = 1$ sei $\mathcal{A} = (v)$, $\mathcal{B} = (w)$ mit $v, w \neq \mathbf{0}$ und

$$w = s \cdot v \quad \text{mit} \quad s \in K^*. \quad (*)$$

Jedes $u \in V$ hat die beiden Darstellungen

$$u = x \cdot v = y \cdot w \quad \text{mit} \quad x, y \in K.$$

Daraus folgt $x \cdot v = y \cdot s \cdot v$, also $x = s \cdot y$ und

$$y = s^{-1} \cdot x. \quad (**)$$

Aus (*) und (**) sieht man, dass sich die Koordinate mit dem inversen Faktor transformiert wie der Basisvektor. Das ist ganz klar: Ist w doppelt so lang wie v , so genügt mit w der halbe Faktor; so wie bei Währungskursen und Preisen.

Beispiel 2 In $V = K^2$ betrachten wir die Basen $\mathcal{A} = (e_1, e_2)$ und $\mathcal{B} = (w_1, w_2)$ mit $w_1 = e_1 + e_2$ und $w_2 = 2e_1 + e_2$. Für jeden Vektor $u \in K^2$ hat man zwei verschiedene Darstellungen

$$\begin{aligned} u &= x_1 e_1 + x_2 e_2 = y_1 w_1 + y_2 w_2 = y_1(e_1 + e_2) + y_2(2e_1 + e_2) \\ &= (y_1 + 2y_2)e_1 + (y_1 + y_2)e_2. \end{aligned}$$

Also folgt $x_1 = y_1 + 2y_2$ und $x_2 = y_1 + y_2$.

Das Ganze kann man auch in Matrizen beschreiben. Ist

$$S := \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$$

die Matrix mit den Vektoren von \mathcal{B} als Spalten, so wird $\Phi_{\mathcal{B}} : K^2 \rightarrow K^2$ beschrieben durch S , d.h.

$$w_j = \sum_{i=1}^2 s_{ij} e_i \quad \text{für } j = 1, 2. \quad (*)$$

Aus der obigen Rechnung folgt

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}, \quad \text{also } x = S \cdot y,$$

wenn x und y als Spaltenvektoren angesehen werden. Umgekehrt gilt daher

$$y = S^{-1} \cdot x. \quad (**)$$

Wie wir in 2.4.6 schon ausgerechnet hatten, ist

$$S^{-1} = \begin{pmatrix} -1 & 2 \\ 1 & -1 \end{pmatrix}, \quad \text{also } y_1 = -x_1 + 2x_2, y_2 = x_1 - x_2.$$

Durch Vergleich von (*) und (**) sieht man, dass sich die Übergänge zwischen Basen und Koordinaten in diesem Fall durch die inversen Matrizen beschreiben lassen. Wir wollen nun zeigen, dass dies allgemein gilt.

Gegeben sei also ein K -Vektorraum V mit zwei Basen

$$\mathcal{A} = (v_1, \dots, v_n) \quad \text{und} \quad \mathcal{B} = (w_1, \dots, w_n).$$

Jeder Vektor w_j aus \mathcal{B} hat eine eindeutige Darstellung

$$w_j = \sum_{i=1}^n s_{ij} v_i \quad \text{mit } s_{ij} \in K.$$

Diese Skalare kann man zusammenfassen zu einer Matrix

$$S_{\mathcal{B}}^{\mathcal{A}} := (s_{ij}) \in \text{GL}(n; K)$$

mit den zu w_1, \dots, w_n gehörenden Skalaren als Spalten. Man kann S_B^A bezeichnen als *Transformationsmatrix des Basiswechsels* von \mathcal{A} nach \mathcal{B} . Man betrachtet \mathcal{B} als die neue Basis, sie wird beschrieben durch die alte Basis \mathcal{A} .

Weiter gehören zu \mathcal{A} und \mathcal{B} zwei Koordinatensysteme

$$\Phi_{\mathcal{A}} : K^n \rightarrow V \quad \text{und} \quad \Phi_{\mathcal{B}} : K^n \rightarrow V.$$

Da beides Isomorphismen sind, erhält man daraus einen Isomorphismus

$$T_B^A := \Phi_B^{-1} \circ \Phi_{\mathcal{A}} : K^n \rightarrow K^n,$$

den man als invertierbare Matrix

$$T_B^A \in GL(n; K)$$

ansehen kann. T_B^A heißt die *Transformationsmatrix der Koordinaten* bezüglich \mathcal{A} und \mathcal{B} . Ist $u \in V$ und

$$u = \Phi_{\mathcal{A}}(x) = \Phi_{\mathcal{B}}(y), \quad \text{so gilt} \quad y = T_B^A(x).$$

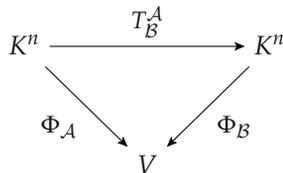
Mit Hilfe von T_B^A erhält man also die neuen Koordinaten aus den alten. Der Zusammenhang zwischen S_B^A und T_B^A ist naheliegend:

Satz Sind \mathcal{A} und \mathcal{B} zwei endliche Basen eines Vektorraums V , so gilt für die oben erklärten Transformationsmatrizen, dass

$$T_B^A = (S_B^A)^{-1}, \quad \text{also} \quad S_B^A = T_{\mathcal{A}}^{\mathcal{B}}.$$

Kurz ausgedrückt: Die Koordinaten transformieren sich invers zu den Basen.

Beweis Zum besseren Verständnis der Situation kann das Diagramm von Isomorphismen



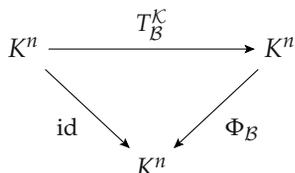
helfen. Da $T_B^A = \Phi_B^{-1} \circ \Phi_{\mathcal{A}}$, genügt es $\Phi_{\mathcal{A}} \circ S_B^A = \Phi_{\mathcal{B}}$ zu zeigen. Für die Gleichheit dieser beiden Abbildungen von K^n nach V genügt es nach 2.4.1 zu zeigen, dass sie auf den Basisvektoren e_j des K^n gleiche Werte haben. Das ist leicht zu sehen:

$$\Phi_{\mathcal{B}}(e_j) = w_j,$$

$$(\Phi_{\mathcal{A}} \circ S_B^A)(e_j) = \Phi_{\mathcal{A}}(S_B^A(e_j)) = \Phi_{\mathcal{A}}(s_{1j}, \dots, s_{nj}) = \sum_{i=1}^n s_{ij} v_i = w_j.$$



Der wichtigste Spezialfall ist der, dass wie in Beispiel 2 im K^n statt der kanonischen Basis \mathcal{K} eine andere Basis \mathcal{B} gewählt wird; als Spalten in eine Matrix eingetragen ergibt das $S_{\mathcal{B}}^{\mathcal{K}}$. Da $\Phi_{\mathcal{K}}$ die identische Abbildung ist, sieht unser Diagramm dann so aus



Es folgt für diese Abbildungen, als Matrizen angesehen,

$$S_{\mathcal{B}}^{\mathcal{K}} = T_{\mathcal{K}}^{\mathcal{B}} = \Phi_{\mathcal{B}}, \quad \text{also} \quad T_{\mathcal{B}}^{\mathcal{K}} = (S_{\mathcal{B}}^{\mathcal{K}})^{-1}.$$

Wer gerne mit Diagrammen spielt, kann sich auch noch überlegen, dass die Transformationsmatrix $T_{\mathcal{B}}^{\mathcal{A}}$ eine beschreibende Matrix der identischen Abbildung von V ist, genauer gilt

$$T_{\mathcal{B}}^{\mathcal{A}} = M_{\mathcal{B}}^{\mathcal{A}}(\text{id}_V) = S_{\mathcal{B}}^{\mathcal{B}}.$$

2.5.2 Transformationsformel für lineare Abbildungen

Ist $F: V \rightarrow W$ eine lineare Abbildung, so hatten wir für Basen \mathcal{A} und \mathcal{B} von V und W in 2.4.2 eine darstellende Matrix $M_{\mathcal{B}}^{\mathcal{A}}$ erklärt. Sind nun \mathcal{A}' und \mathcal{B}' weitere Basen, so stellt sich die Frage nach dem Zusammenhang zwischen

$$M_{\mathcal{B}}^{\mathcal{A}} \quad \text{und} \quad M_{\mathcal{B}'}^{\mathcal{A}'}$$

Wir beginnen mit dem extrem einfachen aber schon typischen

Beispiel 1 Ist $\dim V = \dim W = 1$, so hat man $\mathcal{A} = (v)$, $\mathcal{A}' = (v')$ mit $\mathbf{o} \neq v, v' \in V$ und $\mathcal{B} = (w)$, $\mathcal{B}' = (w')$ mit $\mathbf{o} \neq w, w' \in W$.

Dann gibt es $s, t \in K^*$ so dass $w = s \cdot w'$ und $v = t \cdot v'$. Für die entsprechenden Koordinaten gilt $x' = tx$ und $y' = sy$. Ist nun $F: V \rightarrow W$ gegeben durch

$$F(v) = a \cdot w \quad \text{mit} \quad a \in K,$$

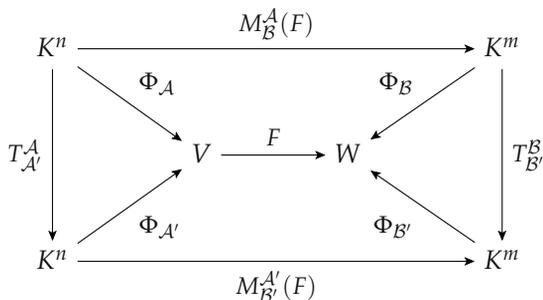
so folgt

$$F(v') = F(t^{-1} \cdot v) = t^{-1} \cdot F(v) = t^{-1} \cdot a \cdot w = s \cdot a \cdot t^{-1} \cdot w' = a' \cdot w',$$

wenn $a' := s \cdot a \cdot t^{-1}$. In diesem Fall ist also

$$M_{\mathcal{B}'}^{A'} = (a') = s \cdot (a) \cdot t^{-1} = s \cdot M_{\mathcal{B}}^A \cdot t^{-1}.$$

Der allgemeine Fall verläuft ganz analog, nur die beteiligten Matrizen können größer werden. Am übersichtlichsten ist die Situation zu beschreiben durch das Diagramm



wobei $n = \dim V$, $m = \dim W$. Dabei werden die darstellenden Matrizen $M_{\mathcal{B}}^A(F)$ und $M_{\mathcal{B}'}^{A'}(F)$, sowie die invertierbaren Transformationsmatrizen $T_{\mathcal{A}'}^A$ und $T_{\mathcal{B}'}^B$, der Koordinaten (vgl. 2.5.1) als lineare Abbildungen der Standardräume angesehen.

Wie wir in 2.4.2 und 2.5.1 gesehen hatten, kommutieren die vier Teildiagramme des obigen Diagramms, also führen auch je zwei mögliche Wege von K^n nach K^m zum gleichen Ergebnis. Das kann man zusammenfassen in einer

Transformationsformel Ist $F : V \rightarrow W$ eine lineare Abbildung und hat man endliche Basen

$$\mathcal{A}, \mathcal{A}' \text{ von } V \text{ und } \mathcal{B}, \mathcal{B}' \text{ von } W,$$

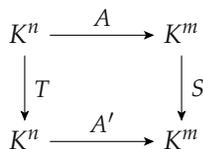
so gilt für die darstellenden Matrizen von F

$$M_{\mathcal{B}'}^{A'}(F) = T_{\mathcal{B}'}^B \cdot M_{\mathcal{B}}^A(F) \cdot (T_{\mathcal{A}'}^A)^{-1}. \quad \blacksquare$$

Das wird vielleicht etwas suggestiver, wenn man weniger Buchstaben verwendet. Setzt man

$$A := M_{\mathcal{B}}^A(F), \quad A' := M_{\mathcal{B}'}^{A'}(F), \quad T := T_{\mathcal{A}'}^A \text{ und } S := T_{\mathcal{B}'}^B,$$

so hat man das vereinfachte Diagramm



und die Transformationsformel

$$A' = S \cdot A \cdot T^{-1}.$$

Im Spezialfall eines Endomorphismus erhält man das

Korollar Ist $F : V \rightarrow V$ eine lineare Abbildung und hat man endliche Basen $\mathcal{B}, \mathcal{B}'$ von V , so gilt

$$M_{\mathcal{B}'}(F) = T_{\mathcal{B}'}^{\mathcal{B}} \cdot M_{\mathcal{B}}(F) \cdot (T_{\mathcal{B}'}^{\mathcal{B}})^{-1}.$$

Ist wieder $A := M_{\mathcal{B}}(F)$, $A' = M_{\mathcal{B}'}(F)$ und $S := T_{\mathcal{B}'}^{\mathcal{B}}$, so hat man das Diagramm

$$\begin{array}{ccc} K^n & \xrightarrow{A} & K^n \\ \downarrow S & & \downarrow S \\ K^n & \xrightarrow{A'} & K^n \end{array}$$

und die Transformationsformel

$$A' = S \cdot A \cdot S^{-1}.$$

In späteren Beispielen ist oft $\mathcal{B} = \mathcal{K} = (e_1, \dots, e_n)$ die kanonische Basis. Führt man eine neue Basis $\mathcal{B}' = (v_1, \dots, v_n)$ ein, so hat man das Diagramm

$$\begin{array}{ccccc} K^n & \xrightarrow{A} & K^n & & \\ \Phi_{\mathcal{B}'} \uparrow & & \uparrow \Phi_{\mathcal{B}'} & \cdot & \\ K^n & \xrightarrow{A'} & K^n & & \end{array}$$

Da $\Phi_{\mathcal{B}'}(e_j) = v_j$ für $j = 1, \dots, n$ erhält man die Matrix, die $S^{-1} = \Phi_{\mathcal{B}'}$ beschreibt, indem man die Vektoren v_1, \dots, v_n als Spalten einträgt, kurz

$$S^{-1} = \left(\begin{array}{c|ccc|c} & & & & \\ & v_1 & \dots & v_n & \\ & | & & | & \end{array} \right).$$

Durch Berechnung der Inversen findet man S , dann ist $A' = S \cdot A \cdot S^{-1}$.

2.5.3 Eine Normalform für darstellende Matrizen

Im vorigen Abschnitt haben wir gesehen, wie sich die darstellenden Matrizen beim Übergang zu anderen Basen transformieren. Es ist nun naheliegend zu fragen, ob man zu einer vorgegebenen linearen Abbildung die Basen so wählen kann, dass die beschreibende Matrix besonders übersichtlich wird. In diesem Abschnitt werden wir das Problem für Homomorphismen $F : V \rightarrow W$ lösen; das ist recht einfach, da man hier zwei

Basen, nämlich in V und W , variieren kann. Bei einem Endomorphismus ist es angemessen nur eine Basis zu verändern. Dadurch wird das Problem viel schwieriger, es ist das zentrale Thema des Kapitels 4 über Eigenwerte.

Zunächst ist es ziemlich klar, dass eine $(m \times n)$ -Matrix vom Rang r „besonders übersichtlich“ ist, wenn sie die Form

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

hat. Die durch dieses A beschriebene lineare Abbildung $F_A : K^n \rightarrow K^m$ hat folgende Eigenschaft: Sind

$$\mathcal{K} = (e_1, \dots, e_n) \quad \text{und} \quad \mathcal{K}' = (e'_1, \dots, e'_m)$$

die kanonischen Basen von K^n und K^m , so erkennt man an den Spalten von A , dass

$$F_A(e_j) = \begin{cases} e'_j & \text{für } j = 1, \dots, r, \\ \mathbf{0} & \text{für } j = r + 1, \dots, n. \end{cases}$$

Allgemeiner hat man den folgenden

Satz Ist $F : V \rightarrow W$ eine lineare Abbildung zwischen endlich dimensionalen Vektorräumen vom Rang $r = \text{rang} F$, so gibt es Basen \mathcal{A} von V und \mathcal{B} von W , so dass

$$M_{\mathcal{B}}^{\mathcal{A}} = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Betrachtet man Matrizen als lineare Abbildungen und verwendet man die Transformationsformel aus 2.5.2, so erhält man das

Korollar Zu jeder Matrix $A \in M(m \times n; K)$ gibt es $S \in GL(m; K)$ und $T \in GL(n; K)$ so dass

$$S \cdot A \cdot T^{-1} = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}, \quad \text{wobei } r = \text{rang } A. \quad \blacksquare$$

Diese transformierte Matrix nennt man eine **Normalform** der $(m \times n)$ -Matrizen vom Rang r .

Beweis des Satzes Basen der gesuchten Art wurden schon zum Beweis der Dimensionsformel in 2.3.4 konstruiert. Es genügt, die Bezeichnungen etwas zu variieren. Eine Basis (w_1, \dots, w_r) von $F(V)$ wird ergänzt zu einer Basis

$$\mathcal{B} = (w_1, \dots, w_r, w_{r+1}, \dots, w_m) \quad \text{von } W.$$

Dazu gibt es, wie in 2.3.4 ausgeführt, eine Basis

$$\mathcal{A} = (v_1, \dots, v_r, v_{r+1}, \dots, v_n) \quad \text{von } V$$

derart dass

$$F(v_j) = \begin{cases} w_j & \text{für } j = 1, \dots, r, \\ \mathbf{o} & \text{für } j = r + 1, \dots, n. \end{cases}$$

Dann hat $M_{\mathcal{B}}^{\mathcal{A}}(F)$ offensichtlich die angegebene Normalform. ■

Vorsicht! Die Basen \mathcal{A} und \mathcal{B} im Satz und entsprechend die Matrizen S und T im Korollar sind keinesfalls eindeutig bestimmt. Das sieht man schon im einfachsten Fall $m = n = 1$ und $A = (1)$. Hier kann man

$$S = T = (\lambda) \quad \text{mit } \lambda \in K^*$$

beliebig wählen.

Erfreulicherweise gibt es ein einfaches Rechenverfahren, um eine gegebene Matrix auf Normalform zu transformieren. Eine formal schöne Begründung des Verfahrens erhält man wieder mit Hilfe der Elementarmatrizen.

Sei also $A \in M(m \times n; K)$ gegeben. Im ersten Teil des Verfahrens wird A durch elementare Zeilenumformungen auf Zeilenstufenform A' gebracht. Im zweiten Teil kann man A' durch elementare Spaltenumformungen auf die Normalform A'' bringen. Diese Umformungen führt man im ersten Teil auch an E_m , im zweiten Teil auch an E_n durch. Mit Hilfe von Elementarmatrizen

$$B_1, \dots, B_k \in GL(m; K) \quad \text{und} \quad C_1, \dots, C_l \in GL(n; K)$$

erhält man folgendes Schema

E_m	A	
$B_1 \cdot E_m$	$B_1 \cdot A$	
\vdots	\vdots	
$B_k \cdot \dots \cdot B_1 \cdot E_m$	$B_k \cdot \dots \cdot B_1 \cdot A = A'$	E_n
	$B_k \cdot \dots \cdot B_1 \cdot A \cdot C_1$	$E_n \cdot C_1$
	\vdots	\vdots
	$B_k \cdot \dots \cdot B_1 \cdot A \cdot C_1 \cdot \dots \cdot C_l = A''$	$E_n \cdot C_1 \cdot \dots \cdot C_l$

Mit Hilfe der so erhaltenen Matrizen

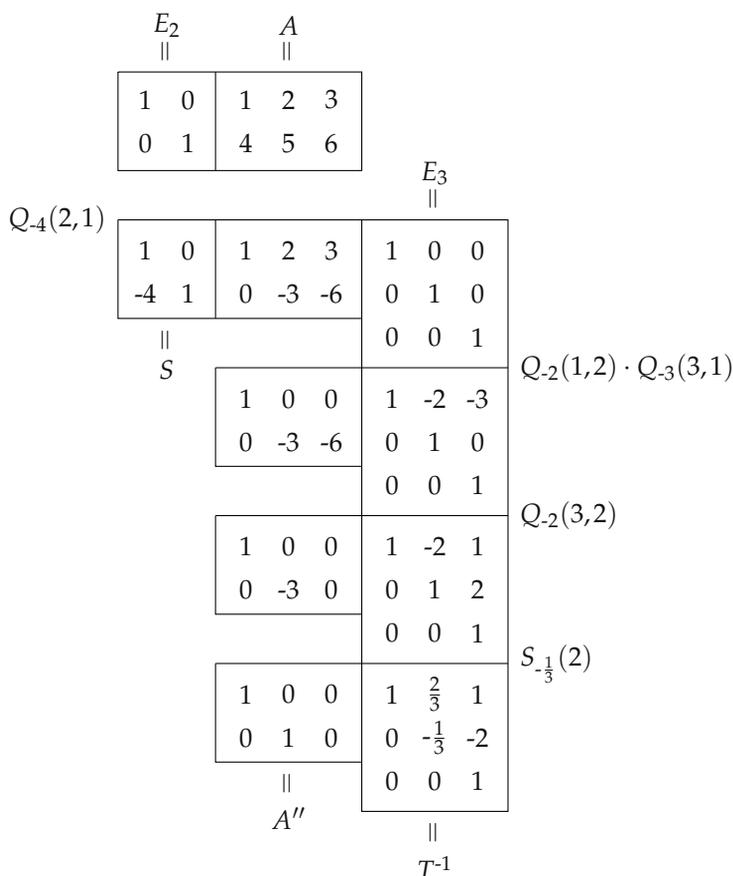
$$S := B_k \cdot \dots \cdot B_1 \in \text{GL}(m;K) \quad \text{und} \\ T^{-1} := C_1 \cdot \dots \cdot C_l \in \text{GL}(n;K)$$

erhält man die Normalform $A'' = S \cdot A \cdot T^{-1}$.

Beispiel 2 Um nicht viel rechnen zu müssen, wählen wir $m = 2, n = 3$ und

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}.$$

An den Rändern des Schemas stehen die den Umformungen entsprechenden Elementarmatrizen.



Im Fall eines Endomorphismus $F : V \rightarrow V$ ist es angebracht, nur eine Basis \mathcal{B} von V zu verwenden. Dann kann man versuchen, die Matrix $M_{\mathcal{B}}(F)$ durch geschickte Wahl von \mathcal{B} möglichst einfach werden zu lassen. Da man hier viel weniger Freiheiten hat, als bei der Variation von zwei Basen, ist diese Aufgabe weit schwieriger. Im Fall von

Matrizen kann man eine $n \times n$ -Matrix A umformen zu $S \cdot A \cdot S^{-1}$ mit $S \in \text{GL}(n;K)$. Ist $n = 1$ und $A = (\lambda)$, so ist $S = (s)$ und $S \cdot A \cdot S^{-1} = A$, denn $s \cdot \lambda \cdot s^{-1} = \lambda$. Der zu A gehörende Wert $\lambda \in K$ kann also nicht verändert werden. Das führt zur Untersuchung von „Eigenwerten“ und „Eigenvektoren“; dazu benötigt man Determinanten, die im folgenden Kapitel beschrieben werden.

*... in sequentibus docebimus,
determinantem huius formae vocabimus.*
CARL FRIEDRICH GAUSS

Kapitel 3

Determinanten

3.1 Motivation

Determinanten treten in der Mathematik an verschiedenen Stellen auf. Wir geben hier einige elementare Situationen an, in denen man auf Determinanten stößt.

3.1.1 Lineare Gleichungssysteme

Zum ersten Mal tauchen Rechenausdrücke in Form von Determinanten bei der Lösung von linearen Gleichungssystemen auf: bei LEIBNIZ 1683 und später bei CRAMER 1750. Am einfachsten sieht man das bei zwei Gleichungen mit zwei Unbekannten:

$$\begin{aligned} (1) \quad a_{11}x_1 + a_{12}x_2 &= b_1 \\ (2) \quad a_{21}x_1 + a_{22}x_2 &= b_2 \end{aligned} \quad A := \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

Dabei setzen wir $\text{rang } A = 2$ voraus, nach 0.3.6 ist das äquivalent zu $a_{11}a_{22} - a_{12}a_{21} \neq 0$. Aus der allgemeinen Theorie weiß man, dass es in diesem Fall genau eine Lösung gibt. Um sie explizit auszurechnen, benutzen wir geeignete Umformungen. Da der Fall $a_{22} = a_{12} = 0$ durch die Voraussetzung $\text{rang } A = 2$ ausgeschlossen ist, können wir die Gleichung $a_{22} \cdot (1) - a_{12} \cdot (2)$ benutzen, sie lautet

$$(a_{11}a_{22} - a_{21}a_{12})x_1 = a_{22}b_1 - a_{12}b_2, \quad \text{also } x_1 = \frac{a_{22}b_1 - a_{12}b_2}{a_{11}a_{22} - a_{21}a_{12}}.$$

Analog erhält man aus $a_{11} \cdot (2) - a_{21} \cdot (1)$

$$(a_{11}a_{22} - a_{21}a_{12})x_2 = a_{11}b_2 - a_{21}b_1, \quad \text{also } x_2 = \frac{a_{11}b_2 - a_{21}b_1}{a_{11}a_{22} - a_{21}a_{12}}.$$

Das kann man mit Hilfe von Determinanten von (2×2) -Matrizen so schreiben:

$$x_1 = \frac{\det \begin{pmatrix} b_1 & a_{12} \\ b_2 & a_{22} \end{pmatrix}}{\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}}, \quad x_2 = \frac{\det \begin{pmatrix} a_{11} & b_1 \\ a_{21} & b_2 \end{pmatrix}}{\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}}.$$

Diese Formeln nennt man **CRAMERSche Regel** im Fall $n = 2$.

3.1.2 Flächeninhalt und Orientierung

Bevor wir die allgemeine Theorie der Determinanten starten, soll in diesem Abschnitt erst einmal ganz elementar die geometrische Bedeutung im \mathbb{R}^2 beleuchtet werden. Sind $v = (a_1, a_2)$ und $w = (b_1, b_2) \in \mathbb{R}^2$ gegeben, so tragen wir sie als Zeilen ein in die Matrix

$$A = \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}.$$

Wie wir schon in 0.3.6 gesehen hatten, sind v, w genau dann linear unabhängig, wenn

$$\det A := a_1 b_2 - a_2 b_1 \neq 0.$$

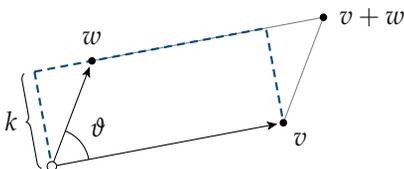
Die naheliegende Frage ist, was der Wert der reellen Zahl $\det A$ bedeutet. Der Betrag hängt eng zusammen mit dem von v und w aufgespannten **Parallelogramm**

$$P := \{\lambda v + \mu w \in \mathbb{R}^2 : \lambda, \mu \in \mathbb{R}, 0 \leq \lambda, \mu \leq 1\}.$$

Bezeichnet $I(P)$ den Flächeninhalt von P , so gilt das

Lemma $I(P) = |\det A|$.

Beweis



Nach dem Prinzip von CAVALIERI (man denke an die Verschiebung eines Papierstoßes) gilt

$$I(P) = \text{Grundlinie} \cdot \text{Höhe} = \|v\| \cdot (\|w\| \cdot \sin \vartheta), \quad (*)$$

wobei $\vartheta = \angle(v, w) \in [0, \pi]$ den nicht orientierten Winkel zwischen v und w bezeichnet (vgl. 0.3.3). Um die Formel (*) mit der Determinante in Verbindung zu bringen, geben wir zwei Wege an.

1. *Mit dem Vektorprodukt* Dazu legen wir den \mathbb{R}^2 in den \mathbb{R}^3 , d.h. wir betrachten zu v und w die Vektoren

$$v' = (a_1, a_2, 0) \quad \text{und} \quad w' = (b_1, b_2, 0) \in \mathbb{R}^3.$$

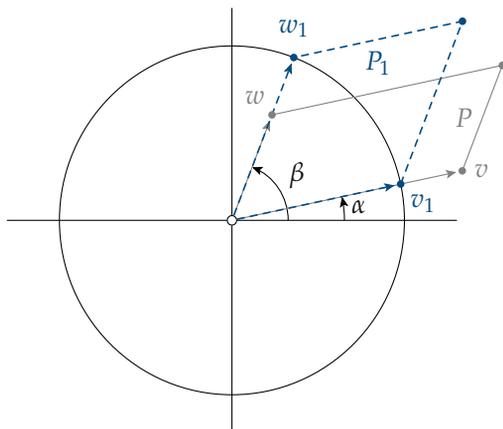
Dann ist $\|v'\| = \|v\|$ und $\|w'\| = \|w\|$, sowie $v' \times w' = (0, 0, a_1 b_2 - a_2 b_1)$. Daraus folgt

$$\|v' \times w'\| = |\det A|.$$

In 0.3.7 hatten wir gezeigt, dass $\|v' \times w'\| = \|v'\| \cdot \|w'\| \cdot \sin \vartheta$, also ergibt sich insgesamt

$$I(P) = \|v\| \cdot \|w\| \cdot \sin \vartheta = \|v'\| \cdot \|w'\| \cdot \sin \vartheta = \|v' \times w'\| = |\det A|.$$

2. *Mit einem Additionstheorem*



Wir können $v \neq 0$ und $w \neq 0$ annehmen (sonst ist $I(P) = 0$) und diese beiden Vektoren normieren zu

$$v_1 = \frac{1}{\|v\|} \cdot v = (\cos \alpha, \sin \alpha), \quad w_1 = \frac{1}{\|w\|} \cdot w = (\cos \beta, \sin \beta).$$

Bezeichnet P_1 das von v_1 und w_1 aufgespannte Parallelogramm, so gilt nach den elementaren Regeln für Flächeninhalte

$$I(P) = \|v\| \cdot \|w\| \cdot I(P_1).$$

Daraus folgt aus (*) und dem Additionstheorem für den Sinus, dass

$$I(P_1) = \sin \vartheta = |\sin(\beta - \alpha)| = |\sin \beta \cos \alpha - \cos \beta \sin \alpha| = \left| \det \begin{pmatrix} \cos \alpha & \sin \alpha \\ \cos \beta & \sin \beta \end{pmatrix} \right|.$$

Insgesamt erhält man daraus

$$\begin{aligned} \left| \det \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix} \right| &= \left| \det \begin{pmatrix} \|v\| \cdot \cos \alpha & \|v\| \cdot \sin \alpha \\ \|w\| \cdot \cos \beta & \|w\| \cdot \sin \beta \end{pmatrix} \right| \\ &= \left| \|v\| \cdot \|w\| \cdot \cos \alpha \sin \beta - \|v\| \cdot \|w\| \cdot \sin \alpha \cos \beta \right| \\ &= \|v\| \cdot \|w\| \cdot \left| \det \begin{pmatrix} \cos \alpha & \sin \alpha \\ \cos \beta & \sin \beta \end{pmatrix} \right| = \|v\| \cdot \|w\| \cdot I(P_1) = I(P). \end{aligned}$$

■

Nachdem der Betrag von $\det A$ als Flächeninhalt nachgewiesen wurde, bleibt die Frage nach einer Interpretation des *Vorzeichens* von $\det A$. Grundlegend ist die folgende Beobachtung: Vertauscht man $v = (a_1, a_2)$ und $w = (b_1, b_2)$, so ist

$$\det \begin{pmatrix} b_1 & b_2 \\ a_1 & a_2 \end{pmatrix} = b_1 a_2 - b_2 a_1 = -(a_1 b_2 - a_2 b_1) = -\det \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}.$$

Bei Vertauschung der Zeilen ändert die Determinante also ihr Vorzeichen. Diese Eigenschaft ist bei der Berechnung der Determinanten ein oft unangenehmes Problem, aber es hat einen sehr wichtigen geometrischen Hintergrund.

Für $v, w \in \mathbb{R}^2 \setminus \{\mathbf{o}\}$ hatten wir in 0.3.3 einen unorientierten Winkel erklärt durch

$$\angle(v, w) := \arccos \frac{\langle v, w \rangle}{\|v\| \cdot \|w\|} \in [0, \pi].$$

Um einen orientierten Winkel zu erklären, können wir $\|v\| = \|w\| = 1$, also

$$v = (\cos \alpha, \sin \alpha), \quad w = (\cos \beta, \sin \beta) \quad \text{mit} \quad \alpha, \beta \in [0, 2\pi[$$

annehmen. Dann ist

$$\angle_o(v, w) := \beta - \alpha \in] - 2\pi, 2\pi[$$

der *orientierte Winkel* zwischen v und w . Er misst, wie weit man v entgegen dem Uhrzeigersinn drehen muss, bis w erreicht ist. Wie oben erhält man aus dem Additionstheorem für den Sinus

$$\sin \angle_o(v, w) = \det A, \quad \text{wobei} \quad A := \begin{pmatrix} \cos \alpha & \sin \alpha \\ \cos \beta & \sin \beta \end{pmatrix}.$$

Man kann den orientierten Winkel modulo 2π so reduzieren, dass $\angle_o(v, w) \in [0, 2\pi[$. Dann gilt zwischen orientiertem und nicht orientiertem Winkel die Beziehung

$$\angle(v, w) = \begin{cases} \angle_o(v, w) & \text{für } \angle_o(v, w) \in [0, \pi[\\ 2\pi - \angle_o(v, w) & \text{für } \angle_o(v, w) \in [\pi, 2\pi[\end{cases}$$

(v, w) ist genau dann eine Basis von \mathbb{R}^2 , wenn $\det A \neq 0$. In diesem Fall kann man das Vorzeichen von A als „Orientierung“ interpretieren. Man nennt die Basis (v, w)

- positiv orientiert** : $\Leftrightarrow \det A > 0$,
- negativ orientiert** : $\Leftrightarrow \det A < 0$.

Das ist leicht zu definieren, aber nicht ganz so einfach zu verstehen. Die einfachsten Beispiele sind

$$(e_1, e_2) \quad \text{mit} \quad \det A = \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1 > 0 \quad \text{und}$$

$$(e_2, e_1) \quad \text{mit} \quad \det A = \det \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = -1 < 0.$$

Die Bezeichnungen „positiv“ und „negativ“ sind keine Wertungen, sondern dienen nur dem Vergleich mit der Standardbasis (e_1, e_2) . Das kann man gut sehen, wenn man $v = e_1$ und $w = (\cos \beta, \sin \beta)$ beliebig wählt. Dann ist $\det A = \sin \beta$ und man kann folgende Fälle unterscheiden:

- $\beta = 0$: $\sin \beta = 0$, (e_1, w) linear abhängig,
- $\beta \in]0, \pi[$: $\sin \beta > 0$, (e_1, w) positiv orientiert,
- $\beta = \pi$: $\sin \beta = 0$, (e_1, w) linear abhängig,
- $\beta \in]\pi, 2\pi[$: $\sin \beta < 0$, (e_1, w) negativ orientiert.

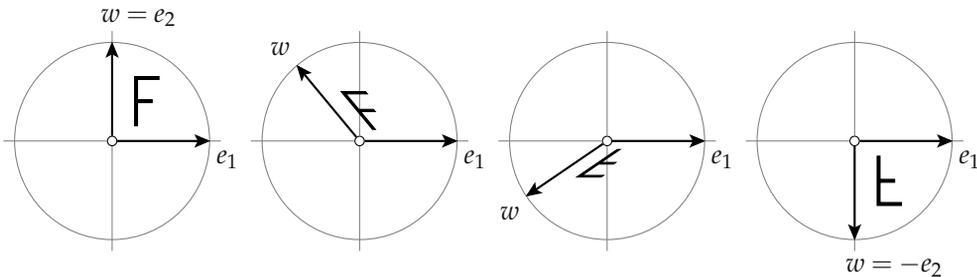
Man kann sich auch vorstellen, dass die Standardbasis (e_1, e_2) durch eine lineare Abbildung $F : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ in (v, w) abgebildet wird. Diese Abbildung wird beschrieben durch die Matrix

$${}^tA = \begin{pmatrix} \cos \alpha & \cos \beta \\ \sin \alpha & \sin \beta \end{pmatrix} \quad \text{mit} \quad \det {}^tA = \cos \alpha \sin \beta - \cos \beta \sin \alpha = \det A.$$

Dann heißt F

- orientierungstreu** : $\Leftrightarrow \det A > 0$,
- nicht orientierungstreu** : $\Leftrightarrow \det A < 0$.

Wie sich eine Figur bei einer solchen Abbildung F mit $F(e_1) = e_1$ und $F(e_2) = w$ ändert, sieht man an den folgenden Bildern.



Das Ganze kann man auch „dynamisch“ beschreiben. Jede positiv orientierte Basis (e_1, w) kann aus (e_1, e_2) erhalten werden, indem man e_2 stetig nach w dreht, dabei bleiben e_1 und der sich drehende Vektor linear unabhängig. Will man e_2 nach $-e_2$ drehen, muss der Winkel 0 oder π überschritten werden, an diesen Stellen werden die beiden Vektoren linear abhängig. Ganz allgemein kann man zwei Basen des \mathbb{R}^n „gleichorientiert“ nennen, wenn sie sich stetig ineinander überführen lassen und eine Basis heißt *positiv orientiert*, wenn sie mit der Standardbasis (e_1, \dots, e_n) gleichorientiert ist. Auch diese Eigenschaft kann durch das Vorzeichen einer Determinante kontrolliert werden (vgl. etwa [FI₁, 3.4]).

3.2 Berechnung von Determinanten

Die Geschichte der Determinanten ist lange und bewegt; eine ausführliche Schilderung findet man etwa bei [MU]. Es gibt noch immer mehrere Richtungen des Zugangs: *Einerseits* kann man sie durch *Formeln* zur Berechnung erklären und damit die grundlegenden Eigenschaften nachweisen. Dazu muss man zur Handhabung der Vorzeichenprobleme zunächst Permutationen untersuchen. *Andererseits* kann man ganz einfache grundlegende Eigenschaften als *Axiome* formulieren und daraus die wichtigsten praktischen Verfahren zur Berechnung herleiten. Um das Ganze zu rechtfertigen, müssen anschließend Existenz und Eindeutigkeit bewiesen werden. Dann kann man die Permutationen nicht mehr umgehen. Jeder dieser Wege hat Vorteile und Nachteile. Wir haben uns hier für die axiomatische Methode entschieden, die wohl ausgehend von WEIERSTRASS von der Göttinger Schule der Algebra konsequent beschrritten wurde und in den klassischen Texten von SCHREINER-SPERNER [S-S] und VAN DER WAERDEN [WA] zu finden ist.

3.2.1 Axiome für Determinanten

In diesem ganzen Abschnitt bezeichnet K einen beliebigen Körper und n eine natürliche Zahl ungleich Null. Ist

$$A = (a_{ij}) \in M(n \times n; K)$$

eine quadratische Matrix, so sei $a_i := (a_{i1}, \dots, a_{in})$ der i -te Zeilenvektor. Dann kann man zur Abkürzung

$$A = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

schreiben.

Definition Eine Abbildung

$$\det : M(n \times n; K) \rightarrow K, \quad A \mapsto \det A,$$

heißt **Determinante**, wenn sie folgende Eigenschaften hat:

D1 Die Abbildung \det ist **linear in jeder Zeile** von A . Das bedeutet:

a) Ist die Zeile a_i eine Summe, d.h. $a_i = a'_i + a''_i$, so folgt

$$\det \begin{pmatrix} \vdots \\ a_i \\ \vdots \end{pmatrix} = \det \begin{pmatrix} \vdots \\ a'_i \\ \vdots \end{pmatrix} + \det \begin{pmatrix} \vdots \\ a''_i \\ \vdots \end{pmatrix}$$

b) Ist die Zeile a_i ein Vielfaches von a'_i , d.h. $a_i = \lambda \cdot a'_i$ mit $\lambda \in K$, so folgt

$$\det \begin{pmatrix} \vdots \\ a_i \\ \vdots \end{pmatrix} = \lambda \cdot \det \begin{pmatrix} \vdots \\ a'_i \\ \vdots \end{pmatrix}.$$

An den mit Punkten angedeuteten Positionen stehen dabei in allen der auftretenden Matrizen unverändert die Zeilenvektoren $a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n$.

D2 Die Abbildung \det ist **alternierend**, d.h. falls A zwei gleiche Zeilen hat, so folgt

$$\det A = 0.$$

D3 Die Abbildung \det ist **normiert**, d.h. $\det E_n = 1$.

Der Name „alternierend“ für die Eigenschaft D2 ist wenig plausibel, er passt eher für

D2' Entsteht A' aus A durch Vertauschung von zwei verschiedenen Zeilen, so ist

$$\det A' = -\det A.$$

Die beiden Bedingungen D2 und D2' sind fast, aber nicht ganz, äquivalent:

Bemerkung Unter der Voraussetzung D1a) gilt stets $D2 \Rightarrow D2'$ und im Fall $\text{char}(K) \neq 2$ auch $D2' \Rightarrow D2$.

Beweis $D2 \Rightarrow D2'$: Sei $A = \begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix}$ und $A' = \begin{pmatrix} \vdots \\ a_j \\ \vdots \\ a_i \\ \vdots \end{pmatrix}$, wobei $j \neq i$, kürzer $A = \begin{pmatrix} a_i \\ a_j \end{pmatrix}$ und

$A' = \begin{pmatrix} a_j \\ a_i \end{pmatrix}$. Da die Zeilen außer i und j unbeteiligt sind, ist die kürzere Schreibweise ausreichend. Dann folgt durch Addition von nach D2 verschwindenden Determinanten und D1a)

$$\begin{aligned} \det A + \det A' &= \det \begin{pmatrix} a_i \\ a_j \end{pmatrix} + \det \begin{pmatrix} a_i \\ a_i \end{pmatrix} + \det \begin{pmatrix} a_j \\ a_i \end{pmatrix} + \det \begin{pmatrix} a_j \\ a_j \end{pmatrix} \\ &= \det \begin{pmatrix} a_i \\ a_j + a_i \end{pmatrix} + \det \begin{pmatrix} a_j \\ a_i + a_j \end{pmatrix} = \det \begin{pmatrix} a_i + a_j \\ a_i + a_j \end{pmatrix} = 0. \end{aligned}$$

$D2' \Rightarrow D2$: Hat A zwei gleiche Zeilen, so ist die Vertauschung ohne Wirkung, also ist $\det A' = \det A$. Nach $D2'$ folgt aber

$$\det A' + \det A = 0, \quad \text{also} \quad \det A + \det A = (1 + 1) \cdot \det A = 0.$$

Wegen $1 + 1 \neq 0$ in K muss $\det A = 0$ sein. ■

Die aufgestellten Axiome sind ganz plausibel, aber Existenz und Eindeutigkeit der Determinante für beliebiges n ist gar nicht offensichtlich. Für sehr kleine n ist der Beweis ganz elementar, das wollen wir ausführen.

Der Fall $n = 1$ ist ganz offensichtlich. Hier ist $A = (a) = a \cdot (1)$; aus D1b) und D3 folgt, dass $\det A = a$ sein muss. Das zeigt die Eindeutigkeit. Definiert man $\det A := a$, so sind die Axiome erfüllt.

Im Fall $n = 2$ zeigen wir zunächst die Eindeutigkeit. Ist

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \text{so gilt} \quad A = \begin{pmatrix} ae_1 + be_2 \\ ce_1 + de_2 \end{pmatrix},$$

wobei in der zweiten Darstellung die Zeilenvektoren als Linearkombination der kanonischen Basis von K^2 eingetragen sind. Nach D1 gilt

$$\begin{aligned} \det A &= a \cdot \det \begin{pmatrix} e_1 \\ ce_1 + de_2 \end{pmatrix} + b \cdot \det \begin{pmatrix} e_2 \\ ce_1 + de_2 \end{pmatrix} \\ &= a \cdot c \cdot \det \begin{pmatrix} e_1 \\ e_1 \end{pmatrix} + a \cdot d \cdot \det \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} + b \cdot c \cdot \det \begin{pmatrix} e_2 \\ e_1 \end{pmatrix} + b \cdot d \cdot \det \begin{pmatrix} e_2 \\ e_2 \end{pmatrix}. \end{aligned}$$

Nach D2 ist $\det \begin{pmatrix} e_1 \\ e_1 \end{pmatrix} = \det \begin{pmatrix} e_2 \\ e_2 \end{pmatrix} = 0$, nach D3 ist $\det \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = 1$ und nach $D2'$ ist

$\det \begin{pmatrix} e_2 \\ e_1 \end{pmatrix} = -1$. Also folgt

$$\det A = ad - bc. \tag{*}$$

Damit ist gezeigt: Wenn es im Fall $n = 2$ eine Determinante im Sinn der Axiome gibt, dann muss sie von der Form (*) sein. Nun könnten aber aus beliebig aufgeschriebenen Axiomen unsinnige Folgerungen entstehen. Also ist noch die *Existenz* zu zeigen. Dazu definieren wir entsprechend (*)

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} := ad - bc,$$

und es sind die Axiome D1 bis D3 nachzuweisen.

D1:

$$\begin{aligned} \det \begin{pmatrix} a' + a'' & b' + b'' \\ c & d \end{pmatrix} &= (a' + a'')d - (b' + b'')c = a'd - b'c + a''d - b''c \\ &= \det \begin{pmatrix} a' & b' \\ c & d \end{pmatrix} + \det \begin{pmatrix} a'' & b'' \\ c & d \end{pmatrix}, \\ \det \begin{pmatrix} \lambda a & \lambda b \\ c & d \end{pmatrix} &= \lambda ad - \lambda bc = \lambda(ad - bc) = \lambda \cdot \det \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \end{aligned}$$

und analog für die zweite Zeile.

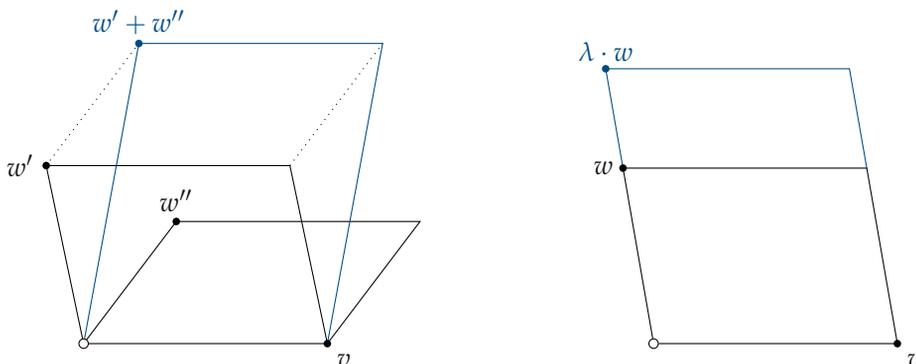
$$\text{D2: } \det \begin{pmatrix} a & b \\ a & b \end{pmatrix} = ab - ba = 0 \quad \text{D3: } \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1 - 0 = 1.$$

■

Im Fall $n = 2$ und $K = \mathbb{R}$ kann man die Axiome für die Determinante auch einfach geometrisch interpretieren. Bezeichnen wir die Zeilenvektoren von A mit v, w , so haben wir in 3.1.2 gesehen, dass der Betrag von $\det A$ gleich der Fläche des von v und w aufgespannten Parallelogramms ist.

D1a) Die Fläche des Parallelogramms aus v und $w' + w''$ ist gleich der Summe der Flächen der Parallelogramme aus v und w' , sowie v und w'' .

D1b) Die Fläche des Parallelogramms aus v und λw ist das $|\lambda|$ -fache der Fläche des Parallelogramms aus v und w .



D2 bedeutet, dass ein aus v und $w = v$ gebildetes „plattes Parallelogramm“ die Fläche 0 hat und D3 bedeutet, dass ein aus $v = e_1$ und $w = e_2$ gebildetes Quadrat die Fläche 1 hat.

3.2.2 Weitere Eigenschaften der Determinante

Wir werden nun zeigen, dass sich aus den Axiomen ein sehr bequemes Verfahren zur Berechnung von Determinanten ableiten lässt. Entscheidend dabei ist die Wirkung von

Zeilenumformungen der Matrix auf den Wert der Determinante. Die Multiplikation einer Zeile mit einem Faktor $\lambda \in K$ (das ist eine Umformung vom Typ (3)) multipliziert nach D1b) die Determinante mit λ . Nach Eigenschaft D2' ändern Zeilenvertauschungen (d.h. Umformungen vom Typ (1)) das Vorzeichen. Nun zu Typ (2)

D4 Sei $\lambda \in K$ und $i \neq j$. Entsteht A' aus A durch Addition der λ -fachen Zeile j zur Zeile i , so ist

$$\det A' = \det A.$$

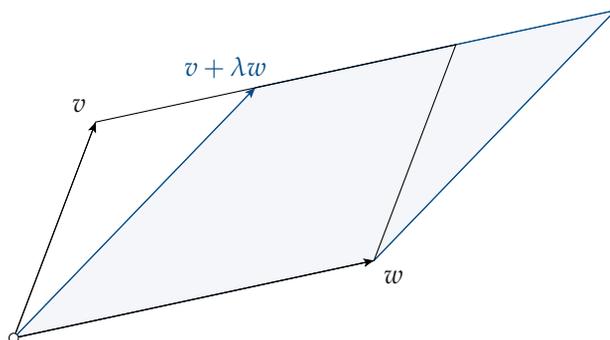
Die Determinante bleibt also bei Zeilenumformungen von Typ (2) unverändert.

Beweis Durch die Anwendung von D1 und D2 erhält man

$$\det A' = \det \begin{pmatrix} a_i + \lambda a_j \\ a_j \end{pmatrix} = \det \begin{pmatrix} a_i \\ a_j \end{pmatrix} + \lambda \cdot \det \begin{pmatrix} a_j \\ a_j \end{pmatrix} = \det \begin{pmatrix} a_i \\ a_j \end{pmatrix} = \det A.$$

■

Im Fall $n = 2$ und $K = \mathbb{R}$ bedeutet das geometrisch, dass sich die Fläche eines Parallelogramms bei einer *Scherung* nicht ändert.



D5 Ist eine Zeile von A gleich Null, so folgt $\det A = 0$.

Das folgt sofort aus D1b).

■

Eine Matrix $A = (a_{ij}) \in M(n \times n; K)$ heißt

obere Dreiecksmatrix, wenn $a_{ij} = 0$ für $i > j$,
untere Dreiecksmatrix, wenn $a_{ij} = 0$ für $i < j$,
Diagonalmatrix, wenn $a_{ij} = 0$ für $i \neq j$.

D6 Ist $A = (a_{ij})$ eine untere oder obere Dreiecksmatrix, so ist

$$\det A = a_{11} \cdot \dots \cdot a_{nn}.$$

Beweis Eine obere Dreiecksmatrix ist von der Form

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ & \ddots & \vdots \\ 0 & & a_{nn} \end{pmatrix}.$$

Sind alle Diagonalelemente $a_{11}, \dots, a_{nn} \neq 0$, so kann man A von unten beginnend durch wiederholte Zeilenumformungen vom Typ (2) zur Diagonalmatrix

$$A' = \begin{pmatrix} a_{11} & & 0 \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix}$$

machen; nach D4 gilt $\det A' = \det A$. Durch wiederholte Anwendung von D1b) und schließlich mit D3 folgt

$$\det A' = a_{11} \cdot \dots \cdot a_{nn} \cdot \det E_n = a_{11} \cdot \dots \cdot a_{nn}.$$

Ist mindestens ein $a_{ii} = 0$, so folgt $\det A = 0$. Das kann man so einsehen: Man wähle das größte i mit $a_{ii} = 0$. Ist $i = n$, so ist die letzte Zeile gleich Null und $\det A = 0$ folgt aus D5. Andernfalls betrachte man den unteren Teil der Matrix ab der Zeile i :

$$\begin{array}{cccc} 0 & a_{i,i+1} & \dots & a_{in} \\ & a_{i+1,i+1} & & \vdots \\ & & \ddots & \\ & & & a_{nn} \end{array}$$

Mit Hilfe der von Null verschiedenen Einträge $a_{nn}, \dots, a_{i+1,i+1}$ kann man durch Zeilenumformungen vom Typ (2) die Zeile i von A schrittweise zu Null machen. Nach D4 und D5 folgt $\det A = 0$.

Ganz analog kann man den Fall einer unteren Dreiecksmatrix behandeln. ■

Mit Hilfe von D6 kann man nun ein einfaches Verfahren angeben, Determinanten zu berechnen. Die theoretische Rechtfertigung wird in 3.2.5 vervollständigt.

Rechenverfahren Man bringe A durch Zeilenumformungen von Typ (1) und (2) auf Zeilenstufenform; das Ergebnis ist eine obere Dreiecksmatrix $B = (b_{ij})$. Ist s die Anzahl der verwendeten Zeilenumformungen, so gilt

$$\det A = (-1)^s \cdot \det B = (-1)^s \cdot b_{11} \cdot \dots \cdot b_{nn}.$$

Beispiel 1

$$\det \begin{pmatrix} 0 & 3 & 1 \\ 2 & 1 & 4 \\ 1 & -1 & 0 \end{pmatrix} = -\det \begin{pmatrix} 1 & -1 & 0 \\ 2 & 1 & 4 \\ 0 & 3 & 1 \end{pmatrix} = -\det \begin{pmatrix} 1 & -1 & 0 \\ 0 & 3 & 4 \\ 0 & 3 & 1 \end{pmatrix} = -\det \begin{pmatrix} 1 & -1 & 0 \\ 0 & 3 & 4 \\ 0 & 0 & -3 \end{pmatrix} \\ = -1 \cdot 3 \cdot (-3) = 9.$$

Leider gibt es auch Matrizen, die bei solchen Umformungen sehr heftig auf Rundungen reagieren:

Beispiel 2 Ist A die HILBERT-Matrix aus 0.5.5, also

$$A = \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{3} \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} \\ \frac{1}{3} & \frac{1}{4} & \frac{1}{5} \end{pmatrix},$$

so folgt aus den in 0.5.5 durchgeführten rationalen Umformungen, dass

$$\det A = \det \tilde{A} = \frac{1}{12 \cdot 180} = \frac{1}{2160} \approx 0.46 \cdot 10^{-3}.$$

Rundet man $\frac{1}{3} \approx 0.33$, und rechnet man weiter mit Rundung auf 2 Stellen, so erhält man wie in 0.5.5.

$$\det A' \approx \det \tilde{A}' = 0.08 \cdot 0.01 = 0.8 \cdot 10^{-3}.$$

Rationale Umformungen von

$$A'' = \begin{pmatrix} 1 & \frac{1}{2} & \frac{33}{100} \\ \frac{1}{2} & \frac{33}{100} & \frac{1}{4} \\ \frac{33}{100} & \frac{1}{4} & \frac{1}{5} \end{pmatrix} \quad \text{ergeben} \quad \tilde{A}'' = \begin{pmatrix} 1 & \frac{1}{2} & \frac{33}{100} \\ 0 & \frac{2}{25} & \frac{17}{200} \\ 0 & 0 & \frac{63}{80000} \end{pmatrix}.$$

Daraus erhält man den exakten Wert:

$$\det A' = \det A'' = 0.63 \cdot 10^{-4}.$$

Aus dem angegebenen Rechenverfahren erhält man die Eigenschaft

D7 Für $A \in M(n \times n; K)$ gilt $\text{rang } A = n \Leftrightarrow \det A \neq 0$.

Beweis Hat man A auf Zeilenstufenform $B = (b_{ij})$ gebracht, so ist $\text{rang } A = n$ gleichwertig damit, dass die Diagonalelemente b_{11}, \dots, b_{nn} alle von Null verschieden sind. Da

$$\det A = \pm \det B = \pm b_{11} \cdot \dots \cdot b_{nn},$$

folgt die Behauptung. ■

In späteren Anwendungen benötigen wir noch eine Regel für *Blockmatrizen*:

D8 Sei $n \geq 2$ und $A \in M(n \times n; K)$ von der Gestalt

$$A = \begin{pmatrix} A_1 & C \\ 0 & A_2 \end{pmatrix},$$

wobei A_1 und A_2 quadratisch sind. Dann gilt

$$\det A = (\det A_1) \cdot (\det A_2).$$

Beweis Durch Zeilenumformungen an A vom Typ (1) und (2) mache man A_1 zu einer oberen Dreiecksmatrix B_1 . Dabei bleibt A_2 unverändert, aus C wird C' . Ist k die Anzahl der dabei ausgeführten Zeilenvertauschungen, so folgt

$$\det A_1 = (-1)^k \cdot \det B_1.$$

In der nächsten Etappe mache man analog A_2 zu einer oberen Dreiecksmatrix B_2 ; dabei werden B_1 und C' nicht verändert. Ist l die Zahl der dabei ausgeführten Zeilenvertauschungen, so folgt

$$\det A_2 = (-1)^l \cdot \det B_2.$$

Insgesamt erhalten wir als Ergebnis der Umformungen die Dreiecksmatrix

$$B = \begin{pmatrix} B_1 & C' \\ 0 & B_2 \end{pmatrix},$$

nach D6 ist $\det B = (\det B_1) \cdot (\det B_2)$. Da

$$\det A = (-1)^{k+l} \cdot \det B$$

folgt die Behauptung. ■

Man kann quadratische Matrizen addieren und multiplizieren. Dabei entsteht die Frage, ob die Determinante mit diesen Operationen verträglich ist. Zunächst betrachten wir die Multiplikation einer Matrix mit einem Faktor $\lambda \in K$.

D9 Für $A \in M(n \times n; K)$ und $\lambda \in K$ gilt $\det(\lambda \cdot A) = \lambda^n \cdot \det A$.

Beweis In $\lambda \cdot A$ ist jede Zeile mit λ multipliziert, also folgt die Behauptung durch n -fache Anwendung von D1b). ■

Vorsicht! Die quadratischen Matrizen bilden einen Vektorraum; an D9 sieht man, dass die Abbildung

$$\det : M(n \times n; K) \rightarrow K$$

für $n \geq 2$ i. Allg. nicht linear ist. Etwa im Fall $K = \mathbb{F}_2$ ist jedoch stets $\det(\lambda \cdot A) = \lambda \cdot \det A$.

Analog ist es mit der Addition:

D10 Im allgemeinen ist $\det(A + B) \neq \det A + \det B$.

Einfachstes Gegenbeispiel ist $n = 2$, $A = E_2$ und $B = -E_2$ im Fall $\text{char}(K) \neq 2$.

Umso erfreulicher ist die nicht-triviale Eigenschaft

D11 Determinanten-Multiplikations-Satz Für $A, B \in M(n \times n; K)$ gilt

$$\det(A \cdot B) = \det A \cdot \det B.$$

Insbesondere ist $\det(B \cdot A) = \det(A \cdot B)$ und $\det(A^{-1}) = (\det A)^{-1}$, falls $A \in \text{GL}(n; K)$.

Beweis Der Leser möge diesen Satz erst einmal im Fall $n = 2$ für

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

durch direkte Rechnung beweisen. Dabei wird deutlich, dass es geschickter ist, etwas Theorie zu investieren.

Zunächst eine Vorbemerkung: Die Matrizen A, B ergeben lineare Abbildungen F_A, F_B und $F_A \circ F_B = F_{A \cdot B}$, d.h. man hat ein kommutatives Diagramm

$$\begin{array}{ccc} K^n & \xrightarrow{F_{A \cdot B}} & K^n \\ & \searrow F_B & \nearrow F_A \\ & & K^n \end{array}$$

Wie man in der Integrationstheorie lernt, gibt $|\det A|$ im Fall $K = \mathbb{R}$ die Volumenverzerrung bei der Abbildung F_A an. Daher ist die Produktformel für die Beträge der Determinanten plausibel. Die Vorzeichen der Determinante hängen mit der Orientierung zusammen (vgl. 3.1.2).

Aus obigem Diagramm folgt $F_{A \cdot B}(K^n) \subset F_A(K^n)$, also

$$\text{rang}(A \cdot B) = \dim F_{A \cdot B}(K^n) \leq \dim F_A(K^n) = \text{rang } A.$$

Ist $\text{rang } A < n$, so folgt $\text{rang}(A \cdot B) < n$, also gilt $\det A = 0$ und $\det(A \cdot B) = 0$ nach D7.

Ist $\text{rang } A = n$, so folgt $A \in \text{GL}(n; K)$. Nach 2.4.6 gibt es Elementarmatrizen C_1, \dots, C_k so, dass

$$A = C_1 \cdot \dots \cdot C_k. \quad (*)$$

Hilfssatz Ist $S \in M(n \times n; K)$ beliebig und $C \in GL(n; K)$ eine Elementarmatrix, so gilt

$$\det(C \cdot S) = (\det C) \cdot (\det S).$$

Beweis des Hilfssatzes Wir unterscheiden entsprechend 2.4.6 drei Typen von Elementarmatrizen.

(1) Ist $C = P(i, j)$ mit $i \neq j$, so ist $\det C = -1$ nach D3 und D2'. Da C Zeilen in S vertauscht, ist

$$\det(C \cdot S) = -\det S = (\det C) \cdot (\det S).$$

(2) Ist $C = Q_\lambda(i, j)$ mit $i \neq j$, so ist $\det C = 1$ nach D6. Nach D4 folgt

$$\det(C \cdot S) = \det S = (\det C) \cdot (\det S).$$

(3) Ist $C = S_\lambda(i)$, so ist $\det C = \lambda$ nach D1 und D3. Daraus folgt

$$\det(C \cdot S) = \lambda \cdot \det S = (\det C) \cdot (\det S).$$

Damit ist der Hilfssatz bewiesen, und es ist gezeigt, dass die Produktformel gilt, wenn die links stehende Matrix elementar ist. Also folgt aus (*)

$$\begin{aligned} \det A &= \det(C_1 \cdot (C_2 \cdot \dots \cdot C_k)) = \det C_1 \cdot \det(C_2 \cdot \dots \cdot C_k) \\ &= \dots = \det C_1 \cdot \dots \cdot \det C_k \end{aligned}$$

und weiter

$$\begin{aligned} \det(A \cdot B) &= \det(C_1 \cdot (C_2 \cdot \dots \cdot C_k \cdot B)) = \det C_1 \cdot \det(C_2 \cdot \dots \cdot C_k \cdot B) \\ &= \det C_1 \cdot \dots \cdot \det C_k \cdot \det B = \det A \cdot \det B. \end{aligned}$$

■

Bei der Definition der Determinante hatten wir die Zeilen der Matrix in den Vordergrund gestellt. Dass die Spalten gleichberechtigt sind, folgt aus

D12 Für jedes $A \in M(n \times n; K)$ gilt

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

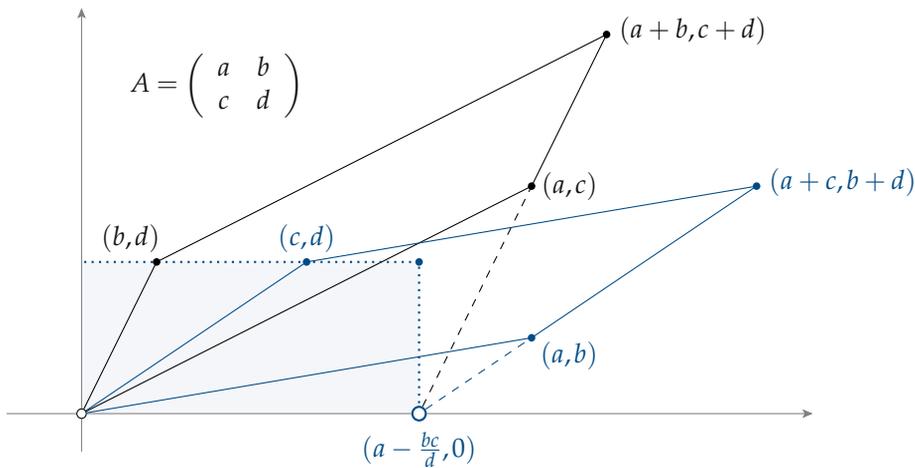
Daraus folgt sofort das

Korollar Alle in 3.2.1 für Zeilen formulierten Regeln gelten analog für Spalten in einer quadratischen Matrix. ■

Beweis Zum Beweis von D12 zunächst ein paar Vorbemerkungen. Der Fall $n = 1$ ist klar; für $n = 2$ ist

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad \text{und} \quad {}^tA = \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix},$$

also $\det A = a_{11}a_{22} - a_{12}a_{21}$ und $\det {}^tA = a_{11}a_{22} - a_{21}a_{12}$. In 3.1.2 hatten wir gesehen, dass $|\det A|$ die Fläche des von den Zeilenvektoren aufgespannten Parallelogramms angibt. Wegen $\det A = \det {}^tA$ hat das von den Spaltenvektoren aufgespannte Parallelogramm die gleiche Fläche. Wie das folgende Bild zeigt, ist das geometrisch nicht ganz offensichtlich, man beachte dabei die möglichen Scherungen.



Für allgemeines n betrachten wir zunächst den Fall $\text{rang } A < n$. Dann ist $\det A = 0$ nach D7 und da nach 2.2.6 Spaltenrang gleich Zeilenrang ist, folgt auch $\det {}^tA = 0$. Im Fall $\text{rang } A = n$ gibt es nach 2.4.6 Elementarmatrizen C_1, \dots, C_k derart, dass

$$A = C_1 \cdot \dots \cdot C_k.$$

Für Elementarmatrizen ist D12 klar:

Ist $C = P(i, j)$, so folgt ${}^tC = C$.

Ist $C = Q_\lambda(i, j)$, so folgt $\det C = 1 = \det {}^tC$ nach D6.

Ist $C = S_\lambda(i)$, so folgt ${}^tC = C$.

Mit Hilfe von D11 erhält man daraus

$$\begin{aligned} \det {}^tA &= \det {}^t(C_1 \cdot \dots \cdot C_k) = (\det {}^tC_k) \cdot \dots \cdot (\det {}^tC_1) \\ &= (\det C_k) \cdot \dots \cdot (\det C_1) = (\det C_1) \cdot \dots \cdot (\det C_k) = \det A. \end{aligned}$$

■

Wer noch immer nicht vom Nutzen der Elementarmatrizen überzeugt ist, möge die Regeln D11 und D12 für $n = 3$ mit Hilfe der Regel von SARRUS aus 3.2.5 nachrechnen!

3.2.3 Permutationen

Zum Beweis von Existenz und Eindeutigkeit der Determinante benötigen wir eine subtile technische Vorbereitung. Nach Axiom D3 ist $\det E_n = 1$. Entsteht A aus E_n durch wiederholte Vertauschungen von Zeilen, so muss nach D2' gelten, dass

$$\det A = (-1)^k,$$

wenn k die Anzahl der hintereinander durchgeführten Vertauschungen ergibt. Ist nur das Ergebnis der Vertauschungen bekannt, etwa für $n = 3$

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

so kann A auf mehrere verschiedene Arten aus E_3 durch Zeilenvertauschungen entstanden sein, und die Zahl k ist nicht eindeutig bestimmt. Um diese Situation aufzuklären identifiziert man die Zeilenvektoren von A mit den kanonischen Basisvektoren, also

$$A = \begin{pmatrix} e_3 \\ e_1 \\ e_2 \end{pmatrix}.$$

Diese Matrix kann aus E_3 durch Zeilenvertauschungen entstanden sein, etwa

$$E_3 = \begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix} \mapsto \begin{pmatrix} e_1 \\ e_3 \\ e_2 \end{pmatrix} \mapsto \begin{pmatrix} e_3 \\ e_1 \\ e_2 \end{pmatrix} = A, \quad \text{oder}$$

$$E_3 = \begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix} \mapsto \begin{pmatrix} e_2 \\ e_1 \\ e_3 \end{pmatrix} \mapsto \begin{pmatrix} e_3 \\ e_1 \\ e_2 \end{pmatrix} = A.$$

Also folgt $\det A = (-1)^2 \cdot \det E_3 = 1$.

Die Zeilen von A sind im Ergebnis entstanden aus den Zeilen von E_3 durch die bijektive Abbildung oder **Permutation**

$$\sigma: \{1,2,3\} \rightarrow \{1,2,3\} \quad \text{mit} \quad \sigma(1) = 3, \quad \sigma(2) = 1, \quad \sigma(3) = 2.$$

Allgemein kann man eine Permutation

$$\{1, \dots, n\} \rightarrow \{1, \dots, n\}$$

ganz explizit beschreiben in Form einer „Wertetabelle“

$$\sigma = \begin{bmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{bmatrix}.$$

Nun können wir das **Problem** formulieren, das in diesem Abschnitt zu lösen ist:

Bezeichnet e_1, \dots, e_n die kanonische Basis des K^n und ist σ eine Permutation, so ist zu klären, ob als Konsequenz aus den Axiomen für die Determinante

$$\det \begin{pmatrix} e_{\sigma(1)} \\ \vdots \\ e_{\sigma(n)} \end{pmatrix} = +1 \quad \text{oder} \quad -1$$

sein muss.

Man beachte dabei, dass Existenz und Eindeutigkeit der Determinante noch nicht bewiesen sind! Sonst könnte man den Wert der Determinante schon angeben.

Wir wollen nun jeder Permutation σ als **Signum** (oder Vorzeichen) eine Zahl $+1$ oder -1 zuordnen, die ein Kandidat für den Wert der problematischen Determinante ist. Dazu betrachten wir alle Paare von Zahlen $i, j \in \{1, \dots, n\}$. Ein **Fehlstand** liegt vor, wenn

$$i < j \quad \text{aber} \quad \sigma(i) > \sigma(j).$$

So hat etwa $\sigma = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$ zwei Fehlstände:

$$1 < 2 \quad \text{aber} \quad 3 > 1, \quad \text{und} \quad 1 < 3 \quad \text{aber} \quad 3 > 2.$$

Es gibt insgesamt $\frac{n(n-1)}{2}$ Paare $i < j$, also gilt für die Zahl $r(\sigma)$ der Fehlstände von σ

$$0 \leq r(\sigma) \leq \frac{n(n-1)}{2}.$$

Nun ist das **Signum** von σ erklärt durch

$$\text{sign } \sigma := (-1)^{r(\sigma)},$$

d.h. das Signum ist $+1$, wenn die Anzahl der Fehlstände gerade ist, und -1 , wenn sie ungerade ist. Das für die Theorie der Determinanten entscheidende Ergebnis ist nun der

Satz Aus den in 3.2.1 formulierten Axiomen D1, D2 und D3 für die Determinante folgt, dass für jede Permutation σ von $\{1, \dots, n\}$

$$\det \begin{pmatrix} e_{\sigma(1)} \\ \vdots \\ e_{\sigma(n)} \end{pmatrix} = \text{sign } \sigma$$

gelten muss.

Es gibt viele Möglichkeiten das zu beweisen; wir wählen hier einen etwas abstrakten Weg, der eine tiefere Einsicht in die Eigenschaften von Permutationen vermittelt. Wer das zunächst überspringen möchte, kann gleich in 3.2.5 weiter lesen.

Schon in 1.2.3 hatten wir bemerkt, dass die Menge S_n der bijektiven Abbildungen von $\{1, \dots, n\}$ auf sich mit der Hintereinanderschaltung der Abbildungen als Verknüpfung eine Gruppe ist. Diese *symmetrische Gruppe* S_n hat $n!$ Elemente. Die beiden Gruppen

$$S_1 = \{\text{id}\} \quad \text{und} \quad S_2 = \{\text{id}, \sigma\} \quad \text{mit} \quad \sigma = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$$

sind abelsch.

Bemerkung Die Gruppe S_n ist für $n \geq 3$ nicht abelsch.

Beweis Es genügt, ein Beispiel anzugeben. Ist

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{bmatrix} \quad \text{und} \quad \tau = \begin{bmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 1 & 3 & 2 & 4 & \dots & n \end{bmatrix}$$

so folgt

$$\sigma \circ \tau = \begin{bmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{bmatrix} \quad \text{aber} \quad \tau \circ \sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 1 & 2 & 4 & \dots & n \end{bmatrix} \neq \sigma \circ \tau.$$

Man beachte dabei, dass bei der Multiplikation von Permutationen – wie für Abbildungen üblich – erst die rechts stehende Permutation angewandt wird, also

$$(\tau \circ \sigma)(i) = \tau(\sigma(i)).$$

■

Neben der Gruppe S_n betrachten wir auch die Gruppe $Z_2 := \{+1, -1\}$ mit der Multiplikation als Verknüpfung. Die weitere Behandlung der Permutationen wird viel klarer durch das grundlegende

Lemma 1 Die Abbildung $\text{sign} : S_n \rightarrow Z_2$ ist ein Homomorphismus von Gruppen, d.h.

$$\text{sign}(\tau \circ \sigma) = (\text{sign} \tau) \cdot (\text{sign} \sigma) \quad \text{für} \quad \sigma, \tau \in S_n.$$

Insbesondere ist $\text{sign}(\sigma^{-1}) = \text{sign} \sigma$ für alle $\sigma \in S_n$.

Beweis Damit sich der Beweis formal schöner aufschreiben lässt, ist es von Vorteil die Definition des Signums in eine Formel zu verpacken. Nehmen wir das Beispiel

$$\begin{aligned} \text{sign } \sigma &= \text{sign} \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \stackrel{(1)}{=} \frac{\sigma(2) - \sigma(1)}{|\sigma(2) - \sigma(1)|} \cdot \frac{\sigma(3) - \sigma(1)}{|\sigma(3) - \sigma(1)|} \cdot \frac{\sigma(3) - \sigma(2)}{|\sigma(3) - \sigma(2)|} \\ &\stackrel{(2)}{=} \frac{1-3}{3-1} \cdot \frac{2-3}{3-2} \cdot \frac{2-1}{2-1} \\ &\stackrel{(3)}{=} \frac{\sigma(2) - \sigma(1)}{2-1} \cdot \frac{\sigma(3) - \sigma(1)}{3-1} \cdot \frac{\sigma(3) - \sigma(2)}{3-2} \end{aligned}$$

Bei Gleichung (1) werden die Fehlstände gezählt, bei (2) werden die Werte eingesetzt; es folgt

$$\text{sign } \sigma = (-1) \cdot (-1) \cdot 1 = 1.$$

Bei Gleichung (3) wird die Reihenfolge der Nenner den Zählern angepasst.

Für ein beliebiges $\sigma \in \mathcal{S}_n$ folgt mit den gleichen Argumenten

$$\text{sign } \sigma = \prod_{i < j} \frac{\sigma(j) - \sigma(i)}{j - i}, \quad (*)$$

wobei das Produkt insgesamt $\frac{n(n-1)}{2}$ Faktoren hat. Man beachte jedoch, dass – wie im obigen Beispiel – die einzelnen Faktoren rationale Zahlen sind. Nur das Produkt ist gleich ± 1 .

Sind nun $\sigma, \tau \in \mathcal{S}_n$, so folgt durch Anwendung der Formel (*)

$$\text{sign}(\tau \circ \sigma) = \prod_{i < j} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{j - i} = \prod_{i < j} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{\sigma(j) - \sigma(i)} \cdot \prod_{i < j} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Das zweite Produkt ist gleich $\text{sign } \sigma$; also bleibt zu zeigen, dass das erste Produkt gleich $\text{sign } \tau$ ist, also dass

$$\prod_{i < j} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{\sigma(j) - \sigma(i)} = \prod_{k < l} \frac{\tau(l) - \tau(k)}{l - k}.$$

Beide Produkte bestehen aus $\binom{n}{2}$ Faktoren. Für einen Faktor von links sind zwei Fälle möglich:

Ist $\sigma(i) < \sigma(j)$, so steht er in der gleichen Form mit $k = \sigma(i)$ und $l = \sigma(j)$ auch rechts.

Ist $\sigma(i) > \sigma(j)$, so setzt man $k := \sigma(j)$ und $l := \sigma(i)$. Dann ist

$$\frac{\tau(\sigma(j)) - \tau(\sigma(i))}{\sigma(j) - \sigma(i)} = \frac{\tau(k) - \tau(l)}{k - l} = \frac{\tau(l) - \tau(k)}{l - k},$$

also steht der Faktor im Ergebnis auch rechts. ■

Zum Beweis des obigen Satzes benötigen wir eine weitere Vorbereitung. Eine Permutation $\tau \in S_n$ heißt **Transposition**, wenn sie zwei verschiedene Zahlen vertauscht und alle anderen festlässt. Genauer gesagt, wenn es $i, j \in \{1, \dots, n\}$ gibt mit $i \neq j$ und

$$\tau(k) = \begin{cases} j & \text{für } k = i \\ i & \text{für } k = j \\ k & \text{sonst} \end{cases}$$

Zur Abkürzung schreibt man dafür $\tau = [i, j]$. Dabei ist selbstverständlich $n \geq 2$ vorausgesetzt.

Lemma 2 Sei $n \geq 2$.

- a) Für jede Transposition $\tau \in S_n$ gilt $\tau^{-1} = \tau$ und $\text{sign } \tau = -1$.
 b) Zu jeder Permutation $\sigma \in S_n$ gibt es Transpositionen τ_1, \dots, τ_r so dass

$$\sigma = \tau_1 \circ \dots \circ \tau_r.$$

Wie wir schon an einem Beispiel gesehen hatten, ist die Darstellung als Produkt von Transpositionen keinesfalls eindeutig. Sind

$$\sigma = \tau_1 \circ \dots \circ \tau_r = \tau'_1 \circ \dots \circ \tau'_s$$

zwei solche Darstellungen, so folgt jedoch aus Lemma 1, dass

$$\text{sign } \sigma = (-1)^r = (-1)^s.$$

Die Zahlen r und s müssen also die gleiche **Parität** haben, d.h. $r \equiv s \pmod{2}$.

Beweis von Lemma 2 Ad a) Die Eigenschaft $\tau^{-1} = \tau$ ist offensichtlich. Da die Fehlstände in einer beliebigen Transposition etwas mühsam zu zählen sind, betrachten wir zunächst

$$\tau_0 := [1, 2] = \begin{bmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 1 & 3 & \dots & n \end{bmatrix}.$$

Offensichtlich hat τ_0 nur einen Fehlstand, also folgt $\text{sign } \tau_0 = -1$. Ist $\tau = [i, j]$, so verwenden wir ein $\sigma \in S_n$ mit $\sigma(1) = i$ und $\sigma(2) = j$. Dann ist

$$\tau = \sigma \circ \tau_0 \circ \sigma^{-1}, \quad \text{und es folgt} \quad \text{sign } \sigma \cdot \text{sign } \tau_0 \cdot \text{sign } \sigma = -1$$

nach Lemma 1. Im Fall $\{i, j\} = \{1, 2\}$ ist $\tau = \tau_0$. Ist $i = 1$ und $j > 2$, so folgt

$$[1, j] = [2, j] \circ [1, 2] \circ [2, j].$$

Im allgemeinen Fall $i, j > 2$ folgt

$$[i, j] = [1, i] \circ [2, j] \circ [1, 2] \circ [2, j] \circ [1, i].$$

Ad b) Wir beginnen mit dem Beispiel

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{bmatrix} \in \mathcal{S}_4.$$

Es ist $\sigma(1) = 3 \neq 1$, daher setzen wir $\tau_1 := [1, 3]$. Dann ist

$$\tau_1 \circ \sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{bmatrix}.$$

Der nächste Schritt ist $\tau_2 = [3, 4]$, es folgt

$$\tau_2 \circ \tau_1 \circ \sigma = \text{id}, \quad \text{also} \quad \sigma = \tau_1 \circ \tau_2.$$

Im allgemeinen Fall von $\sigma \in \mathcal{S}_n$ mit $n \geq 2$ kann man im Fall $\sigma = \text{id}$ die Darstellung $\sigma = [1, 2] \circ [1, 2]$ wählen. Ist $\sigma \neq \text{id}$, so gibt es ein kleinstes $i_1 \in \{1, \dots, n\}$ mit

$$\sigma(i_1) \neq i_1, \quad \text{also} \quad \sigma(i_1) > i_1 \quad \text{und man setzt} \quad \tau_1 := [i_1, \sigma(i_1)].$$

Dann ist $(\tau_1 \circ \sigma)(i) = i$ für $i \leq i_1$, im zweiten Schritt wird $i_2 \in \{1, \dots, n\}$ minimal gewählt mit

$$(\tau_1 \circ \sigma)(i_2) \neq i_2, \quad \text{also} \quad (\tau_1 \circ \sigma)(i_2) > i_2 \quad \text{und} \quad \tau_2 := [i_2, (\tau_1 \circ \sigma)(i_2)]$$

gesetzt. Dieses Verfahren bricht nach endlich vielen Schritten ab, dann ist

$$\tau_r \circ \dots \circ \tau_1 \circ \sigma = \text{id}, \quad \text{also} \quad \tau_r \circ \dots \circ \tau_1 = \sigma^{-1} \quad \text{und} \quad \sigma = \tau_1 \circ \dots \circ \tau_r.$$

■

Nach all diesen Vorbereitungen kommen wir nun endlich zum

Beweis des Satzes Gegeben sei also die durch Permutation der Zeilen von E_n entstandene Matrix

$$P_\sigma := \begin{pmatrix} e_{\sigma(1)} \\ \vdots \\ e_{\sigma(n)} \end{pmatrix}.$$

Nach Lemma 2 gibt es Transpositionen τ_1, \dots, τ_r , so dass $\sigma = \tau_1 \circ \dots \circ \tau_r$. Daher kann P_σ aus E_n erhalten werden, indem man nacheinander die τ_r, \dots, τ_1 entsprechenden Zeilenvertauschungen durchführt. Nach D2' und Lemma 1 folgt

$$\det P_\sigma = (-1)^r = \text{sign } \sigma.$$

■

Man nennt P_σ eine **Permutationsmatrix**. Wir überlassen dem Leser den Beweis der einfachen

Bemerkung Für jeden Körper K ist die Abbildung

$$\mathcal{S}_n \rightarrow \text{GL}(n; K), \quad \sigma \mapsto P_\sigma,$$

ein injektiver Homomorphismus von Gruppen. Für $n \geq 2$ ist er nicht surjektiv.

3.2.4 Die alternierende Gruppe

Wie wir in 3.2.3 gesehen hatten, gibt es in \mathcal{S}_n Permutationen von positivem und negativem Signum. Es ist eine naheliegende und für die Berechnung von Determinanten wichtige Frage, wie sich die Gruppe \mathcal{S}_n aus diesen beiden Arten von Elementen zusammensetzt. Eine Antwort darauf gibt das folgende

Lemma a) Für jedes $n \geq 1$ ist

$$\mathcal{A}_n := \{\sigma \in \mathcal{S}_n : \text{sign } \sigma = +1\}$$

eine Untergruppe von \mathcal{S}_n .

b) Für $n \geq 2$ ist $\text{ord } \mathcal{A}_n = \frac{1}{2}n!$ und für jedes beliebige $\tau \in \mathcal{S}_n$ mit $\text{sign } \tau = -1$ gilt

$$\mathcal{S}_n \setminus \mathcal{A}_n = \mathcal{A}_n \circ \tau = \tau \circ \mathcal{A}_n,$$

insbesondere hat man disjunkte Zerlegungen

$$\mathcal{S}_n = \mathcal{A}_n \cup \mathcal{A}_n \circ \tau = \mathcal{A}_n \cup \tau \circ \mathcal{A}_n.$$

Die Untergruppe $\mathcal{A}_n \subset \mathcal{S}_n$ heißt *alternierende Gruppe*.

Beweis Aussage a) folgt sofort aus dem in 3.2.3 bewiesenen Lemma 1.

Zum Beweis von Aussage b) benützen wir, dass – wie allgemein in Gruppen – für jedes $\tau \in \mathcal{S}_n$ die Abbildungen

$$\mathcal{S}_n \rightarrow \mathcal{S}_n, \sigma \mapsto \sigma \circ \tau, \quad \text{und} \quad \mathcal{S}_n \rightarrow \mathcal{S}_n, \sigma \mapsto \tau \circ \sigma,$$

bijektiv sind. Das folgt sofort aus dem Korollar in 1.2.3. Ist insbesondere $\text{sign } \tau = -1$, so folgt

$$\mathcal{A}_n \cap \mathcal{A}_n \circ \tau = \mathcal{A}_n \cap \tau \circ \mathcal{A}_n = \emptyset$$

wieder aus Lemma 1 in 3.2.3. Das ergibt b). ■

Für $n = 3$ werden wir die Zerlegung in 3.2.5 explizit angeben.

3.2.5 Existenz und Eindeutigkeit

Zentrales Ergebnis dieses Abschnitts ist das folgende

Theorem Sei K ein Körper und $n \in \mathbb{N}^*$. Dann gibt es genau eine Abbildung

$$\det : M(n \times n; K) \rightarrow K, \quad A \mapsto \det A,$$

die den Axiomen D1, D2 und D3 aus 3.2.1 genügt.

$$\text{Ist } A = (a_{ij}), \text{ so gilt } \det A = \sum_{\sigma \in \mathcal{S}_n} (\text{sign } \sigma) \cdot a_{1\sigma(1)} \cdot \dots \cdot a_{n\sigma(n)}. \quad (*)$$

Eine Regel, die der Formel (*) entspricht, wurde schon von G. W. LEIBNIZ angegeben. Daher wird (*) oft als **LEIBNIZ-Formel** bezeichnet. Sie ist nützlich für viele theoretische Überlegungen, aber wenig geeignet für explizite Berechnungen, da man $n!$ Produkte mit je n Faktoren summieren muss. Für sehr kleine n geht das noch:

$n = 1$: Hier ist $A = (a)$ und $\det A = a$.

$n = 2$: \mathcal{S}_2 hat zwei Elemente, also ist

$$\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11}a_{22} - a_{12}a_{21}.$$

$n = 3$: \mathcal{S}_3 hat 6 Elemente. Wir verwenden die Zerlegung $\mathcal{S}_3 = \mathcal{A}_3 \cup \mathcal{A}_3 \circ \tau$ mit $\tau = [1, 3]$.

\mathcal{A}_3 besteht aus den Elementen mit Signum $+1$:

$$\sigma_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \quad \sigma_2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \quad \sigma_3 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}.$$

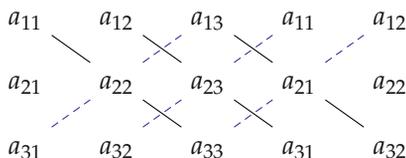
Die Elemente mit Signum -1 liegen in $\mathcal{A}_3 \circ \tau$:

$$\sigma_1 \circ \tau = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}, \quad \sigma_2 \circ \tau = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \quad \sigma_3 \circ \tau = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}.$$

Wie man sieht, besteht $\mathcal{A}_3 \circ \tau$ aus Transpositionen. Aus dieser Zerlegung von \mathcal{S}_3 folgt

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

Das ist die **Regel von SARRUS**. Man kann sie besonders suggestiv angeben, indem man die beiden ersten Spalten noch einmal rechts anfügt:



Die Produkte längs der Parallelen zur „Hauptdiagonalen“ haben positives Vorzeichen, die Produkte längs der gestrichelten (blauen) „Gegendiagonalen“ haben negatives Vorzeichen.

$n = 4$: Da $\text{ord } \mathcal{S}_4 = 24$ hat man in der LEIBNIZ-Formel 24 Summanden, das ist für eine Rechnung mit Kopf und Hand schon recht unangenehm. Außerdem hüte man sich vor einer Verallgemeinerung der Regel von SARRUS auf $n \geq 4$. Man würde statt $n!$ nur $2n$ Summanden erhalten und diese nicht alle mit den richtigen Vorzeichen. Etwa das Produkt

$$a_{12}a_{23}a_{34}a_{41} \text{ gehört zu } \sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} \text{ mit } \text{sign } \sigma = -1.$$

Man hüte sich auch vor der Illusion, für größere n benötige man zur Anwendung der LEIBNIZ-Formel nur genügend schnelle Rechner. Da $n!$ Produkte mit n Faktoren addiert werden, sind $(n-1) \cdot n!$ Multiplikationen nötig. Ein Superrechner, der pro Sekunde 10^9 Multiplikationen ausführt, würde dafür folgende Zeiten benötigen:

n	$(n-1) \cdot n!$	Sekunden
10	$0.327 \cdot 10^8$	0.0327
15	$0.183 \cdot 10^{14}$	$0.183 \cdot 10^5 \approx 5$ Stunden
20	$0.462 \cdot 10^{20}$	$0.462 \cdot 10^{11} \approx 1465$ Jahre
25	$0.372 \cdot 10^{27}$	$0.372 \cdot 10^{18} \approx 0.118 \cdot 10^{11}$ Jahre

Was dabei gar nicht berücksichtigt ist, sind die Additionen (die sind harmlos) und die Bestimmung aller $n!$ Permutationen (das ist gar nicht harmlos). Diese erschreckenden Zahlen zeigen, dass die LEIBNIZ-Formel für die Berechnung größerer Determinanten wenig praktischen Nutzen hat. Dagegen ist sie sehr hilfreich in der Theorie. So zeigt etwa die Struktur der Formel, dass der Wert der Determinanten stetig von den Einträgen abhängt. Insbesondere bleibt eine invertierbare Matrix bei genügend kleinen Veränderungen der Einträge invertierbar.

Beweis des Theorems Er verläuft nach dem Muster des in 3.2.1 ausgeführten Spezialfalls $n = 2$. Zunächst die *Eindeutigkeit*. Wir führen den Beweis so, dass er die LEIBNIZ-Formel ergibt.

$$\text{Sei } A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix},$$

wobei a_1, \dots, a_n die Zeilenvektoren bezeichnen. Dann ist

$$a_i = a_{i1}e_1 + \dots + a_{in}e_n \quad \text{für } i = 1, \dots, n.$$

Nun wendet man, von oben beginnend, Zeile für Zeile die Regel D1 an. Das ergibt

$$\begin{aligned} \det A &= \sum_{j_1=1}^n a_{1j_1} \cdot \det \begin{pmatrix} e_{j_1} \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{pmatrix} = \sum_{j_1=1}^n a_{1j_1} \cdot \left(\sum_{j_2=1}^n a_{2j_2} \cdot \det \begin{pmatrix} e_{j_1} \\ e_{j_2} \\ a_3 \\ \vdots \\ a_n \end{pmatrix} \right) \\ &= \dots = \sum_{j_1, \dots, j_n=1}^n a_{1j_1} \cdot \dots \cdot a_{nj_n} \cdot \det \begin{pmatrix} e_{j_1} \\ \vdots \\ e_{j_n} \end{pmatrix}, \end{aligned} \quad (**)$$

also eine Summe von n^n Produkten. Schließlich muss man die Matrix

$$E' := \begin{pmatrix} e_{j_1} \\ \vdots \\ e_{j_n} \end{pmatrix}$$

mit kanonischen Basisvektoren betrachten. Ist die Abbildung

$$\sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\} \quad \text{mit } \sigma(k) := j_k$$

bijektiv, so ist σ eine Permutation und es folgt aus 3.2.3

$$\det E' = \text{sign } \sigma.$$

Andernfalls ist σ nicht injektiv; dann hat E' mindestens zwei gleiche Zeilen und es folgt $\det E' = 0$. Damit wird die Summe $(**)$ von n^n Produkten auf $n!$ Summanden reduziert und es folgt $(*)$. Wenn also die Axiome D1, D2 und D3 erfüllbar sind, dann muss die LEIBNIZ-Formel gelten.

Zum Nachweis der Existenz wird die LEIBNIZ-Formel zur Definition der Determinante verwendet und es ist zu zeigen, dass die Axiome erfüllt sind.

D1 Zur Vereinfachung der Schreibweise zeigen wir die Linearität in der ersten Zeile.

$$\det \begin{pmatrix} \lambda a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \sum_{\sigma \in \mathcal{S}_n} (\text{sign } \sigma) \cdot \lambda \cdot a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdot \dots \cdot a_{n\sigma(n)} = \lambda \cdot \det \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}.$$

$$\begin{aligned}
 \det \begin{pmatrix} a'_1 + a''_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} &= \sum_{\sigma \in \mathcal{S}_n} (\text{sign } \sigma) \cdot (a'_{1\sigma(1)} + a''_{1\sigma(1)}) \cdot a_{2\sigma(2)} \cdot \dots \cdot a_{n\sigma(n)} \\
 &= \sum_{\sigma \in \mathcal{S}_n} (\text{sign } \sigma) \cdot a'_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdot \dots \cdot a_{n\sigma(n)} \\
 &\quad + \sum_{\sigma \in \mathcal{S}_n} (\text{sign } \sigma) \cdot a''_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdot \dots \cdot a_{n\sigma(n)} \\
 &= \det \begin{pmatrix} a'_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \det \begin{pmatrix} a''_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}.
 \end{aligned}$$

D2 ist etwas komplizierter. Man verwendet das Lemma aus 3.2.4, dass mit jeder beliebigen Transposition $\tau \in \mathcal{S}_n$ eine disjunkte Zerlegung

$$\mathcal{S}_n = \mathcal{A}_n \cup \mathcal{A}_n \circ \tau$$

vorliegt. Da sich der Beweis in den Indizes abspielt, geben wir zunächst ein konkretes Beispiel mit $n = 3$. Sei also

$$A = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \quad \text{mit} \quad a_1 = a_3 \quad \text{und} \quad \mathcal{S}_3 = \mathcal{A}_3 \cup \mathcal{A}_3 \circ \tau \quad \text{mit} \quad \tau = [1, 3].$$

Benützen wir in der Regel von SARRUS die Gleichungen $a_{3j} = a_{1j}$ für $j \in \{1, 2, 3\}$, so folgt

$$\begin{aligned}
 \det A &= a_{11}a_{22}a_{13} + a_{12}a_{23}a_{11} + a_{13}a_{21}a_{12} \\
 &\quad - a_{13}a_{22}a_{11} - a_{11}a_{23}a_{12} - a_{12}a_{21}a_{13}.
 \end{aligned}$$

Wie man sofort sieht, heben sich je zwei untereinander stehende Summanden mit entgegengesetzten Vorzeichen auf, und es folgt $\det A = 0$. Man beachte, dass hier die Kommutativität der Multiplikation von K benutzt wurde.

Im allgemeinen Fall sei

$$A = \begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \quad \text{mit} \quad i \neq j \quad \text{und} \quad a_j = a_i.$$

Dann verwenden wir die Zerlegung $\mathcal{S}_n = \mathcal{A}_n \cup \mathcal{A}_n \circ \tau$ mit $\tau = [i, j]$. Dann ist

$$\det A = \sum_{\sigma \in \mathcal{A}_n} \dots \cdot a_{i\sigma(i)} \cdot \dots \cdot a_{j\sigma(j)} \cdot \dots - \sum_{\sigma \in \mathcal{A}_n} \dots \cdot a_{i\sigma(\tau(i))} \cdot \dots \cdot a_{j\sigma(\tau(j))} \cdot \dots$$

wobei die restlichen Faktoren nicht ausgeschrieben sind. Nun vergleicht man die zu einem $\sigma \in \mathcal{A}_n$ gehörenden Summanden aus der linken und der rechten Summe. Da $a_j = a_i$, $\tau(j) = i$ und $\tau(i) = j$ gilt

$$a_{j\sigma(\tau(j))} = a_{i\sigma(i)} \quad \text{und} \quad a_{j\sigma(j)} = a_{i\sigma(\tau(i))}.$$

Da alle anderen Faktoren in den beiden Produkten gleich sind, heben sich die beiden Summanden mit verschiedenen Vorzeichen auf, also folgt insgesamt $\det A = 0$. Man beachte, dass bei diesem Vergleich der Produkte die Kommutativität der Multiplikation benutzt wurde.

D3 ist ganz einfach, denn für $A = E_n$ verschwinden in der LEIBNIZ-Formel alle Summanden mit $\sigma \neq \text{id}$ und es verbleibt $\det E_n = 1 \cdot \dots \cdot 1 = 1$. ■

Wenn man sich den Beweis von Eindeutigkeit und Existenz der Determinante noch einmal ansieht, so stellt man fest, dass er genauso durchgeführt werden kann, wenn die Einträge der Matrix aus einem kommutativen Ring mit Eins stammen. Damit erhält man das für spätere Verwendung nützliche

Korollar Sei R ein kommutativer Ring mit 1 und $M(n \times n; R)$ die Menge der $n \times n$ -Matrizen mit Einträgen aus R . Dann gibt es genau eine Abbildung

$$\det : M(n \times n; R) \longrightarrow R$$

mit den Eigenschaften D1, D2, D3 aus 3.2.1. Ist $A = (a_{ij})$, so gilt die LEIBNIZ-Formel

$$\det A = \sum_{\sigma \in \mathcal{S}_n} (\text{sign } \sigma) \cdot a_{1\sigma(1)} \cdot \dots \cdot a_{n\sigma(n)}.$$

Die Eigenschaften D4 bis D12 hatten wir für Matrizen mit Einträgen aus einem Körper ohne Benutzung der LEIBNIZ-Formel aus D1 bis D3 abgeleitet. Immer dort, wo Zeilenumformungen benutzt wurden, muss man auch dividieren können; das geht nur uneingeschränkt bei Körpern. Ohne Zeilenumformungen wurden die Eigenschaften

$$D2', D4, D5, D9 \text{ und } D10$$

bewiesen, dabei waren keine Divisionen nötig. Die Eigenschaften

$$D6, D8, D11 \text{ und } D12$$

kann man auch ohne Divisionen, dafür aber mit mehr oder weniger mühsamen Betrachtungen der Permutationen, aus der LEIBNIZ-Formel ableiten. Die Eigenschaft D7 schließlich benötigt den Begriff des Rangs einer Matrix, dazu müssen die Einträge aus einem Körper stammen.

In der folgenden Theorie der Eigenwerte werden wir die Eigenschaften D6 und D8 im Falle eines Polynomrings $R = K[X]$ benutzen. Wir skizzieren kurz, wie man sie ohne Umformungen auch aus der LEIBNIZ-Formel ableiten kann.

D6* Ist R ein kommutativer Ring mit 1 und $A = (a_{ij}) \in M(n \times n; R)$ eine obere oder untere Dreiecksmatrix, so ist

$$\det A = a_{11} \cdot \dots \cdot a_{nn}.$$

Beweis Ist A eine obere Dreiecksmatrix, so betrachten wir in den Summanden aus der LEIBNIZ-Formel zunächst die letzten Faktoren $a_{n\sigma(n)}$. Sie sind alle Null bis auf eventuell a_{nn} . Für $a_{n-1, \sigma(n-1)}$ ist $\sigma(n-1) = n$ schon vergeben und es ist $a_{n-1, j} = 0$ für $j < n-1$, also verbleibt nur $\sigma(n-1) = n-1$. So geht man weiter nach oben, bis $\sigma(1) = 1$, also a_{11} verbleibt.

Für eine untere Dreiecksmatrix verfährt man analog von oben nach unten. ■

D8* Ist R ein kommutativer Ring mit 1 und

$$A = \begin{pmatrix} A_1 & C \\ 0 & A_2 \end{pmatrix} \in M(n \times n; R)$$

eine Blockmatrix mit $A_1 \in M(k \times k; R)$, so gilt

$$\det A = (\det A_1) \cdot (\det A_2).$$

Beweis Die Voraussetzung Blockmatrix bedeutet, dass

$$a_{ij} = 0 \quad \text{für} \quad i = k+1, \dots, n \quad \text{und} \quad j = 1, \dots, k. \quad (*)$$

In der vollen Permutationsgruppe S_n betrachten wir die Untergruppe

$$S'_n = \{\sigma \in S_n : \sigma(\{1, \dots, k\}) = \{1, \dots, k\}\}.$$

Die Permutationen aus S'_n lassen damit auch $\{k+1, \dots, n\}$ invariant. Aus Voraussetzung (*) folgt, dass

$$\det A = \sum_{\sigma \in S'_n} (\text{sign } \sigma) \cdot a_{1\sigma(1)} \cdot \dots \cdot a_{n\sigma(n)}.$$

Wie man sich leicht überlegt, ist diese Summe von $k!(n-k)!$ Produkten gleich $(\det A_1) \cdot (\det A_2)$. ■

3.3 Minoren

Wie wir in 0.5 und 2.4.6 gesehen hatten, kann man zur Lösung linearer Gleichungssysteme und zur Berechnung inverser Matrizen elementare Umformungen benutzen. Es gibt als Alternative auch klassische Verfahren mit Hilfe von Determinanten, die wir hier kurz beschreiben wollen. Sie sind wenig geeignet für numerische Rechnungen, aber nützlich für die Theorie, etwa im Fall $K = \mathbb{R}$ oder $K = \mathbb{C}$ bei der Frage nach der stetigen Abhängigkeit der Lösungen eines linearen Gleichungssystems von den Koeffizienten oder der stetigen Abhängigkeit der Einträge der inversen Matrix A^{-1} von den Einträgen in A .

3.3.1 Die komplementäre Matrix

Wir beschränken uns hier auf eine quadratische Matrix $A = (a_{ij}) \in M(n \times n; K)$.

Mit $A'_{ij} \in M((n-1) \times (n-1); K)$ bezeichnen wir die Matrix, die aus A durch Streichen (d.h. Weglassen) der Zeile i und der Spalte j entsteht. Dann ist die zu A **komplementäre Matrix**

$$A^\# = (a_{ij}^\#) \text{ erklärt durch } a_{ij}^\# = (-1)^{i+j} \cdot \det A'_{ji}.$$

Man beachte dabei die Umkehrung der Indizes i und j . Im Fall $n = 2$ ist

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, A^\# = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \text{ und } A \cdot A^\# = (ad - bc) \cdot E_2.$$

Das ist ein Spezialfall von folgendem

Satz Ist $n \geq 2$ und $A \in M(n \times n; K)$, so gilt

$$A \cdot A^\# = A^\# \cdot A = \det A \cdot E_n.$$

Ist insbesondere $A \in GL(n; K)$, so folgt

$$A^{-1} = \frac{1}{\det A} \cdot A^\#.$$

Beweis Neben der $(n-1) \times (n-1)$ -Matrix A'_{ij} betrachten wir die $n \times n$ -Matrix

$$A_{ij}^{(1)} := \begin{pmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1n} \\ \vdots & & \vdots & & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,j} & \cdots & a_{i-1,n} \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ a_{i+1,1} & \cdots & a_{i+1,j} & \cdots & a_{i+1,n} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nn} \end{pmatrix}$$

bei der die Zeile i von A durch e_j ersetzt wurde. Für ein beliebiges $k \in \{1, \dots, n\}$ ist dann

$$\sum_{j=1}^n a_{kj} \cdot \det A_{ij}^{(1)} = \begin{cases} \det A & \text{für } k = i, \\ 0 & \text{für } k \neq i, \end{cases} \quad (*)$$

denn nach D1 ergibt diese Summe den Wert der Determinante der Matrix, die aus A durch Ersatz der Zeile i durch die Zeile k entsteht. Weiter gilt

$$\det A_{ij}^{(1)} = (-1)^{i+j} \cdot \det A'_{ij}, \quad (**)$$

denn man kann $A_{ij}^{(1)}$ umformen zu

$$\left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & & \\ 0 & & & \end{array} A'_{ij} \right).$$

Dabei werden zunächst die Einträge von A'_{ij} in Spalte j oberhalb und unterhalb der 1 durch Zeilenumformungen zu Null gemacht; das ändert den Wert der Determinante nicht. Die entstandene Matrix kann man durch $i-1$ Vertauschungen benachbarter Zeilen und $j-1$ Vertauschungen benachbarter Spalten auf die angegebene Form bringen. Da $(-1)^{(i-1)+(j-1)} = (-1)^{i+j}$ folgt (**). Nun kann man den Eintrag von $A \cdot A^\#$ an der Stelle (k, i) berechnen, das ist nach (**) und (*)

$$\begin{aligned} \sum_{j=1}^n a_{kj} \cdot a_{ji}^\# &= \sum_{j=1}^n a_{kj} \cdot (-1)^{i+j} \cdot \det A'_{ij} = \sum_{j=1}^n a_{kj} \cdot \det A_{ij}^{(1)} \\ &= \begin{cases} \det A & \text{für } k = i, \\ 0 & \text{für } k \neq i. \end{cases} \end{aligned}$$

Also gilt $A \cdot A^\# = \det A \cdot E_n$. Die Gleichung $A^\# \cdot A = \det A \cdot E_n$ folgt analog. ■

Beispiel Sei

$$A := \begin{pmatrix} 7 & -5 & 6 \\ -2 & 3 & -3 \\ -1 & 2 & -1 \end{pmatrix}.$$

Dann ist $\det A = 10$ und

$$a_{11}^\# = \det \begin{pmatrix} 3 & -3 \\ 2 & -1 \end{pmatrix} = 3, \quad a_{12}^\# = -\det \begin{pmatrix} -5 & 6 \\ 2 & -1 \end{pmatrix} = 7, \quad a_{13}^\# = \det \begin{pmatrix} -5 & 6 \\ 3 & -3 \end{pmatrix} = -3,$$

$$\text{u.s.w., also } A^{-1} = \frac{1}{10} \begin{pmatrix} 3 & 7 & -3 \\ 1 & -1 & 9 \\ -1 & -9 & 11 \end{pmatrix}.$$

3.3.2 LAPLACE-Entwicklung

Nach dem Satz aus 3.3.1 gilt für den Eintrag von $A \cdot A^\#$ an der Stelle (i, i)

$$\det A = \sum_{j=1}^n a_{ij} \cdot a_{ji}^\# = \sum_{j=1}^n (-1)^{i+j} \cdot a_{ij} \cdot \det A_{ij} \quad (*)$$

und analog für den Eintrag von $A^\# \cdot A$ an der Stelle (j, j)

$$\det A = \sum_{i=1}^n a_{ji}^\# \cdot a_{ij} = \sum_{i=1}^n (-1)^{i+j} \cdot a_{ij} \cdot \det A_{ij}. \quad (**)$$

Bei Formel (*) spricht man von der **Entwicklung nach einer Zeile** i , bei Formel (**) von der **Entwicklung nach einer Spalte** j . Die durch den Faktor $(-1)^{i+j}$ gegebene Verteilung der Vorzeichen kann man sich ähnlich wie ein Schachbrettmuster vorstellen, etwa im Fall $n = 3$:

+	-	+
-	+	-
+	-	+

In diesem Fall sieht man auch, dass durch die Formeln (*) oder (**) der Rechenaufwand im allgemeinen der gleiche ist, wie bei der LEIBNIZ-Formel. So erhält man durch Entwicklung nach der 1. Zeile

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

Das ist dieselbe Summe wie nach der Regel von SARRUS. Die Rechnung wird höchstens dann einfacher, wenn in einer Zeile oder Spalte möglichst viele Nullen auftreten. So ist etwa

$$\det \begin{pmatrix} 0 & 3 & 1 \\ 2 & 1 & 4 \\ 1 & -1 & 0 \end{pmatrix} = -3 \cdot (-4) + 1 \cdot (-3) = 12 - 3 = 9.$$

3.3.3 Die CRAMERSche Regel

Ist in einem linearen Gleichungssystem $Ax = b$ die Matrix A quadratisch und invertierbar, also $A \in \text{GL}(n; K)$ und $b = {}^t(b_1, \dots, b_n)$, so gibt es nach der allgemeinen Theorie genau eine Lösung $x = {}^t(x_1, \dots, x_n)$ und man kann sie berechnen als

$$x = A^{-1} \cdot b,$$

denn die durch A definierte lineare Abbildung $F_A : K^n \rightarrow K^n$ ist ein Isomorphismus. Ist

$$A^{-1} = (a'_{ij}), \quad \text{so folgt} \quad x_i = \sum_{j=1}^n a'_{ij} \cdot b_j.$$

Da $\det A \cdot a'_{ij} = (-1)^{i+j} \cdot \det A'_{ji}$ nach dem Satz aus 3.3.1, folgt

$$\det A \cdot x_i = \sum_{j=1}^n (-1)^{i+j} \cdot b_j \cdot \det A'_{ji}.$$

Die Summe rechts ist die LAPLACE-Entwicklung der Determinante von A , nachdem die Spalte i durch b ersetzt wurde. Dieses Ergebnis kann man noch einmal explizit aufschreiben:

$$x_i = \frac{\det \begin{pmatrix} a_{11} & \cdots & a_{1,i-1} & b_1 & a_{1,i+1} & \cdots & a_{1n} \\ & & & \vdots & & & \\ a_{n1} & \cdots & a_{n,i-1} & b_n & a_{n,i+1} & \cdots & a_{nn} \end{pmatrix}}{\det A}$$

Das ist die **CRAMERSche Regel**, die wir für $n = 2$ schon in 3.1.1 gefunden hatten. Sie ist wenig geeignet zur Berechnung der Lösung x , da man $n + 1$ Determinanten ausrechnen müsste. Aber sie zeigt die stetige Abhängigkeit der Lösung x von den Koeffizienten a_{ij} und b_j . Genauer gesagt, sind die x_i rationale Funktionen (d.h. Quotienten von Polynomen) in den a_{ij} und b_j . Man sieht auch, dass bei kleinen Werten von $\det A$ kleine Veränderungen der Koeffizienten große Auswirkungen auf die Lösungen haben können. Das war schon bei der HILBERT-Matrix A in 0.5.5 zu beobachten gewesen. Nach Beispiel 2 aus 3.2.2 ist $\det A = \frac{1}{2160}$.

*Eigenvalues are the most important feature
of practically any dynamical system.*

GILBERT STRANG

Kapitel 4

Eigenwerte

4.1 Grundbegriffe

4.1.1 Eigenwerte und Eigenvektoren

Wir erinnern zunächst an die Darstellung einer linearen Abbildung $F: V \rightarrow W$ zwischen Vektorräumen über einem Körper K durch eine Matrix. Nach 2.5.3 gibt es stets spezielle Basen $\mathcal{A} = (v_1, \dots, v_n)$ von V und $\mathcal{B} = (w_1, \dots, w_m)$ von W derart, dass

$$F(v_j) = \begin{cases} w_j & \text{für } j = 1, \dots, r, \\ 0 & \text{für } j = r + 1, \dots, n. \end{cases}$$

Die darstellende Matrix ist dann in der Normalform

$$M_{\mathcal{B}}^{\mathcal{A}}(F) = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Dabei ist $r = \text{rang } F = \dim F(V)$ der Rang von F . Diese Matrix ist offenbar von nicht zu übertreffender Übersichtlichkeit.

Im Fall einer linearen Abbildung $F: V \rightarrow V$, d.h. eines *Endomorphismus* von V , ist es angemessen, nur eine Basis \mathcal{B} von V zu verwenden und zu versuchen, die Matrix

$$M_{\mathcal{B}}(F) := M_{\mathcal{B}}^{\mathcal{B}}(F)$$

durch geschickte Wahl von \mathcal{B} möglichst einfach werden zu lassen. Wie wir schon am Ende von 2.5.3 gesehen hatten, wird ein Endomorphismus F eines 1-dimensionalen Vektorraums V bezüglich jeder Basis $\mathcal{B} = (v)$ durch die gleiche Matrix (λ) beschrieben.

Dieser Faktor λ gehört also unzertrennlich zu F . Ist $\dim V = n$, so ist ein Endomorphismus $F : V \rightarrow V$ besonders übersichtlich, wenn es eine Basis $\mathcal{B} = (v_1, \dots, v_n)$ und Skalare $\lambda_1, \dots, \lambda_n \in K$ gibt, so dass

$$F(v_1) = \lambda_1 \cdot v_1, \dots, F(v_n) = \lambda_n \cdot v_n.$$

In diesem Fall gilt für die darstellende Matrix

$$M_{\mathcal{B}}(F) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

Wann es so eine Basis gibt, ist ganz und gar nicht offensichtlich, aber diese Frage ist der Ausgangspunkt für folgende

Definition Sei V ein K -Vektorraum und $F : V \rightarrow V$ ein Endomorphismus. Ein $\lambda \in K$ heißt **Eigenwert** von F , wenn es ein $v \in V$ gibt mit

$$v \neq \mathbf{0} \quad \text{und} \quad F(v) = \lambda \cdot v.$$

Ein $v \in V$ mit $v \neq \mathbf{0}$ heißt **Eigenvektor**, wenn es ein $\lambda \in K$ gibt, so dass

$$F(v) = \lambda \cdot v.$$

Vorsicht! Ein Eigenwert kann gleich Null sein, ein Eigenvektor muss vom Nullvektor verschieden sein. Denn $F(\mathbf{0}) = \lambda \cdot \mathbf{0}$ für jedes $\lambda \in K$.

Die Probleme sind offensichtlich: Wie findet man bei einem gegebenen Endomorphismus eventuell vorhandene Eigenwerte und Eigenvektoren? Bevor wir typische Beispiele behandeln, stellen wir die grundlegenden algebraischen Werkzeuge im Spezialfall $V = K^n$ bereit. In diesem Fall kann man den Endomorphismus F durch eine Matrix A ersetzen. Dann heißt $\lambda \in K$ **Eigenwert** von A , wenn es ein $x \in K^n$ gibt mit

$$x \neq \mathbf{0} \quad \text{und} \quad A \cdot x = \lambda \cdot x,$$

und ein derartiges x heißt **Eigenvektor** der Matrix A .

Schließlich erklärt man den **Eigenraum** eines Endomorphismus F von V zu $\lambda \in K$ als

$$\text{Eig}(F; \lambda) := \{v \in V : F(v) = \lambda \cdot v\} \subset V.$$

Analog ist für eine Matrix $A \in M(n \times n; K)$

$$\text{Eig}(A; \lambda) := \{x \in K^n : A \cdot x = \lambda \cdot x\} \subset K^n.$$

Offensichtlich hat der Eigenraum folgende Eigenschaften:

- Bemerkung** a) $\text{Eig}(F; \lambda) \subset V$ ist ein Untervektorraum.
 b) $\text{Eig}(F; \lambda) \neq \{\mathbf{o}\} \Leftrightarrow \lambda$ ist Eigenwert von F .
 c) $\text{Eig}(F; \lambda) \setminus \{\mathbf{o}\}$ ist die Menge der Eigenvektoren zum Eigenwert λ .
 d) $\text{Eig}(F; \lambda) = \text{Ker}(F - \lambda \cdot \text{id}_V)$.
 e) $\dim \text{Eig}(F; \lambda) = \dim V - \text{rang}(F - \lambda \cdot \text{id}_V)$.

Aussage e) folgt dabei sofort aus d) und der Dimensionsformel für lineare Abbildungen aus 2.3.4.

Das kann man alles munter definieren; die Frage, wie groß diese Eigenräume sind, hängt ganz von F ab. Damit beschäftigen sich die folgenden Abschnitte. Entscheidend für die Suche nach Eigenwerten ist das

Lemma Sei $A \in M(n \times n; K)$ und $\lambda \in K$. Dann gilt:

$$\lambda \text{ Eigenwert von } A \Leftrightarrow \det(A - \lambda \cdot E_n) = 0.$$

Beweis Zunächst sei bemerkt, dass die Matrix $A - \lambda \cdot E_n$ aus A entsteht, indem man von allen Einträgen in der Diagonale λ abzieht. Somit ist etwa

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} - \lambda \cdot E_2 = \begin{pmatrix} a - \lambda & b \\ c & d - \lambda \end{pmatrix}.$$

Die Behauptung folgt nun durch eine Kombination von Ergebnissen der vorhergehenden Kapitel: Für ein $\lambda \in K$ ist die Existenz eines $x \neq \mathbf{o}$ mit $A \cdot x = \lambda \cdot x$ äquivalent zu

$$\begin{aligned} A \cdot x - \lambda \cdot x &= \mathbf{o} \\ \Leftrightarrow (A - \lambda \cdot E_n) \cdot x &= \mathbf{o} && \text{nach 2.4.4,} \\ \Leftrightarrow \text{Das homogene Gleichungssystem } (A - \lambda \cdot E_n) \cdot x &= \mathbf{o} \\ &\text{hat eine Lösung } x \neq \mathbf{o} && \text{nach 2.3.5,} \\ \Leftrightarrow \text{rang}(A - \lambda \cdot E_n) < n &&& \text{nach 2.3.5,} \\ \Leftrightarrow \det(A - \lambda \cdot E_n) = 0 &&& \text{nach D7 in 3.2.2.} \end{aligned}$$

Daraus erhält man sofort das

Korollar Ein Vektor $x \in K^n$ ist genau dann ein Eigenvektor von A zu $\lambda \in K$, wenn er eine nicht-triviale Lösung des homogenen linearen Gleichungssystems

$$(A - \lambda \cdot E_n) \cdot x = \mathbf{o}$$

ist.

4.1.2 Endomorphismen des \mathbb{R}^2

Wir beginnen die Suche nach Eigenwerten und Eigenvektoren von Endomorphismen des \mathbb{R}^2 bei den *Drehungen* um einen Winkel α . Nach 2.4.3 sind sie beschrieben durch

$$A_\alpha := \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \quad \text{mit } \alpha \in [0, 2\pi[.$$

Aus der geometrischen Anschauung ist klar, dass es Eigenvektoren nur für die Winkel $\alpha = 0$ und $\alpha = \pi$ geben kann. Für $\alpha = 0$ ist $A_0 = E_2$, also gilt für jeden Vektor $x \in \mathbb{R}^2$

$$A_0 \cdot x = 1 \cdot x,$$

somit ist jedes $x \neq \mathbf{o}$ ein Eigenvektor von A_0 zum Eigenwert 1, also $\text{Eig}(A_0; 1) = \mathbb{R}^2$. Für $\alpha = \pi$ ist

$$A_\pi = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -E_2, \quad \text{also } A_\pi \cdot x = (-1) \cdot x.$$

Somit ist jedes $x \neq \mathbf{o}$ Eigenvektor von A_π zum Eigenwert -1 , also $\text{Eig}(A_\pi; -1) = \mathbb{R}^2$. Dieses geometrische Ergebnis kann man algebraisch mit Hilfe des Lemmas aus 4.1.1 überprüfen. Dazu berechnet man

$$\det(A_\alpha - \lambda \cdot E_2) = \det \begin{pmatrix} \cos \alpha - \lambda & -\sin \alpha \\ \sin \alpha & \cos \alpha - \lambda \end{pmatrix} = \lambda^2 - (2 \cos \alpha) \cdot \lambda + 1.$$

Das ergibt die quadratische Gleichung $\lambda^2 - (2 \cos \alpha) \cdot \lambda + 1 = 0$ für α mit der Diskriminante

$$D = 4 \cos^2 \alpha - 4.$$

Offensichtlich ist $D \leq 0$ und $D = 0$ genau dann, wenn $\cos \alpha = \pm 1$, d.h. $\alpha = 0$ oder $\alpha = \pi$. Im Fall $\alpha = 0$ ist

$$\lambda^2 - 2\lambda + 1 = 0, \quad \text{also } \lambda = 1 \quad \text{und} \quad A - \lambda \cdot E_2 = \mathbf{o}.$$

Also ist der Lösungsraum des entsprechenden linearen Gleichungssystems ganz \mathbb{R}^2 .

Im Fall $\alpha = \pi$ ist

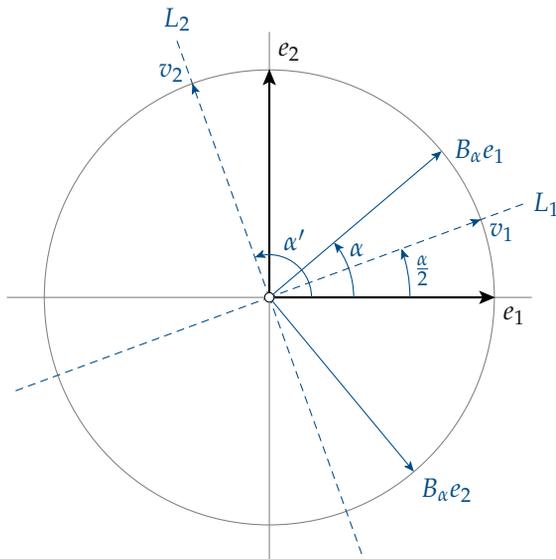
$$\lambda^2 + 2\lambda + 1 = 0, \quad \text{also } \lambda = -1 \quad \text{und} \quad A - \lambda \cdot E_2 = \mathbf{o}.$$

Auch in diesem Fall ist der Lösungsraum gleich \mathbb{R}^2 . Für alle anderen Winkel ist $D < 0$, also gibt es keine reellen Eigenwerte.

Indem wir in der obigen Matrix A das Vorzeichen der zweiten Spalte umkehren, erhalten wir

$$B_\alpha := \begin{pmatrix} \cos \alpha & \sin \alpha \\ \sin \alpha & -\cos \alpha \end{pmatrix} \quad \text{mit } \alpha \in [0, 2\pi[.$$

Aus der Zeichnung sieht man, dass durch B_α eine *Spiegelung* der Ebene an der Geraden L_1 mit dem Winkel $\frac{\alpha}{2}$ bewirkt wird.



Auch das kann man durch Rechnung bestätigen. Zunächst ist

$$\det(B_\alpha - \lambda \cdot E_2) = \det \begin{pmatrix} \cos \alpha - \lambda & \sin \alpha \\ \sin \alpha & -\cos \alpha - \lambda \end{pmatrix} = \lambda^2 - 1.$$

Also hat man Eigenwerte $\lambda_1 = +1$ und $\lambda_2 = -1$, und zwar unabhängig vom Winkel α .

Um Eigenvektoren zu $\lambda_1 = 1$ zu finden, hat man das Gleichungssystem

$$(\cos \alpha - 1) \cdot x_1 + \sin \alpha \cdot x_2 = 0 \quad (1)$$

$$\sin \alpha \cdot x_1 - (\cos \alpha + 1) \cdot x_2 = 0 \quad (2)$$

zu lösen. Da ein Eigenwert eingesetzt wurde, ist der Rang dieses Systems kleiner als 2, es genügt also eine der beiden Gleichungen zu betrachten. Für $\alpha = 0$ erhält man aus (2)

$$x_2 = 0, \quad \text{also den Eigenvektor } e_1.$$

Für $\alpha \in]0, 2\pi[$ ist $\cos \alpha - 1 \neq 0$, in diesem Fall kann man (1) verwenden. Um eine Lösung zu erhalten setzt man $\alpha = 2\beta$; dann ist

$$\sin 2\beta = 2 \sin \beta \cdot \cos \beta \quad \text{und} \quad \cos 2\beta = \cos^2 \beta - \sin^2 \beta.$$

Benutzt man diese Gleichungen, so folgt $(\cos 2\beta - 1) \cdot \cos \beta + \sin 2\beta \cdot \sin \beta = 0$, also ist

$$v_1 := \begin{pmatrix} \cos \frac{\alpha}{2} \\ \sin \frac{\alpha}{2} \end{pmatrix}$$

für alle $\alpha \in [0, 2\pi[$ ein Eigenvektor zum Eigenwert $\lambda_1 = 1$.

Zum Eigenwert $\lambda_2 = -1$ erhält man nach einer ähnlichen Rechnung für beliebiges α den Eigenvektor

$$v_2 := {}^t \left(\cos \frac{\alpha + \pi}{2}, \sin \frac{\alpha + \pi}{2} \right).$$

Die beiden Geraden $L_1 = \mathbb{R} \cdot v_1$ und $L_2 = \mathbb{R} \cdot v_2$ sind die Eigenräume zu den Eigenwerten λ_1 und λ_2 .

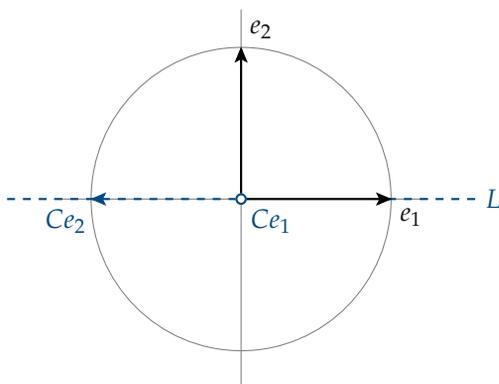
Nach den Drehungen und Spiegelungen des \mathbb{R}^2 betrachten wir noch den Endomorphismus, der beschrieben ist durch die Matrix

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

Da $\det(C - \lambda \cdot E_2) = \lambda^2$, gibt es nur den Eigenwert $\lambda = 0$. Die Eigenvektoren dazu sind bestimmt durch die Gleichung

$$0 \cdot x_1 - x_2 = 0,$$

also ist jeder Eigenvektor von der Form $v = q \cdot e_1$ mit $q \neq 0$. Er ist enthalten im Eigenraum $L = \mathbb{R} \cdot e_1$, das ist der Kern des durch C bestimmten Endomorphismus.



4.1.3 Differentialgleichungen*

Ganz allgemein stellt die lineare Algebra wichtige Hilfsmittel für die Analysis bereit. Speziell helfen Eigenwerte und Eigenvektoren bei der Lösung von Differentialgleichungen. Das wird etwa in [FO₂, §16] ausführlich dargestellt; wir begnügen uns hier mit einfachen Beispielen.

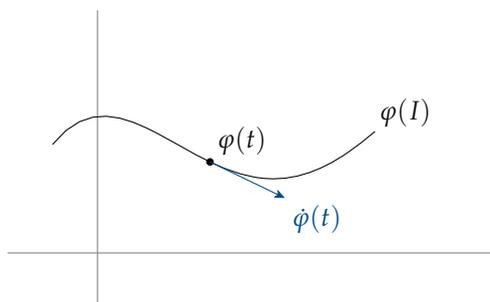
Zunächst erinnern wir daran, dass man unter einer differenzierbaren ebenen **Kurve** eine differenzierbare Abbildung

$$\varphi : I \rightarrow \mathbb{R}^2, t \mapsto \begin{pmatrix} x(t) \\ y(t) \end{pmatrix},$$

versteht; dabei ist $I \subset \mathbb{R}$ ein Intervall. Der Buchstabe t deutet an, dass man sich unter $\varphi(t)$ einen Punkt vorstellen kann, der sich im Laufe der Zeit bewegt. Zu jedem $t \in I$ ist

$$\dot{\varphi}(t) := \begin{pmatrix} \dot{x}(t) \\ \dot{y}(t) \end{pmatrix}$$

der **Tangentenvektor** an die Kurve im Punkt $\varphi(t)$.



Ist zu jedem Punkt $p = {}^t(x, y) \in \mathbb{R}^2$ ein Vektor $v(p) \in \mathbb{R}^2$ gegeben, so spricht man von einem **Vektorfeld** oder aus physikalischer Sicht von einem **Fluss**. Eine besonders einfache Regel erhält man durch jede Matrix

$$A \in M(2 \times 2; \mathbb{R}) \quad \text{und} \quad v(p) := A \cdot \begin{pmatrix} x \\ y \end{pmatrix}.$$

Dann kann man $I = [0, \infty[$ setzen und eine differenzierbare Kurve $\varphi: I \rightarrow \mathbb{R}^2$ suchen mit

$$\dot{\varphi}(t) = A \cdot \varphi(t) \quad \text{für alle } t \in I \quad \text{und} \quad \varphi(0) = \begin{pmatrix} a \\ b \end{pmatrix}.$$

Das bedeutet, dass die Kurve zur Zeit $t = 0$ in $\begin{pmatrix} a \\ b \end{pmatrix}$ starten und an jeder Stelle $\varphi(t)$ den Tangentenvektor $A \cdot \varphi(t)$ haben soll. Wieder aus der Sicht der Physik setzt man ein Boot im Startpunkt ein und beobachtet, wie es von der Strömung im Lauf der Zeit getrieben wird.

Bemerkung a) Für jedes Intervall $I \subset \mathbb{R}$ ist die Menge

$$\mathcal{D} := \{ \varphi \in \text{Abb}(I, \mathbb{R}^2) : \varphi \text{ differenzierbar} \}$$

ein \mathbb{R} -Vektorraum.

b) Für jede Matrix $A \in M(2 \times 2; \mathbb{R})$ ist die Teilmenge

$$\mathcal{L}_A := \{ \varphi \in \mathcal{D} : \dot{\varphi} = A \cdot \varphi \} \subset \mathcal{D}$$

ein Untervektorraum.

Der *Beweis* ist ganz einfach. Man beachte, dass \mathcal{D} unendliche Dimension hat. Wie man in der Analysis lernt, gibt es zu jeder Anfangsbedingung genau eine Lösung; daraus folgt $\dim \mathcal{L}_A = 2$ für jedes A [FO2, §13]. ■

Dass Lösungen existieren, ist beruhigend, aber man möchte sie auch explizit angeben. Dazu zunächst das ganz einfache

Beispiel 1 Für eine Diagonalmatrix

$$A = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \text{ hat man } \dot{x}(t) = \lambda_1 \cdot x(t) \quad \text{und} \quad \dot{y}(t) = \lambda_2 \cdot y(t).$$

Die Lösungen dazu sind von der Form

$$\varphi(t) = \begin{pmatrix} x(t) \\ y(t) \end{pmatrix} = \begin{pmatrix} c_1 e^{\lambda_1 t} \\ c_2 e^{\lambda_2 t} \end{pmatrix} \quad \text{mit } c_1, c_2 \in \mathbb{R} \text{ beliebig.}$$

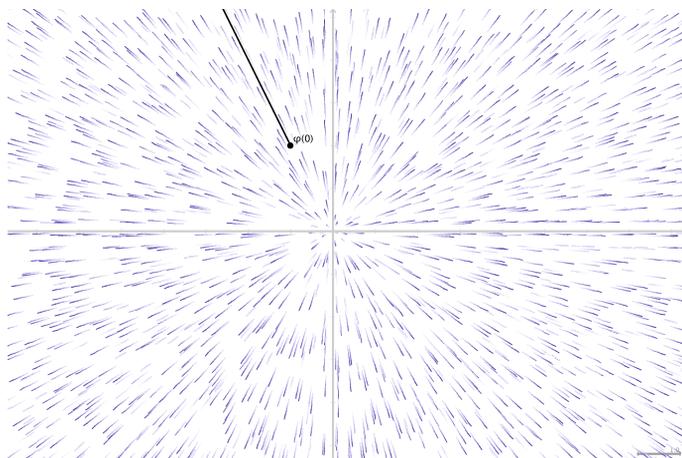
Die Anfangsbedingung

$$\varphi(0) = \begin{pmatrix} a \\ b \end{pmatrix} \text{ ergibt } \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix},$$

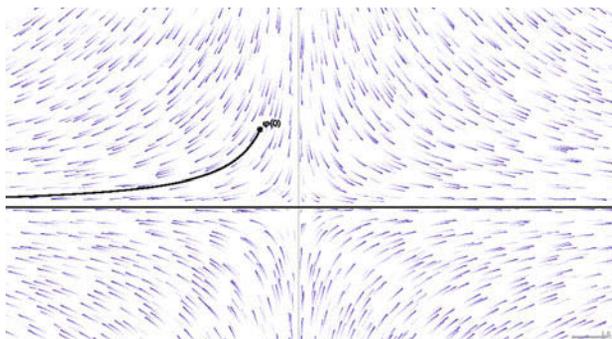
damit wird die Lösung eindeutig. Für die speziellen Werte $\lambda_1 = \lambda_2 = 0$ steht der Fluss still. Für $\lambda_1 = \lambda_2 = 1$ ist

$$\varphi(t) = e^t \cdot \begin{pmatrix} a \\ b \end{pmatrix},$$

das entspricht einer „Explosion“ im Ursprung.



Für $\lambda_1 = 1$ und $\lambda_2 = -1$ ist das Bild komplizierter. Für einen Startpunkt $\begin{pmatrix} a \\ 0 \end{pmatrix}$ geht der Weg geradlinig nach unendlich, für $\begin{pmatrix} 0 \\ b \end{pmatrix}$ wird er vom Ursprung angezogen. Alle anderen Lösungswege laufen auf Hyperbeln mit der Gleichung $x \cdot y = c_1 \cdot c_2$.



Nach dieser guten Erfahrung mit einer Diagonalmatrix kann man im Fall einer beliebigen Matrix A nach Richtungen suchen, in denen Lösungskurven auf Geraden durch den Ursprung verlaufen. Genauer gesagt macht man den „Ansatz“

$$\varphi(t) = e^{\lambda t} \cdot v,$$

wobei $\lambda \in \mathbb{R}$ und $\mathbf{o} \neq v \in \mathbb{R}^2$ gesucht sind. Eingesetzt in die Bedingung

$$\dot{\varphi}(t) = A \cdot \varphi(t) \quad \text{ergibt das} \quad \lambda \cdot e^{\lambda t} \cdot v = e^{\lambda t} \cdot A \cdot v,$$

also $A \cdot v = \lambda \cdot v$, da $e^{\lambda t} \neq 0$. Das ist eine Eigenwert-Bedingung; es entsteht die Frage, ob sie lösbar ist.

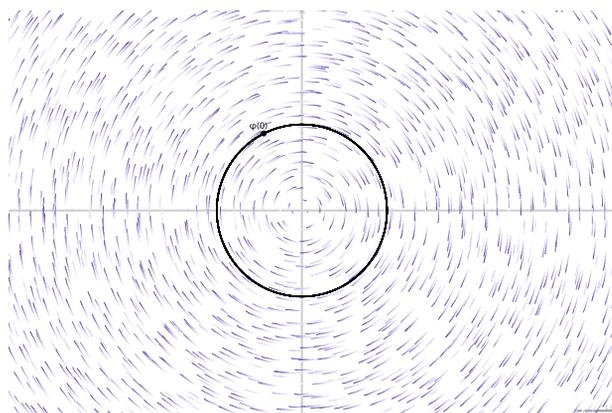
Beispiel 2 Die Matrix einer Drehung um den Winkel $\frac{\pi}{2}$ ist

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

Für den entsprechenden Fluss $\dot{\varphi} = A \cdot \varphi$ bedeutet das, dass er um den Ursprung kreist. Nun ist

$$\det(A - \lambda \cdot E_2) = \det \begin{pmatrix} -\lambda & -1 \\ 1 & -\lambda \end{pmatrix} = \lambda^2 + 1,$$

also gibt es keinen reellen Eigenwert λ und somit auch keinen Eigenwert v . Um die kreisförmigen Lösungen zu finden, kann man die komplexen Eigenwerte $\pm i$ verwenden (vgl. [FO₂, §16]).



Beispiel 3 Eine Spiegelung an der Geraden $y = x$ wird beschrieben durch

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

Zur Bestimmung der Eigenwerte berechnet man

$$\det(A - \lambda \cdot E_2) = \det \begin{pmatrix} -\lambda & 1 \\ 1 & -\lambda \end{pmatrix} = \lambda^2 - 1 = (\lambda - 1)(\lambda + 1).$$

Also hat man die Eigenwerte $\lambda_1 = 1$ und $\lambda_2 = -1$. Eigenvektoren dazu sind

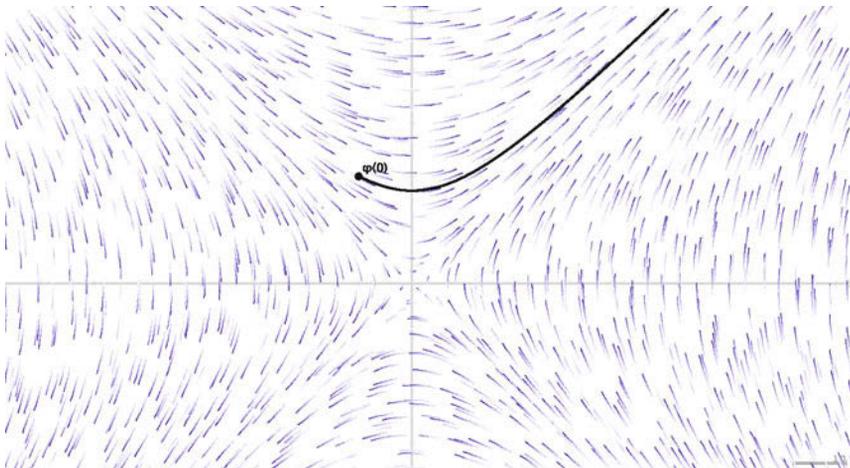
$$v_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \text{und} \quad v_2 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

Daraus erhält man als Lösungen von $\dot{\varphi} = A \cdot \varphi$

$$\varphi_1 = e^{\lambda_1 t} \cdot v_1 = e^t \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} e^t \\ e^t \end{pmatrix} \quad \text{und}$$

$$\varphi_2 = e^{\lambda_2 t} \cdot v_2 = e^{-t} \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} e^{-t} \\ -e^{-t} \end{pmatrix}.$$

Die allgemeine Lösung ist dann $\varphi = c_1 \cdot \varphi_1 + c_2 \cdot \varphi_2$ mit $c_1, c_2 \in \mathbb{R}$. Will man die Anfangsbedingung $\varphi(0) = \begin{pmatrix} -1 \\ 2 \end{pmatrix}$ erfüllen, so muss $c_1 = \frac{1}{2}$ und $c_2 = -\frac{3}{2}$ sein.



Die Bilder der Vektorfelder sind mit Hilfe von *mathe-vital* erzeugt.

Mehr über die Bedeutung von Eigenwerten in der Analysis findet man etwa bei [STR].

4.1.4 Das charakteristische Polynom

In 4.1.1 hatten wir einer Matrix $A \in M(n \times n; K)$ zur Bestimmung der Eigenwerte die Funktion

$$K \rightarrow K, \lambda \mapsto \det(A - \lambda \cdot E_n)$$

zugeordnet. Wir wollen nun zeigen, wie man allgemeiner für Endomorphismen eine derartige Funktion erhalten kann. Dabei benötigen wir folgendes

Lemma Sei V ein K -Vektorraum mit $\dim V < \infty$ und zwei Basen \mathcal{A} und \mathcal{B} sowie $F : V \rightarrow V$ ein Endomorphismus. Dann gilt

$$\det M_{\mathcal{B}}(F) = \det M_{\mathcal{A}}(F).$$

Wegen dieser Unabhängigkeit von der Wahl einer Basis \mathcal{B} kann man für jeden Endomorphismus F von V eine **Determinante** definieren durch

$$\det F := \det M_{\mathcal{B}}(F).$$

Beweis Wir setzen $A := M_{\mathcal{A}}(F)$ und $B := M_{\mathcal{B}}(F)$. Nach 2.5.2 gibt es eine Matrix $S \in GL(n; K)$ so dass $B = S \cdot A \cdot S^{-1}$. Daraus folgt nach D11 in 3.2.2

$$\det B = \det S \cdot \det A \cdot (\det S)^{-1} = \det A. \quad \blacksquare$$

Zu jedem Endomorphismus F von V und $\lambda \in K$ können wir $G_{\lambda} := F - \lambda \cdot id_V$ erklären. Daraus ergibt sich eine **charakteristische Funktion** von F

$$\chi_F : K \rightarrow K, \quad \lambda \mapsto \det(G_{\lambda}).$$

Ist F bezüglich einer Basis \mathcal{B} durch die Matrix A beschrieben, so ist

$$\chi_F(\lambda) = \det(A - \lambda \cdot E_n),$$

und diese Definition ist nach obigen Lemma unabhängig von der Wahl der Basis \mathcal{B} .

Nun entsteht das Problem, wie man die Funktion χ_F effizient beschreiben kann. Dazu ersetzt man das beliebig wählbare $\lambda \in K$ durch die Unbestimmte X . Bei der Berechnung der Determinante

$$\det(A - X \cdot E_n)$$

tritt aber ein delikates formales und ein unangenehmes praktisches Problem auf. Die Einträge in der Diagonalen von $A - X \cdot E_n$ sind nicht mehr Elemente von K , sondern lineare Polynome

$$a_{11} - X, \dots, a_{nn} - X \in K[X], \quad \text{also ist } A - X \cdot E_n \in M(n \times n; K[X]).$$

Da $K[X]$ kommutativer Ring mit 1 ist, kann man $\det(A - X \cdot E_n)$ entsprechend dem Korollar aus 3.2.5 nach der LEIBNIZ-Formel berechnen. Damit ist

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

ein Polynom. Für die praktische Berechnung der Determinante P_A entstehen gravierende Probleme, weil sie nicht mehr auf Zeilenumformungen zurückgeführt werden kann: durch lineare Polynome darf man nicht ohne Weiteres dividieren. Wie man doch noch mit Umformungen zum Ziel kommen kann, wird anschließend in einem Beispiel beschrieben.

Entsprechend seiner Definition beschreibt das Polynom P_A die charakteristische Funktion χ_F . Ist der Körper K unendlich, so folgt nach Korollar 2 aus 1.4.4, dass das Polynom P_A dadurch eindeutig bestimmt, und somit unabhängig ist von der Wahl der Basis \mathcal{B} . Im allgemeinen Fall kann man wie oben $B = SAS^{-1}$ mit $S \in \text{GL}(n; K)$ benutzen. Dann kann die Unbestimmte $X \in K[X]$ wie ein Skalar behandelt werden, somit ist

$$\begin{aligned} P_B &= \det(B - X \cdot E_n) = \det(SAS^{-1} - X \cdot (SE_nS^{-1})) = \\ &= \det(S(A - X \cdot E_n)S^{-1}) = \det(A - X \cdot E_n) = P_A. \end{aligned}$$

Dabei hat man allerdings die Rechenregeln für Matrizen aus 2.4.4 und den Determinanten-Multiplikationssatz D11 aus 3.2.2 für Matrizen mit Einträgen aus $K[X]$ verwendet.

Als Ergebnis halten wir schließlich fest:

Satz Sei V ein K -Vektorraum mit einer Basis \mathcal{B} , $F : V \rightarrow V$ ein Endomorphismus und $A := M_{\mathcal{B}}(F)$. Dann ist

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

ein Polynom vom Grad n und diese Definition ist unabhängig von der Wahl der Basis \mathcal{B} . Die Nullstellen von P_F sind die Eigenwerte von F .

P_F heißt das *charakteristische Polynom* von F .

Für eine Matrix A ist $P_A := \det(A - X \cdot E_n)$ das charakteristische Polynom von A .

Für sehr kleine n ist die Berechnung des charakteristischen Polynoms ganz einfach. Im Fall $n = 2$ ist

$$\begin{aligned} \det \begin{pmatrix} a_{11} - X & a_{12} \\ a_{21} & a_{22} - X \end{pmatrix} &= (a_{11} - X)(a_{22} - X) - a_{12}a_{21} \\ &= X^2 - (a_{11} + a_{22})X + (a_{11}a_{22} - a_{12}a_{21}). \end{aligned}$$

Für $n = 3$ erhält man mit $A = (a_{ij})$ nach der Regel von SARRUS

$$\begin{aligned} \det(A - X \cdot E_3) &= (a_{11} - X)(a_{22} - X)(a_{33} - X) + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\ &\quad - a_{13}(a_{22} - X)a_{31} - (a_{11} - X)a_{23}a_{32} - a_{12}a_{21}(a_{33} - X) \\ &= -X^3 + (a_{11} + a_{22} + a_{33})X^2 \\ &\quad - (a_{11}a_{22} - a_{12}a_{21} + a_{11}a_{33} - a_{13}a_{31} + a_{22}a_{33} - a_{23}a_{32})X + \det A. \end{aligned}$$

Wie man sieht, ist der Koeffizient von X eine Summe von speziellen Minoren von A . Im allgemeinen Fall erhält man durch Anwendung der LEIBNIZ-Formel aus 3.2.5

$$\det(A - X \cdot E_n) = (a_{11} - X) \cdot \dots \cdot (a_{nn} - X) + Q,$$

wobei der erste Summand zur Identität in \mathcal{S}_n gehört, und Q alle anderen $n! - 1$ Summanden enthält. Wie man leicht sieht, enthält Q keine Terme mit X^n und X^{n-1} , somit ist $\deg Q \leq n - 2$. Also hat das Polynom

$$P_A := \det(A - X \cdot E_n) = b_n X^n + b_{n-1} X^{n-1} + \dots + b_1 X + b_0$$

die Koeffizienten

$$\begin{aligned} b_n &= (-1)^n \\ b_{n-1} &= (-1)^{n-1} (a_{11} + \dots + a_{nn}) \\ &\vdots \\ b_0 &= \det A. \end{aligned}$$

Man nennt

$$\text{spur}(A) := a_{11} + \dots + a_{nn} \in K$$

die *Spur* der Matrix A . Die anderen Koeffizienten b_1, \dots, b_{n-2} sind nicht so leicht auszurechnen und haben keine speziellen Namen.

Da der konstante Koeffizient von P_F gleich $\det F$ ist, folgt sofort das

Korollar Genau dann ist $0 \in K$ ein Eigenwert von F , wenn $\det F = 0$. ■

Für größere Matrizen ist die Berechnung des charakteristischen Polynoms mit Hilfe der LEIBNIZ-Formel recht mühsam. Man kann sich auf die Berechnung von Determinanten beschränken, in denen die Unbestimmte X nicht vorkommt, das geht mit elementaren Umformungen.

Beispiel Sei

$$A = \begin{pmatrix} -5 & 1 & 6 & 6 \\ -12 & 2 & 12 & 12 \\ 1 & 1 & 0 & -2 \\ -4 & 0 & 4 & 6 \end{pmatrix}.$$

Von $P_A = X^4 + b_3 X^3 + b_2 X^2 + b_1 X + b_0$ kennt man schon die Koeffizienten

$$b_3 = -\text{spur} A = -3 \quad \text{und} \quad b_0 = P_A(0) = \det A = -8.$$

Um die fehlenden Koeffizienten b_1, b_2 zu bestimmen, setzt man in P_A für X zwei von Null verschiedene Argumente ein, etwa 1 und 2. Die Berechnung von zwei Determinanten mit Hilfe von Zeilenumformungen ergibt

$$P_A(1) = \det(A - E_4) = 0 \quad \text{und} \quad P_A(2) = \det(A - 2 \cdot E_4) = 0.$$

Durch Einsetzen dieser Werte in P_A erhält man

$$1 - 3 + b_2 + b_1 - 8 = 0 \quad \text{und} \quad 16 - 24 + 4b_2 + 2b_1 - 8 = 0.$$

Das ergibt die linearen Gleichungen

$$b_1 + b_2 = 10 \quad \text{und} \quad b_1 + 2b_2 = 8$$

mit der Lösung $b_1 = 12$ und $b_2 = -2$. Also folgt

$$P_A = X^4 - 3X^3 - 2X^2 + 12X - 8.$$

Ob es Eigenwerte gibt, hängt davon ab, ob das charakteristische Polynom P Nullstellen hat, und das hängt ab vom Körper K . Im Fall $K = \mathbb{C}$ zerfällt P nach dem Fundamentalsatz der Algebra in Linearfaktoren, im Fall $K = \mathbb{R}$ muss es bei geradem Grad von P nicht einmal eine einzige Nullstelle geben. Die 2×2 -Matrix aus Beispiel 3 in 4.1.3 ist symmetrisch, hier gibt es reelle Eigenwerte. Das ist kein Zufall:

Bemerkung Ist $A \in M(2 \times 2; \mathbb{R})$ symmetrisch, so zerfällt P_A in reelle Linearfaktoren.

Beweis Ist $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$, so folgt $P_A = X^2 - (a+c)X + (ac - b^2)$. Die Diskriminante dieses quadratischen Polynoms ist gleich $(a+c)^2 - 4(ac - b^2) = (a-c)^2 + 4b^2 \geq 0$. ■

In 5.3.5 zeigen wir, dass diese Aussage über P_A für beliebig große symmetrische reelle Matrizen gilt.

4.2 Diagonalisierung und Trigonalisierung

4.2.1 Diagonalisierbarkeit

Nun stehen die wesentlichen Hilfsmittel bereit, um die Frage zu klären, wann ein Endomorphismus durch eine Diagonalmatrix dargestellt werden kann.

Definition Sei V ein K -Vektorraum mit $\dim V = n < \infty$ und $F : V \rightarrow V$ linear. F heißt **diagonalisierbar**, wenn V eine Basis $\mathcal{B} = (v_1, \dots, v_n)$ besitzt, die aus Eigenvektoren von F besteht.

Das bedeutet, dass es zu jedem v_i ein $\lambda_i \in K$ gibt, so dass $F(v_i) = \lambda_i \cdot v_i$. Das ist gleichwertig mit der Bedingung

$$M_{\mathcal{B}}(F) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix},$$

d.h. die darstellende Matrix ist diagonal.

Analog heißt eine Matrix $A \in M(n \times n; K)$ **diagonalisierbar**, wenn die durch A erklärte lineare Abbildung

$$F_A : K^n \rightarrow K^n, x \mapsto A \cdot x,$$

diagonalisierbar ist. Nach 2.5.2 ist das gleichwertig mit der Existenz einer Matrix $S \in GL(n; K)$, derart dass

$$S \cdot A \cdot S^{-1} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix},$$

d.h. eine Diagonalmatrix ist.

Für die Diagonalisierbarkeit gibt es eine offensichtliche notwendige Bedingung.

Bemerkung Ist $F : V \rightarrow V$ diagonalisierbar, so zerfällt das charakteristische Polynom P_F in Linearfaktoren, d.h.

$$P_F = \pm (X - \lambda_1) \cdot \dots \cdot (X - \lambda_n),$$

wobei $n = \dim V$ und $\lambda_1, \dots, \lambda_n \in K$.

Beweis Nach dem Lemma aus 4.1.4 kann man zur Berechnung des charakteristischen Polynoms jede Basis von V verwenden, insbesondere eine Basis \mathcal{B} aus Eigenvektoren.

Dann ist

$$P_F = \det(M_{\mathcal{B}}(F) - X \cdot E_n) = \det \begin{pmatrix} \lambda_1 - X & & 0 \\ & \ddots & \\ 0 & & \lambda_n - X \end{pmatrix} = (\lambda_1 - X) \cdot \dots \cdot (\lambda_n - X).$$

■

Dass die angegebene Bedingung an das charakteristische Polynom nicht hinreichend ist, sieht man an dem ganz einfachen

Beispiel Ist $\lambda \in K$ beliebig und

$$A = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}, \quad \text{so folgt } P_A = (X - \lambda)^2, \quad \text{also } \mu(P_A; \lambda) = 2.$$

Also ist λ der einzige Eigenwert. Ein Eigenvektor $v = {}^t(x_1, x_2)$ muss die Bedingungen $x_2 = 0$ und $x_1 \neq 0$ erfüllen. Daher gilt für den Eigenraum

$$\text{Eig}(A; \lambda) = K \cdot e_1,$$

also gibt es keinen von e_1 linear unabhängigen Eigenvektor, somit kann A nicht diagonalisierbar sein.

In obigem Beispiel hatten wir eine Nullstelle des charakteristischen Polynoms der Vielfachheit 2 (vgl. 1.4.4). Besonders angenehm ist der Fall, dass alle Nullstellen des charakteristischen Polynoms einfach sind:

Satz über einfache Eigenwerte Ist $\dim V = n$, $F \in \text{End}(V)$ und

$$P_F = \pm (X - \lambda_1) \cdot \dots \cdot (X - \lambda_n)$$

mit paarweise verschiedenen Eigenwerten $\lambda_1, \dots, \lambda_n$, so ist F diagonalisierbar.

Diese Bedingung ist offensichtlich in obigem Beispiel nicht erfüllt.

Der *Beweis* ergibt sich sofort aus dem etwas allgemeineren

Lemma Eigenvektoren v_1, \dots, v_m einer linearen Abbildung $F: V \rightarrow V$ zu paarweise verschiedenen Eigenwerten $\lambda_1, \dots, \lambda_m$ sind stets linear unabhängig. Insbesondere ist $m \leq \dim V$.

Beweis des Lemmas Wir führen Induktion über m . Im Fall $m = 1$ hat man einen Eigenvektor $v_1 \neq \mathbf{o}$, er ist linear unabhängig. Sei $m \geq 2$ und

$$q_1 v_1 + \dots + q_{m-1} v_{m-1} + q_m v_m = \mathbf{o}. \quad (*)$$

Nun der kleine Trick: Auf (*) kann man einerseits F anwenden, andererseits mit λ_m multiplizieren. Das ergibt

$$\begin{aligned} \varrho_1 \lambda_1 v_1 + \dots + \varrho_{m-1} \lambda_{m-1} v_{m-1} + \varrho_m \lambda_m v_m &= \mathbf{o} \quad \text{und} \\ \varrho_1 \lambda_m v_1 + \dots + \varrho_{m-1} \lambda_m v_{m-1} + \varrho_m \lambda_m v_m &= \mathbf{o}. \end{aligned}$$

Durch Subtraktion der beiden Gleichungen erhält man

$$\varrho_1 (\lambda_1 - \lambda_m) v_1 + \dots + \varrho_{m-1} (\lambda_{m-1} - \lambda_m) v_{m-1} = \mathbf{o}.$$

Nach Induktionsannahme sind v_1, \dots, v_{m-1} linear unabhängig, also folgt

$$\varrho_1 (\lambda_1 - \lambda_m) = \dots = \varrho_{m-1} (\lambda_{m-1} - \lambda_m) = 0 \quad \text{und} \quad \varrho_1 = \dots = \varrho_{m-1} = 0,$$

denn die λ_i sind paarweise verschieden.

Aus Gleichung (*) wird $\varrho_m v_m = \mathbf{o}$; wegen $v_m \neq \mathbf{o}$ folgt schließlich auch $\varrho_m = 0$. ■

Korollar Jede symmetrische reelle 2×2 -Matrix A ist diagonalisierbar.

Beweis Ist $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$, so hatten wir in der Bemerkung aus 4.1.4 gesehen, dass A genau dann verschiedene Eigenwerte hat, wenn

$$D := (a - c)^2 + 4b^2 > 0.$$

Ist $D = 0$, so muss $b = 0$ sein, also ist A schon eine Diagonalmatrix. ■

In 5.3.5 werden wir zeigen, dass die Voraussetzung $n = 2$ überflüssig ist.

4.2.2 Geometrische und algebraische Vielfachheit

Bei dem Beispiel einer nicht diagonalisierbaren Matrix A aus 4.2.1 hat P_A eine doppelte Nullstelle λ , dagegen liegen alle Eigenvektoren auf einer Geraden. Wir werden in diesem Abschnitt zeigen, dass sich auf diese Weise das Hindernis gegen die Diagonalisierbarkeit aufdecken lässt.

Zunächst erinnern wir an die Definition des Eigenraums

$$\text{Eig}(F; \lambda) = \{v \in V : F(v) = \lambda \cdot v\} \subset V$$

eines $F \in \text{End}(V)$ zu $\lambda \in K$, und die in 4.1.1 zusammengestellten Eigenschaften. Aus der Definition folgt sofort, dass

$$\text{Eig}(F; \lambda_1) \cap \text{Eig}(F; \lambda_2) = \{\mathbf{o}\}, \quad \text{falls } \lambda_1 \neq \lambda_2.$$

Weiter sollte man folgendes bedenken:

Bemerkung Sind v_1, v_2 Eigenvektoren zu verschiedenen Eigenwerten λ_1, λ_2 , so ist $v_1 + v_2$ kein Eigenvektor.

Beweis Angenommen es gibt ein $\lambda \in K$, so dass

$$F(v_1 + v_2) = \lambda(v_1 + v_2).$$

Nach Voraussetzung ist $F(v_1) = \lambda_1 v_1$ und $F(v_2) = \lambda_2 v_2$, daraus folgt

$$(\lambda_1 - \lambda)v_1 + (\lambda_2 - \lambda)v_2 = \mathbf{o}.$$

Nach dem Lemma in 4.2.1 muss $\lambda_1 - \lambda = \lambda_2 - \lambda = 0$ sein, das ist wegen $\lambda_1 \neq \lambda_2$ unmöglich. ■

Nun nennt man die Zahl

$$d(F; \lambda) := \dim \text{Eig}(F; \lambda)$$

die **geometrische Vielfachheit** des Eigenwerts λ von F . Dabei ist zu bedenken, dass λ im Fall $d(F; \lambda) = 0$ kein Eigenwert von F ist.

Kurz ausgedrückt: Die geometrische Vielfachheit $d(F; \lambda)$ ist die maximale Zahl linear unabhängiger Eigenvektoren zu $\lambda \in K$.

Im zweiten Schritt betrachten wir das charakteristische Polynom P_F von F . Es gestattet eine Zerlegung

$$P_F = (X - \lambda_1) \cdot \dots \cdot (X - \lambda_m) \cdot Q,$$

wobei $\lambda_1, \dots, \lambda_m \in K$ die Nullstellen von P_F in K sind, und $Q \in K[X]$ keine Nullstellen in K hat. Offensichtlich ist

$$0 \leq m \leq n = \dim V \quad \text{und} \quad m + \deg Q = n.$$

Nun kann es vorkommen, dass P_F mehrfache Nullstellen hat, d.h. die $\lambda_1, \dots, \lambda_m$ müssen nicht alle verschieden sein. Fasst man gleiche Nullstellen zusammen, so erhält man bei passender Nummerierung die neue Zerlegung

$$P_F = (X - \lambda_1)^{r_1} \cdot \dots \cdot (X - \lambda_k)^{r_k} \cdot Q,$$

mit paarweise verschiedenen $\lambda_1, \dots, \lambda_k$, sowie $r_1, \dots, r_k \geq 1$ und $r_1 + \dots + r_k = m$. Die Zahl

$$\mu(P_F; \lambda_i) = r_i \quad \text{für} \quad i = 1, \dots, k$$

ist die Vielfachheit der Nullstelle λ_i von P_F , sie heißt **algebraische Vielfachheit** des Eigenwerts λ_i von F . Ist $P_F(\lambda) \neq 0$, so kann man $\mu(P_F; \lambda) = 0$ setzen. Dann ist

$$0 = d(F; \lambda) = \mu(P_F; \lambda).$$

Entscheidend ist der Zusammenhang zwischen geometrischer und algebraischer Vielfachheit von Eigenwerten.

Lemma Ist $F : V \rightarrow V$ linear, so gilt für jeden Eigenwert λ von F

$$1 \leq d(F; \lambda) \leq \mu(P_F; \lambda) \leq \dim V.$$

Beweis Zur Berechnung des charakteristischen Polynoms benutzen wir eine Basis

$$\mathcal{B} = (v_1, \dots, v_d, v_{d+1}, \dots, v_n) \quad \text{von } V$$

derart, dass (v_1, \dots, v_d) mit $d = d(F; \lambda)$ eine Basis von $\text{Eig}(F; \lambda)$ ist. Nach dem Basis-Ergänzungs-Satz in 2.2.2 ist das möglich. Dann ist nach D8* in 3.2.5

$$\begin{aligned} P_F &= \det(M_{\mathcal{B}}(F) - X \cdot E_n) = \det \left(\begin{array}{c|c} \lambda \cdot E_d - X \cdot E_d & * \\ \hline \mathbf{0} & C - X \cdot E_{n-d} \end{array} \right) \\ &= (\lambda - X)^d \cdot \det(C - X \cdot E_{n-d}). \end{aligned}$$

Daraus folgt $\mu(P_F; \lambda) \geq d$. ■

Dass die Extremwerte angenommen werden können, zeigt das folgende

Beispiel Sei

$$A = \begin{pmatrix} \lambda & 1 & & & 0 \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ 0 & & & & \lambda \end{pmatrix} \in M(n \times n; K)$$

mit $\lambda \in K$ beliebig. Offensichtlich ist

$$P_A = (\lambda - X)^n, \quad \text{also} \quad \mu(P_A; \lambda) = n.$$

Der zu λ gehörige Eigenraum ist bestimmt durch das lineare Gleichungssystem

$$x_2 = 0, x_3 = 0, \dots, x_n = 0.$$

Also ist $\text{Eig}(A; \lambda) = K \cdot e_1$, und $d(A; \lambda) = 1$ für beliebige $\lambda \in K$.

Mit Hilfe des obigen Lemmas können wir nun das zentrale Ergebnis über die Diagonalisierbarkeit beweisen.

Theorem Sei V ein K -Vektorraum mit $\dim V = n < \infty$. Eine lineare Abbildung $F : V \rightarrow V$ ist genau dann **diagonalisierbar**, wenn folgende Bedingungen erfüllt sind:

a) Das charakteristische Polynom P_F zerfällt in $K[X]$ in Linearfaktoren, d.h.

$$P_F = \pm (X - \lambda_1) \cdot \dots \cdot (X - \lambda_n) \quad \text{mit} \quad \lambda_1, \dots, \lambda_n \in K.$$

b) Für jeden Eigenwert λ von F ist $d(F; \lambda) = \mu(P_F; \lambda)$, d.h. die geometrische Vielfachheit ist gleich der algebraischen Vielfachheit.

Beweis Sind $\lambda_1, \dots, \lambda_k$ die paarweise verschiedenen Eigenwerte von F , so setzen wir

$$d_i := d(F; \lambda_i) \quad \text{und} \quad r_i := \mu(P_F; \lambda_i) \quad \text{für} \quad i = 1, \dots, k.$$

Ist F diagonalisierbar, so muss nach der Bemerkung aus 4.2.1 die notwendige Bedingung a) erfüllt sein, daraus folgt sofort

$$r_1 + \dots + r_k = n = \deg P_F. \quad (*)$$

Außerdem gibt es eine Basis aus Eigenvektoren, daraus folgt

$$d_1 + \dots + d_k = n = \dim V. \quad (**)$$

Da weiter nach dem obigen Lemma $d_i \leq r_i$ für alle i ist, folgt $d_i = r_i$ aus (*) und (**).

Zum Nachweis der umgekehrten Richtung müssen wir eine Basis von V aus Eigenvektoren angeben. Dazu wählen wir zu jedem $i \in \{1, \dots, k\}$ eine Basis

$$\left(v_1^{(i)}, \dots, v_{d_i}^{(i)} \right) \quad \text{von} \quad \text{Eig}(F; \lambda_i).$$

Nach den Voraussetzungen b) und a) ist

$$d_1 + \dots + d_k = r_1 + \dots + r_k = n = \dim V.$$

Also genügt es zu zeigen, dass all diese n Vektoren $v_j^{(i)}$ zusammen linear unabhängig sind. Sei also für $i = 1, \dots, k$ mit $q_1^{(i)}, \dots, q_{d_i}^{(i)} \in K$

$$w_i := q_1^{(i)} v_1^{(i)} + \dots + q_{d_i}^{(i)} v_{d_i}^{(i)} \quad \text{und} \quad w_1 + \dots + w_k = \mathbf{o}.$$

Es ist zu zeigen, dass $w_1 = \dots = w_k = \mathbf{o}$, dann folgt aus $w_i = \mathbf{o}$, dass alle Koeffizienten $q_j^{(i)}$ verschwinden. Angenommen einige der w_i wären nicht Null, etwa w_1, \dots, w_l mit $1 \leq l \leq k$. Dann sind diese $w_i \neq \mathbf{o}$ Eigenvektoren zu den paarweise verschiedenen Eigenwerten $\lambda_1, \dots, \lambda_l$. Nach dem Lemma aus 4.2.1 sind sie linear unabhängig, das ist ein Widerspruch zu $w_1 + \dots + w_l = \mathbf{o}$. ■

Aus der Sicht dieses Theorems ist der Satz aus 4.2.1 ganz klar: Bei n verschiedenen Eigenwerten ist $r_1 = \dots = r_n = 1$, wegen $1 \leq d_i \leq r_i$ folgt $d_i = r_i$.

Man kann dieses Theorem noch etwas anders formulieren, indem man den Begriff der direkten Summen und den Satz aus 2.2.5 verwendet.

Korollar *Eine lineare Abbildung $F : V \rightarrow V$ ist genau dann diagonalisierbar, wenn*

$$V = \text{Eig}(F; \lambda_1) \oplus \dots \oplus \text{Eig}(F; \lambda_k),$$

wobei $\lambda_1, \dots, \lambda_k$ die verschiedenen Eigenwerte von F sind. ■

Damit diese Darstellung als direkte Summe möglich ist, muss es genügend viele Eigenwerte geben, und die Eigenräume dazu müssen die maximal mögliche Dimension haben. Man beachte, dass es außerhalb der k Eigenräume von F keine weiteren Eigenvektoren gibt, das sieht man wie in obiger Bemerkung.

4.2.3 Rechenverfahren zur Diagonalisierung

In diesem Abschnitt wollen wir die Diagonalisierung eines Endomorphismus aus der Sicht des Matrizen-Kalküls betrachten. Wir beginnen mit einer diagonalisierbaren Matrix $A \in M(n \times n; K)$. Dazu gibt es eine Diagonalmatrix D mit den Eigenwerten $\lambda_1, \dots, \lambda_n$ von A in der Diagonalen und eine Matrix $S \in GL(n; K)$ derart, dass das Diagramm

$$\begin{array}{ccc} K^n & \xrightarrow{A} & K^n \\ S \downarrow & & \downarrow S \\ K^n & \xrightarrow{D} & K^n \end{array}$$

kommutiert, d.h. $D = S \cdot A \cdot S^{-1}$. Die Matrix S ist dadurch festgelegt, dass für eine Basis $\mathcal{B} = (v_1, \dots, v_n)$ aus Eigenvektoren von A

$$S \cdot v_i = e_i, \quad \text{also} \quad v_i = S^{-1} \cdot e_i.$$

Man kann also eine derartige (nicht eindeutig bestimmte) Matrix S^{-1} berechnen, indem man eine zuvor bestimmte Basis aus Eigenvektoren als Spalten einträgt. In Koordinaten aufgeschrieben bedeutet das:

Ist $v_i = {}^t(c_{1i}, \dots, c_{ni}) \in K^n$ Eigenvektor von A , so ist

$$S = \begin{pmatrix} c_{11} & \dots & c_{1n} \\ \vdots & & \vdots \\ c_{n1} & \dots & c_{nn} \end{pmatrix}^{-1} \quad \text{und} \quad S \cdot A \cdot S^{-1} = D = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

Für einen Endomorphismus F eines Vektorraums V wählt man eine beliebige Basis \mathcal{A} von V . F ist genau dann diagonalisierbar, wenn $A := M_{\mathcal{A}}(F)$ diagonalisierbar ist. In diesem Fall erhält man ein kommutatives Diagramm

$$\begin{array}{ccccc}
 K^n & \xrightarrow{A} & K^n & & \\
 \downarrow S & \searrow \Phi_A & & \swarrow \Phi_A & \downarrow S \\
 & & V & \xrightarrow{F} & V \\
 & \swarrow \Phi_B & & \searrow \Phi_B & \\
 K^n & \xrightarrow{D} & K^n & &
 \end{array}$$

Dabei werden D und S wie oben aus A erhalten, und die Eigenvektoren von F aus der Basis $\mathcal{B} = (v_1, \dots, v_n)$ sind durch

$$v_i = \Phi_{\mathcal{A}}(S^{-1} \cdot e_i)$$

bestimmt. Anders ausgedrückt: Die Spalten von S^{-1} sind die Koordinaten der v_i bezüglich der zu Beginn vorgegebenen Basis \mathcal{A} .

Beispiel Um nicht viel rechnen zu müssen, betrachten wir die recht einfache Matrix

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 3 & 5 & -3 \\ 6 & 6 & -4 \end{pmatrix} \in M(3 \times 3; \mathbb{R}).$$

Das charakteristische Polynom ist

$$P_A = -(X-2) \cdot (X^2 - X - 2) = -(X-2)^2 \cdot (X+1).$$

Daraus folgt für die algebraischen Vielfachheiten

$$\mu(P_A; -1) = 1 \quad \text{und} \quad \mu(P_A; 2) = 2.$$

Den Eigenraum zu $\lambda_1 = -1$ erhält man als Lösungsraum des Gleichungssystems

$$\begin{array}{rcl}
 3x_1 & & = 0 \\
 3x_1 + 6x_2 - 3x_3 & = & 0 \\
 6x_1 + 6x_2 - 3x_3 & = & 0
 \end{array}$$

vom Rang 2, ein Eigenvektor dazu ist $v_1 = {}^t(0, 1, 2)$, also folgt

$$\text{Eig}(A; -1) = \mathbb{R} \cdot v_1.$$

Zu $\lambda_2 = 2$ erhält man das Gleichungssystem

$$\begin{array}{rcl}
 3x_1 + 3x_2 - 3x_3 & = & 0 \\
 6x_1 + 6x_2 - 6x_3 & = & 0
 \end{array}$$

vom Rang 1. Linear unabhängige Eigenvektoren dazu sind

$$v_2 = {}^t(1,0,1) \quad \text{und} \quad v_3 = {}^t(-1,1,0);$$

$$\text{Eig}(A;2) = \mathbb{R} \cdot v_2 + \mathbb{R} \cdot v_3.$$

Also ist A diagonalisierbar, und man erhält

$$S^{-1} = \begin{pmatrix} 0 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{pmatrix}, \quad S = \begin{pmatrix} -1 & -1 & 1 \\ 2 & 2 & -1 \\ 1 & 2 & -1 \end{pmatrix}, \quad S \cdot A \cdot S^{-1} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Man beachte wieder, dass S nicht eindeutig bestimmt ist. Verwendet man zum Eigenwert $\lambda_2 = 2$ die Eigenvektoren

$$w_1 = {}^t(2,0,2) \quad \text{und} \quad w_2 = {}^t(1,-1,0),$$

und zu $\lambda_1 = -1$ den Eigenvektor $w_3 = {}^t(0, \frac{1}{2}, 1)$, so erhält man

$$T \cdot A \cdot T^{-1} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -1 \end{pmatrix} \quad \text{mit} \quad T^{-1} = \begin{pmatrix} 2 & 1 & 0 \\ 0 & -1 & \frac{1}{2} \\ 2 & 0 & 1 \end{pmatrix} \quad \text{und} \quad T = \begin{pmatrix} 1 & 1 & -\frac{1}{2} \\ -1 & -2 & 1 \\ -2 & -2 & 2 \end{pmatrix}.$$

4.2.4 Trigonalisierung*

Wie wir in 4.2.3 gesehen hatten, gibt es vom Körper K unabhängige Hindernisse gegen die Diagonalisierbarkeit eines Endomorphismus oder einer Matrix. In diesem Abschnitt wollen wir untersuchen, wann sich statt einer Diagonalmatrix wenigstens eine Dreiecksmatrix erreichen lässt. Das ist nützlich für viele Anwendungen, etwa bei Systemen linearer Differentialgleichungen mit konstanten Koeffizienten (vgl. etwa [FO₂, §14]).

Zunächst wollen wir das Problem präzise formulieren: Gegeben sei ein Endomorphismus F eines endlich-dimensionalen Vektorraums V . Gesucht ist eine Basis \mathcal{B} von V derart, dass die darstellende Matrix $D = M_{\mathcal{B}}(F)$ eine obere Dreiecksmatrix ist, also

$$D = (d_{ij}) \quad \text{mit} \quad d_{ij} = 0 \quad \text{für} \quad i > j.$$

Nach der Transformationsformel aus 2.5.2 bedeutet das für eine Matrix $A \in M(n \times n; K)$ die Existenz einer Matrix $S \in GL(n; K)$ derart, dass

$$S \cdot A \cdot S^{-1} = D$$

eine obere Dreiecksmatrix ist.

Zunächst wollen wir überlegen, was die Existenz einer darstellenden Dreiecksmatrix für die geometrischen Eigenschaften eines Endomorphismus bedeutet. Sei also $\dim V = n$, $F \in \text{End}(V)$ und $\mathcal{B} = (v_1, \dots, v_n)$ eine Basis von V derart, dass

$$M_{\mathcal{B}}(F) = \begin{pmatrix} d_{11} & \cdots & d_{1n} \\ & \ddots & \vdots \\ 0 & & d_{nn} \end{pmatrix}.$$

Das bedeutet für die Bilder der Basisvektoren

$$F(v_1) = d_{11}v_1, \dots, F(v_n) = d_{1n}v_1 + \dots + d_{nn}v_n, \quad \text{allgemein} \quad F(v_k) = \sum_{i=1}^k d_{ik}v_i.$$

Definieren wir in V für $k = 0, \dots, n$ die Untervektorräume

$$V_k := \text{Span}(v_1, \dots, v_k), \quad \text{so folgt}$$

$\{\mathbf{o}\} = V_0 \subset V_1 \subset \dots \subset V_n = V$, $\dim V_k = k$ und $F(V_k) \subset V_k$. In einer solchen Situation sind folgende Bezeichnungen üblich

Definition Ist $F : V \rightarrow V$ ein Endomorphismus, so heißt ein Untervektorraum $W \subset V$ **F -invariant**, wenn

$$F(W) \subset W.$$

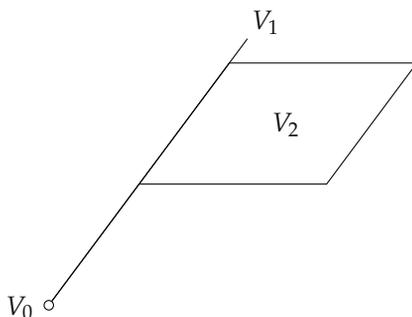
Eine Kette $V_0 \subset V_1 \subset \dots \subset V_n \subset V$ von Untervektorräumen eines Vektorraums V mit $\dim V = n$ heißt **Fahne**, wenn

$$\dim V_k = k \quad \text{für} \quad k = 0, \dots, n.$$

Eine Fahne heißt **F -invariant**, wenn

$$F(V_k) \subset V_k \quad \text{für} \quad k = 0, \dots, n.$$

Der Name „Fahne“ ist wohl auf folgendes Bild zurückzuführen:



Lemma Für einen Endomorphismus F von V sind folgende Bedingungen äquivalent:

- i) Es gibt eine Basis \mathcal{B} von V derart, dass $M_{\mathcal{B}}(F)$ eine obere Dreiecksmatrix ist.
- ii) Es gibt in V eine F -invariante Fahne.

Beweis i) \Rightarrow ii) haben wir schon oben gezeigt.

ii) \Rightarrow i): Wir beginnen mit einem Vektor $\mathbf{o} \neq v_1 \in V_1$ und ergänzen ihn nach dem Basis-Ergänzungssatz aus 2.2.2 zu einer Basis (v_1, v_2) von V_2 . Das Verfahren wird fortgesetzt bis zu einer Ergänzung einer Basis

$$(v_1, \dots, v_{n-1}) \text{ von } V_{n-1} \text{ zu einer Basis } \mathcal{B} = (v_1, \dots, v_n) \text{ von } V.$$

Ist $M_{\mathcal{B}}(F) = (d_{ij})$, so folgt

$$d_{i1} = 0 \quad \text{für } i \geq 2 \quad \text{aus } F(V_1) \subset V_1,$$

und weiter – Schritt für Schritt – für $k = 2, \dots, n$

$$d_{ik} = 0 \quad \text{für } i \geq k + 1 \quad \text{aus } F(V_k) \subset V_k.$$

Also ist $M_{\mathcal{B}}(F)$ eine obere Dreiecksmatrix. ■

Nach diesen Vorbereitungen die grundlegende

Definition Ein Endomorphismus F eines endlich-dimensionalen K -Vektorraums V heißt **trigonalisierbar**, wenn er die äquivalenten Bedingungen des obigen Lemmas erfüllt.

Nach diesen vorbereitenden geometrischen Erläuterungen das zentrale Ergebnis:

Theorem Sei V ein K -Vektorraum, $\dim V = n$ und $F \in \text{End}(V)$. Dann gilt: F ist genau dann trigonalisierbar, wenn das charakteristische Polynom P_F in Linearfaktoren zerfällt, d.h.

$$P_F = \pm(X - \lambda_1) \cdot \dots \cdot (X - \lambda_n) \quad \text{mit } \lambda_1, \dots, \lambda_n \in K.$$

Aus dem Fundamentalsatz der Algebra in 1.4.6 folgt sofort das wichtige

Korollar Jeder Endomorphismus eines endlich-dimensionalen \mathbb{C} -Vektorraums ist trigonalisierbar. ■

Beweis des Theorems Wir verwenden die Bedingung i) des obigen Lemmas. Ist F trigonalisierbar, so gibt es eine Basis \mathcal{B} von F derart, dass $M_{\mathcal{B}}(F) = D = (d_{ij})$ eine obere Dreiecksmatrix ist. Daraus folgt nach D6* aus 3.2.5

$$P_F = \det \begin{pmatrix} d_{11} - X & \cdots & d_{1n} \\ & \ddots & \\ 0 & & d_{nn} - X \end{pmatrix} = (d_{11} - X) \cdot \dots \cdot (d_{nn} - X).$$

Also zerfällt P_F in Linearfaktoren.

Die umgekehrte Richtung ist schwieriger, wir führen Induktion über $n = \dim V$. Für $n = 0$ ist nichts zu beweisen; für $n = 1$ ist jede Matrix Dreiecksmatrix.

Sei also $n > 1$, und die Aussage für $n - 1$ schon bewiesen. Zum Eigenwert λ_1 wählen wir einen Eigenvektor $\mathbf{o} \neq v_1 \in V$, und wir setzen

$$V_1 := K \cdot v_1 \subset V.$$

Nach dem Basis-Ergänzungssatz aus 2.2.2 gibt es eine Basis $\mathcal{B} = (v_1, w_2, \dots, w_n)$ von V . Wir setzen

$$\mathcal{B}' = (w_2, \dots, w_n) \quad \text{und} \quad W := \text{Span}(\mathcal{B}').$$

Dann ist offensichtlich $V = V_1 \oplus W$ eine direkte Summe (vgl. 2.2.5) und $\dim W = n - 1$. Entscheidendes Problem ist nun, dass W nicht F -invariant sein muss. Um die Induktionsannahme anwenden zu können, betrachten wir die Beschränkung $F|_W$ von F auf W , das ist eine lineare Abbildung

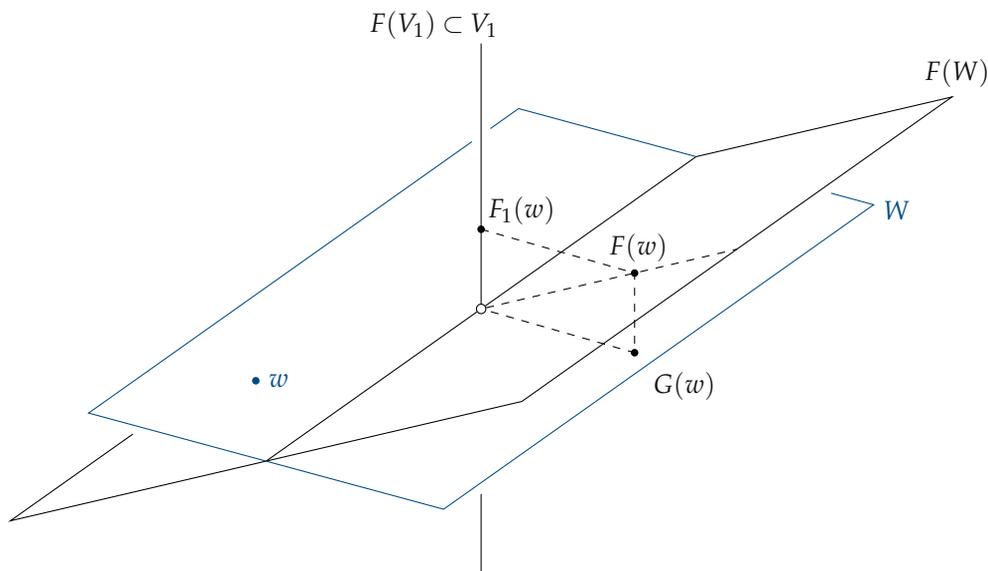
$$F|_W: W \rightarrow V.$$

Um daraus einen Endomorphismus von W zu erhalten, benutzen wir für jedes $w \in W$ die eindeutige Zerlegung des Bildes

$$F(w) = F_1(w) + G(w) \in V_1 \oplus W = V.$$

Auf diese Weise erhalten wir aus $F|_W$ zwei lineare Abbildungen

$$F_1: W \rightarrow V_1 \quad \text{und} \quad G: W \rightarrow W.$$



Das Ganze kann man durch die darstellenden Matrizen beschreiben:

$$M_{\mathcal{B}}(F) = \left(\begin{array}{c|ccc} \lambda_1 & & & \\ 0 & & & \\ \vdots & & & \\ 0 & & & \end{array} \middle| M_{\mathcal{B}'}^{B'}(F|W) \right) = \left(\begin{array}{c|ccc} \lambda_1 & b_{12} & \cdots & b_{1n} \\ 0 & & & \\ \vdots & & & \\ 0 & & & \end{array} \middle| M_{\mathcal{B}'}(G) \right).$$

Dabei ist $F_1(w_j) = b_{1j} \cdot v_1$ für $j = 2, \dots, n$. Für die charakteristischen Polynome gilt nach den Rechenregeln für Determinanten (D8* aus 3.2.5)

$$P_F = \pm(X - \lambda_1) \cdot P_G, \quad \text{also} \quad P_G = \pm(X - \lambda_2) \cdot \dots \cdot (X - \lambda_n).$$

Da $\dim W = n - 1$, können wir die Induktionsannahme auf G anwenden. Danach gibt es eine Basis $\mathcal{B}'' = (v_2, \dots, v_n)$ von W derart, dass $M_{\mathcal{B}''}(G)$ eine obere Dreiecksmatrix ist. Außerdem ist

$$\mathcal{A} = (v_1, v_2, \dots, v_n)$$

eine Basis von W , und somit ist auch

$$M_{\mathcal{A}}(F) = \left(\begin{array}{c|ccc} \lambda_1 & & & * \\ 0 & & & \\ \vdots & & & \\ 0 & & & \end{array} \middle| M_{\mathcal{B}''}(G) \right)$$

eine obere Dreiecksmatrix



Es gibt elegantere und abstraktere Beweise des Trigonalisierungs-Theorems, aber der gerade durchgeführte elementare Beweis durch Induktion ergibt auch eine Anleitung zur schrittweisen expliziten Berechnung der Trigonalisierung. Für die nötigen Basis-Ergänzungen kann man das Rezept aus 2.2.4 benutzen.

Beispiel Sei $F : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ beschrieben durch die Matrix

$$A = \begin{pmatrix} 3 & 2 & -1 \\ 2 & 4 & -1 \\ 5 & 6 & -1 \end{pmatrix}.$$

Zunächst berechnet man

$$P_F = -(X^3 - 6X^2 + 12X - 8) = -(X - 2)^3.$$

Also ist $\lambda = 2$ der einzige Eigenwert mit $\mu(P_F; 2) = 3$. Zur Bestimmung von $\text{Eig}(F; 2)$ hat man das homogene lineare Gleichungssystem mit der Koeffizientenmatrix

$$A - 2 \cdot E_3 = \begin{pmatrix} 1 & 2 & -1 \\ 2 & 2 & -1 \\ 5 & 6 & -3 \end{pmatrix}$$

zu lösen. Es hat den Rang 2 und es folgt

$$\text{Eig}(F;2) = \mathbb{R} \cdot v_1 =: V_1 \quad \text{mit} \quad v_1 = {}^t(0,1,2).$$

Also ist F nicht diagonalisierbar. Eine Zerlegung $\mathbb{R}^3 = V_1 \oplus W$ erhält man zum Beispiel mit

$$W := \text{Span}(w_2, w_3), \quad \text{wenn} \quad w_2 := e_1 \quad \text{und} \quad w_3 := e_2.$$

Um $M_{\mathcal{B}}(F)$ bezüglich der Basis $\mathcal{B} := (v_1, w_2, w_3)$ zu bestimmen, berechnet man

$$\begin{aligned} F(v_1) &= 2v_1, \\ F(w_2) &= {}^t(3,2,5) = \frac{5}{2}v_1 + 3w_2 - \frac{1}{2}w_3, \\ F(w_3) &= {}^t(2,4,6) = 3v_1 + 2w_2 + w_3. \end{aligned}$$

Daraus folgt

$$M_{\mathcal{B}}(F) = \begin{pmatrix} 2 & \frac{5}{2} & 3 \\ 0 & 3 & 2 \\ 0 & -\frac{1}{2} & 1 \end{pmatrix}.$$

Im zweiten Schritt betrachten wir die aus F entstandene Abbildung $G : W \rightarrow W$. Ist $\mathcal{B}' := (w_2, w_3)$, so folgt

$$M_{\mathcal{B}'}(G) = \begin{pmatrix} 3 & 2 \\ -\frac{1}{2} & 1 \end{pmatrix} =: B.$$

Nun berechnet man $P_G = \det(B - X \cdot E_2) = (X - 2)^2$ und

$$\text{Eig}(G;2) = \mathbb{R} \cdot v_2 \quad \text{mit} \quad v_2 := {}^t(2, -1, 0) \in W \subset \mathbb{R}^3.$$

Im dritten Schritt betrachten wir die Basis

$$\mathcal{A} := (v_1, v_2, v_3) \quad \text{mit} \quad v_3 := w_3 = e_2.$$

Dann ist eine F -invariante Fahne im \mathbb{R}^3 gegeben durch

$$\{\mathbf{o}\} = V_0 \subset \text{Span}(v_1) \subset \text{Span}(v_1, v_2) \subset \text{Span}(v_1, v_2, v_3) = \mathbb{R}^3.$$

Trägt man die Basis \mathcal{A} als Spalten in eine Matrix ein, so erhält man

$$\begin{aligned} S^{-1} &= \begin{pmatrix} 0 & 2 & 0 \\ 1 & -1 & 1 \\ 2 & 0 & 0 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & 0 \\ \frac{1}{2} & 1 & -\frac{1}{2} \end{pmatrix} \quad \text{und} \\ M_{\mathcal{A}}(F) &= S \cdot A \cdot S^{-1} = \begin{pmatrix} 2 & 2 & 3 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix} =: D. \end{aligned}$$

Das ist eine obere Dreiecksmatrix mit den Eigenwerten in der Diagonalen.

Die F -invariante Fahne und damit auch die Transformationsmatrix S , sowie die Dreiecksmatrix D , sind keinesfalls eindeutig bestimmt. Wählt man etwa die Basisvektoren

$$v'_1 = v_1 = {}^t(0,1,2), v'_2 = {}^t(1,0,1) \text{ und } v'_3 = {}^t(-1,1,0),$$

so ist durch $V'_1 = \text{Span}(v'_1)$, $V'_2 = \text{Span}(v'_1, v'_2)$ und $V'_3 = (v'_1, v'_2, v'_3)$ eine F -invariante Fahne gegeben, und für

$$T^{-1} := \begin{pmatrix} 0 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{pmatrix} \text{ ist } T = \begin{pmatrix} -1 & -1 & 1 \\ 2 & 2 & -1 \\ 1 & 2 & -1 \end{pmatrix} \text{ und } T \cdot A \cdot T^{-1} = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

Wie man auf die besonders einfache Form dieser letzten Dreiecksmatrix kommt, wird in den folgenden Abschnitten erläutert.

4.2.5 Zerlegung in Haupträume*

Wie wir in 4.2.4 gesehen hatten, kann man jeden Endomorphismus, dessen charakteristisches Polynom in Linearfaktoren zerfällt, bezüglich einer geeigneten Basis durch eine obere Dreiecksmatrix

$$A = \begin{pmatrix} \lambda_1 & a_{12} & \cdots & a_{1n} \\ 0 & \lambda_2 & & \vdots \\ \vdots & & \ddots & a_{n-1,n} \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix}$$

beschreiben. Der Beweis war recht elementar gewesen, aber das Ergebnis ist für viele Anwendungen verbesserungsbedürftig. In der Diagonalen von A müssen die Eigenwerte stehen, daran ist nicht zu rütteln. Aber was oberhalb der Diagonalen steht, kann vereinfacht werden. Setzen wir

$$D := \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \text{ und } N := \begin{pmatrix} 0 & a_{12} & \cdots & a_{1n} \\ 0 & 0 & & \vdots \\ \vdots & & \ddots & a_{n-1,n} \\ 0 & \cdots & 0 & 0 \end{pmatrix},$$

so ist $A = D + N$, wobei D eine Diagonalmatrix ist. Berechnet man die Potenzen N^k von N , so folgt leicht aus den Regeln für die Multiplikation von Matrizen, dass $N^k = \mathbf{o}$ für $k \geq n$. Allgemein nennt man eine quadratische Matrix B **nilpotent**, wenn es ein $k \in \mathbb{N}^*$ gibt, so dass

$$B^k = \mathbf{o}.$$

Dem entsprechend heißt ein Endomorphismus F **nilpotent**, wenn es ein $k \in \mathbb{N}^*$ gibt derart, dass $F^k = \mathbf{o}$.

Etwa bei der Lösung von Systemen linearer Differentialgleichungen ist es möglich, für eine quadratische Matrix A die Matrix

$$\exp A := \sum_{k=0}^{\infty} \frac{1}{k!} A^k$$

zu verwenden. Zur Berechnung von A^k kann man versuchen, eine Zerlegung $A = D + N$ zu verwenden. Dann ist etwa

$$A^2 = (D + N) \cdot (D + N) = D^2 + D \cdot N + N \cdot D + N^2.$$

Das bringt nur dann eine Vereinfachung, wenn $D \cdot N = N \cdot D$. Nehmen wir als Beispiel

$$A = \begin{pmatrix} \lambda_1 & 1 \\ 0 & \lambda_2 \end{pmatrix}, \quad \text{so ist } D \cdot N = \begin{pmatrix} 0 & \lambda_1 \\ 0 & 0 \end{pmatrix} \quad \text{und} \quad N \cdot D = \begin{pmatrix} 0 & \lambda_2 \\ 0 & 0 \end{pmatrix},$$

also $D \cdot N = N \cdot D$ genau dann, wenn $\lambda_1 = \lambda_2$.

In diesem Abschnitt geben wir eine Methode an, wie man den nilpotenten Anteil N von A so vereinfachen kann, dass insbesondere D und N kommutieren. Der Schlüssel zum Erfolg ist eine Verallgemeinerung der Eigenräume eines Endomorphismus.

Sei also F Endomorphismus eines K -Vektorraums V mit $\dim V = n < \infty$. Für jeden Eigenwert λ von F war der Eigenraum erklärt als

$$\text{Eig}(F; \lambda) = \text{Ker}(F - \lambda \cdot \text{id}_V) \subset V.$$

In jedem Fall gilt $\dim \text{Eig}(F; \lambda) \leq \mu(P_F; \lambda) =: r$, und F ist genau dann diagonalisierbar, wenn P_F in Linearfaktoren zerfällt, und für jeden Eigenwert λ die obige Ungleichung eine Gleichung ist. Wenn das für ein λ nicht der Fall ist, kann man versuchen den Eigenraum durch eine Verallgemeinerung zu vergrößern. Ist $G := F - \lambda \cdot \text{id}_V$, so gilt für die Potenzen von G offensichtlich

$$\text{Ker } G \subset \text{Ker } G^2 \subset \dots \subset \text{Ker } G^r.$$

Es wird sich nun zeigen, dass die Definition eines verallgemeinerten Eigenraums, oder kurz eines **Hauptraums**

$$\text{Hau}(F; \lambda) := \text{Ker}(F - \lambda \cdot \text{id}_V)^r$$

von F zum Eigenwert λ mit $r := \mu(P_F; \lambda)$, erfolgreich ist.

Satz über die Zerlegung in Haupträume Gegeben sei ein Endomorphismus F eines K -Vektorraums V mit $\dim V < \infty$ derart, dass

$$P_F = \pm (X - \lambda_1)^{r_1} \cdot \dots \cdot (X - \lambda_k)^{r_k}, \quad \text{wobei } \lambda_1, \dots, \lambda_k \in K$$

die paarweise verschiedenen Nullstellen von P_F sind. Dann gilt:

a) $1 \leq \dim \text{Eig}(F; \lambda_i) \leq \dim \text{Hau}(F; \lambda_i) = r_i$ für $i = 1, \dots, k$.

- b) $V = \text{Hau}(F; \lambda_1) \oplus \dots \oplus \text{Hau}(F; \lambda_k)$.
 c) Die Haupträume $\text{Hau}(F; \lambda_i)$ sind F -invariant.
 d) F hat eine Zerlegung $F = F_D + F_N$, wobei F_D diagonalisierbar und F_N nilpotent ist; weiter gilt $F_D \circ F_N = F_N \circ F_D$. Insbesondere gibt es eine Basis \mathcal{B} von V derart, dass

$$M_{\mathcal{B}}(F) = \begin{pmatrix} \boxed{\lambda_1 E_{r_1} + N_1} & & 0 \\ & \ddots & \\ 0 & & \boxed{\lambda_k E_{r_k} + N_k} \end{pmatrix},$$

wobei die Matrix $N_i \in M(r_i \times r_i; K)$ für $i = 1, \dots, k$ nilpotent ist. Insgesamt ist

$$M_{\mathcal{B}}(F) = D + N, \quad \text{mit} \quad D \cdot N = N \cdot D,$$

wobei D Diagonalmatrix und N nilpotent ist.

Zur Vorbereitung des Beweises des obigen Satzes betrachten wir einen Eigenwert $\lambda = \lambda_1$ von F der Vielfachheit $r = r_1$, und setzen $G := F - \lambda \cdot \text{id}_V$. Es folgt

$$P_G = \pm X^r \cdot (X - \varrho_2) \cdot \dots \cdot (X - \varrho_k) \quad \text{mit} \quad \varrho_i = \lambda_i - \lambda_1 \neq 0.$$

Also ist $\mu(P_G; 0) = r$. Da $\text{Hau}(F; \lambda) = \text{Hau}(G; 0) = \text{Ker } G^r$, ist es angebracht, die Kerne $\text{Ker } G^j$ und die Bilder $\text{Im } G^j := G^j(V)$ zu betrachten. Man hat die Ketten

$$\begin{aligned} \{\mathbf{0}\} &\subset \text{Ker } G \subset \text{Ker } G^2 \subset \dots \subset \text{Ker } G^j \subset \dots \subset V, \\ V &\supset \text{Im } G \supset \text{Im } G^2 \supset \dots \supset \text{Im } G^j \supset \dots \supset \{\mathbf{0}\}, \end{aligned}$$

denn aus $G^j(v) = \mathbf{0}$ folgt $G^{j+1}(v) = G(G^j(v)) = G(\mathbf{0}) = \mathbf{0}$ und aus $w = G^{j+1}(v)$ folgt $w = G^j(G(v))$. Da $\dim V < \infty$, müssen die beiden Ketten stationär werden, d.h. es gibt minimale s_1 und s_2 mit

$$\text{Ker } G^{s_1+1} = \text{Ker } G^{s_1} \quad \text{und} \quad \text{Im } G^{s_2+1} = \text{Im } G^{s_2}.$$

In dieser Situation gilt ein

Lemma von FITTING

- a) $s_1 = s_2 =: s$ und $\text{Ker } G^{s+i} = \text{Ker } G^s$, $\text{Im } G^{s+i} = \text{Im } G^s$ für alle $i \in \mathbb{N}$.
 b) Die Räume $\text{Ker } G^s \subset V$ und $\text{Im } G^s \subset V$ sind G -invariant.
 c) $(G|_{\text{Ker } G^s})^s = \mathbf{0}$ und $G|_{\text{Im } G^s}$ ist ein Isomorphismus.
 d) $V = \text{Ker } G^s \oplus \text{Im } G^s$.
 e) $s \leq r = \mu(P_G; 0)$ und $\text{Ker } G^s = \text{Ker } G^r = \text{Hau}(G; 0)$.

Aus Teil e) ist ersichtlich, dass man bei der Bestimmung des Hauptraums schon mit der Potenz $s \leq r$ auskommt. Dass $s < r$ sein kann, sieht man etwa an dem Beispiel

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{mit } s = 2 \quad \text{und } r = 3.$$

Beweis des Lemmas Für beliebiges j betrachten wir das Diagramm

$$\begin{array}{ccccc} \text{Ker } G^j & \xrightarrow{\subset} & V & \xrightarrow{G^j} & \text{Im } G^j \\ \downarrow \cap & & \parallel & & \uparrow \cup \\ \text{Ker } G^{j+1} & \xrightarrow{\subset} & V & \xrightarrow{G^{j+1}} & \text{Im } G^{j+1} \end{array}$$

Nach der Dimensionsformel aus 2.3.4 ist

$$\dim \text{Ker } G^j + \dim \text{Im } G^j = \dim V = \dim \text{Ker } G^{j+1} + \dim \text{Im } G^{j+1}.$$

Daraus folgt $\text{Ker } G^{j+1} = \text{Ker } G^j \Leftrightarrow \text{Im } G^{j+1} = \text{Im } G^j$, also $s_1 = s_2$.

Weiter hat man für beliebiges j eine Einschränkung $G|_{\text{Im } G^j} : \text{Im } G^j \rightarrow \text{Im } G^{j+1}$, die surjektiv ist. Also ist $G|_{\text{Im } G^s}$ ein Isomorphismus, daraus folgt

$$\text{Im } G^{s+i} = \text{Im } G^s \quad \text{und somit} \quad \text{Ker } G^{s+i} = \text{Ker } G^s.$$

Ad b) Ist $v \in \text{Ker } G^s$, so ist $G^s(v) = \mathbf{o}$, also auch $G^s(G(v)) = G(G^s(v)) = \mathbf{o}$.

Ist $v \in \text{Im } G^s$, so ist $v = G^s(w)$, also $G(v) = G(G^s(w))$.

Ad c) $G^s(v) = \mathbf{o}$, falls $v \in \text{Ker } G^s$. Die zweite Aussage wurde schon unter a) gezeigt.

Ad d) Da $\dim \text{Ker } G^s + \dim \text{Im } G^s = \dim V$, genügt es nach 2.2.5 zu zeigen, dass

$$\text{Ker } G^s \cap \text{Im } G^s = \{\mathbf{o}\}.$$

Ist $v \in \text{Ker } G^s \cap \text{Im } G^s$, so ist $G^s(v) = \mathbf{o}$ und $v = G^s(w)$ für ein $w \in V$. Also folgt

$$\mathbf{o} = G^s(v) = G^{2s}(w), \quad w \in \text{Ker } G^{2s} = \text{Ker } G^s \quad \text{und} \quad v = G^s(w) = \mathbf{o}.$$

Ad e) Ist $U := \text{Ker } G^s$ und $W := \text{Im } G^s$, so folgt wegen d), dass

$$P_G = P_{G|U} \cdot P_{G|W} = X^r \cdot Q \quad \text{mit} \quad Q(0) \neq 0.$$

Da $G|_W$ ein Isomorphismus ist, muss $P_{G|W}(0) \neq 0$ sein, daher ist X^r ein Teiler von $P_{G|U}$. Da $(G|_U)^s = \mathbf{o}$, ist $G|_U$ nilpotent, also kann $P_{G|U}$ keine von Null verschiedene Nullstelle haben, damit ist $P_{G|U} = \pm X^r$ und $\dim U = r$. Die Ungleichung $s \leq r$ folgt aus einer allgemeinen Eigenschaft nilpotenter Endomorphismen (Bemerkung in 4.2.6), wenn wir noch $(G|_U)^{s-1} \neq \mathbf{o}$ gezeigt haben. Das ist aber klar, denn aus $(G|_U)^{s-1} = \mathbf{o}$ würde folgen, dass $U = \text{Ker } G^s \subset \text{Ker } G^{s-1}$, im Widerspruch zu $\text{Ker } G^{s-1} \subsetneq \text{Ker } G^s$. ■

Beweis des Satzes über die Zerlegung in Haupträume Wir führen Induktion über die Zahl $k \geq 1$ der verschiedenen Eigenwerte. Zu λ_1 definieren wir $G := F - \lambda_1 \cdot id_V$. Dann ist wie schon beim Lemma von FITTING bemerkt

$$\mu(P_F; \lambda_1) = \mu(P_G; 0) = r_1 \quad \text{und} \quad \text{Hau}(F; \lambda_1) = \text{Hau}(G; 0) = \text{Ker } G^s = \text{Ker } G^{r_1}.$$

Weiter hat man nach dem Lemma eine Zerlegung

$$V = U \oplus W \quad \text{mit} \quad U = \text{Hau}(F; \lambda_1) \quad \text{und} \quad W = \text{Im } G^{r_1}.$$

Die beiden Summanden sind G -invariant, also wegen $F = G + \lambda_1 \cdot id_V$ auch F -invariant. Im Fall $k = 1$ ist $U = V$, also G nilpotent; damit ist der Induktionsanfang erledigt. Für den Induktionsschluss betrachten wir $F|_W$. Da

$$P_{F|_W} = \pm (X - \lambda_2)^{r_2} \cdots (X - \lambda_k)^{r_k},$$

können wir die Induktionsannahme auf $F|_W$ anwenden:

$$W = \text{Hau}(F|_W; \lambda_2) \oplus \dots \oplus \text{Hau}(F|_W; \lambda_k),$$

damit sind die Aussagen a), b) und c) bewiesen. Zum Beweis von Aussage d) betrachten wir zunächst einen Eigenwert λ_i und den zugehörigen Hauptraum

$$U_i := \text{Hau}(F; \lambda_i) \quad \text{und} \quad G_i := F - \lambda_i \cdot id_V.$$

Dann ist $F|_{U_i} = G_i|_{U_i} + \lambda_i \cdot id_{U_i}$, und da nach dem Lemma von FITTING $(G|_{U_i})^{r_i} = \mathbf{o}$, gibt es eine Basis von U_i derart, dass $F|_{U_i}$ beschrieben wird durch eine Matrix

$$\lambda_i \cdot E_{r_i} + N_i \quad \text{und} \quad N_i^{r_i} = \mathbf{o}.$$

Offensichtlich gilt

$$\lambda_i \cdot E_{r_i} \cdot N_i = \lambda_i \cdot N_i = N_i \cdot \lambda_i \cdot E_{r_i}. \quad (*)$$

Da $V = U_1 \oplus \dots \oplus U_k$, erhält man insgesamt eine Basis \mathcal{B} von V derart, dass $M_{\mathcal{B}}(F)$ die angegebene Gestalt hat. Die Beziehung $D \cdot N = N \cdot D$ folgt aus (*) nach den Regeln für die Multiplikation von Matrizen (man kann kästchenweise multiplizieren). ■

Insbesondere für die Anwendungen bei der Lösung von Differentialgleichungen ist es wichtig, dass die darstellende Matrix – wie bei der Trigonalisierung – zu einer oberen Dreiecksmatrix gemacht werden kann.

Zusatz In jedem Hauptraum $U = \text{Hau}(F; \lambda)$ kann man eine Basis \mathcal{B}' derart wählen, dass $M_{\mathcal{B}'}(F|_U)$ eine obere Dreiecksmatrix ist.

Beweis Sei $G := F|_U - \lambda \cdot id_U$, also $F|_U = G + \lambda \cdot id_U$. Wie im Beweis des Lemmas von FITTING betrachten wir die Kette

$$\{\mathbf{o}\} \subset \text{Ker } G \subset \text{Ker } G^2 \subset \dots \subset \text{Ker } G^r = U.$$

Wir starten mit einer Basis \mathcal{B}_1 von $\text{Ker } G$, ergänzen sie zu einer Basis \mathcal{B}_2 von $\text{Ker } G^2$, u.s.w., bis eine Basis $\mathcal{B}' := \mathcal{B}_r$ von U erreicht ist. \mathcal{B}' hat die behauptete Eigenschaft, denn ist v in \mathcal{B}_l enthalten, so ist

$$G^l(v) = \mathbf{o}, \quad \text{also} \quad G(v) \in \text{Ker } G^{l-1}.$$

Somit ist $G(v)$ durch \mathcal{B}_{l-1} darstellbar. ■

Dieses Verfahren benutzen wir in den folgenden Beispielen.

Beispiel 1 Zunächst betrachten wir die ganz einfache obere Dreiecksmatrix

$$A := \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \in M(3 \times 3; \mathbb{R}).$$

Es ist $-P_A = X^3 - X^2 = X^2(X - 1)$, also $\mu(P_A; 0) = 2$ und $\mu(P_A; 1) = 1$.

Da $\text{Eig}(A; 0) = \text{Span}(e_1)$, ist A nicht diagonalisierbar. Mit Hilfe von

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

erhält man (e_1, e_2) als Ergänzung von (e_1) zu einer Basis von $\text{Hau}(A; 0)$. Weiter ist

$$\text{Hau}(A; 1) = \text{Eig}(A; 1) = \text{Span}^t(2, 1, 1).$$

Setzt man nun $S^{-1} = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, so folgt

$$S = \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{und} \quad S \cdot A \cdot S^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Damit sind die beiden störenden Einträge 1 oberhalb der Diagonalen in A beseitigt.

Etwas mehr Rechnung erfordert

Beispiel 2 Sei

$$A := \begin{pmatrix} 9 & -1 & 9 & -5 \\ 26 & -2 & 32 & -18 \\ -7 & 1 & -7 & 5 \\ -4 & 1 & -5 & 6 \end{pmatrix} \in M(4 \times 4; \mathbb{R}),$$

also $P_A = X^4 - 6X^3 + 13X^2 - 12X + 4 = (X - 1)^2 \cdot (X - 2)^2$. Es ist

$$\text{rang}(A - E_4) = \text{rang}(A - 2 \cdot E_4) = 3,$$

daher ist A nicht diagonalisierbar. Indem man die entsprechenden Gleichungssysteme löst, erhält man Eigenvektoren

$$v_1 = {}^t(1, 4, -1, -1) \quad \text{zu } \lambda_1 = 1 \quad \text{und} \quad v_2 = {}^t(1, 3, -1, -1) \quad \text{zu } \lambda_2 = 2.$$

Um die Eigenräume $\text{Eig}(A; 1) = \mathbb{R} \cdot v_1$ und $\text{Eig}(A; 2) = \mathbb{R} \cdot v_2$ zu den Haupträumen zu erweitern, benötigt man die Matrizen

$$(A - E_4)^2 = \begin{pmatrix} -5 & -1 & -7 & -2 \\ -22 & -3 & -28 & -6 \\ 6 & 1 & 8 & 2 \\ 9 & 1 & 11 & 2 \end{pmatrix} \quad \text{und} \quad (A - 2 \cdot E_4)^2 = \begin{pmatrix} -20 & 1 & -25 & 8 \\ -74 & 4 & -92 & 30 \\ 20 & -1 & 25 & -8 \\ 17 & -1 & 21 & -7 \end{pmatrix}.$$

Neben v_1 bzw. v_2 haben die entsprechenden Gleichungssysteme die davon linear unabhängigen Lösungen

$$w_1 = {}^t(0, -2, 0, 1) \quad \text{und} \quad w_2 = {}^t(0, -7, 1, 4),$$

also erhält man Basen (v_1, w_1) von $\text{Hau}(A; 1)$ und (v_2, w_2) von $\text{Hau}(A; 2)$. Trägt man sie als Spalten in eine Matrix ein, so ergibt sich

$$S^{-1} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 4 & -2 & 3 & -7 \\ -1 & 0 & -1 & 1 \\ -1 & 1 & -1 & 4 \end{pmatrix}, \quad S = \begin{pmatrix} -2 & 1 & -1 & 2 \\ -3 & 0 & -4 & 1 \\ 3 & -1 & 1 & -2 \\ 1 & 0 & 1 & 0 \end{pmatrix} \quad \text{und}$$

$$S \cdot A \cdot S^{-1} = \begin{pmatrix} 1 & -3 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & -4 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

Wie man die darstellende obere Dreiecksmatrix durch einen noch besser organisierten Aufbau der Basen in den Haupträumen weiter vereinfachen kann, wird im folgenden Abschnitt behandelt.

4.2.6 Nilpotente Endomorphismen*

In 4.2.5 war die Frage offen geblieben, wie man nilpotente Matrizen und Endomorphismen auf eine besonders einfache Form bringen kann. Offensichtliche Beispiele für nilpotente Matrizen sind obere oder untere Dreiecksmatrizen mit Nullen in der Diagonalen. Es gibt aber auch andere, wie etwa

$$A = \begin{pmatrix} 2 & 1 \\ -4 & -2 \end{pmatrix} \quad \text{mit} \quad A^2 = \mathbf{o} \quad \text{oder} \quad A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad \text{mit} \quad A^3 = \mathbf{o}.$$

Besonders einfache nilpotente Matrizen sind die **JORDAN-Matrizen**

$$J_m := \begin{pmatrix} 0 & 1 & & & 0 \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ 0 & & & & 0 \end{pmatrix} \in M(m \times m; K),$$

wobei K ein beliebiger Körper und $m \in \mathbb{N}^*$ ist. Dabei ist $J_1 = (0)$. Für die JORDAN-Matrizen gilt

$$J_m^k \neq \mathbf{o} \quad \text{für } k = 0, \dots, m-1 \quad \text{und} \quad J_m^m = \mathbf{o}.$$

Das sieht man besonders einfach, indem man die Wirkung des durch J_m definierten Endomorphismus F von K^n auf der kanonischen Basis betrachtet:

$$F(e_m) = e_{m-1}, F(e_{m-1}) = e_{m-2}, \dots, F(e_2) = e_1 \quad \text{und} \quad F(e_1) = \mathbf{o},$$

also $F^k(e_m) = e_{m-k}$ für $k = 0, \dots, m-1$ und $F^m(e_m) = \mathbf{o}$. Dass die Indizes rückwärts laufen, liegt an der Konvention, JORDAN-Matrizen als obere Dreiecksmatrizen zu erklären. Bei unteren Dreiecksmatrizen würden die Indizes aufsteigen.

Ist allgemeiner $F : V \rightarrow V$ ein nilpotenter Endomorphismus, d.h. $F^k = \mathbf{o}$ für ein $k \in \mathbb{N}^*$, so gibt es zu jedem $\mathbf{o} \neq v \in V$ ein minimales $l \in \mathbb{N}^*$ derart, dass $F^l(v) = \mathbf{o}$. Das l -Tupel

$$(v, F(v), F^2(v), \dots, F^{l-1}(v))$$

nennt man einen **JORDAN-Strang**. Ganz einfach aber wichtig ist die

Bemerkung Jeder JORDAN-Strang ist linear unabhängig.

Beweis Angenommen

$$\mu_0 v + \mu_1 F(v) + \dots + \mu_{l-1} F^{l-1}(v) = \mathbf{o} \quad \text{mit} \quad \mu_0, \dots, \mu_{l-1} \in K, \quad (*)$$

und $\mu_r \neq 0$ für ein $r \in \{0, \dots, l-1\}$. Dann können wir r minimal wählen, und F^{l-1-r} auf (*) anwenden. Das ergibt $\mu_r F^{l-1}(v) + \mathbf{o} + \dots + \mathbf{o} = \mathbf{o}$, im Widerspruch zu $F^{l-1}(v) \neq \mathbf{o}$. ■

Insbesondere folgt für jeden nilpotenten Endomorphismus F von V , dass $F^k = \mathbf{o}$ für $k = \dim V$. Um den Zusammenhang mit den darstellenden Matrizen zu sehen, ordnen wir einen JORDAN-Strang in umgekehrter Reihenfolge zu einer Basis

$$\mathcal{B} = (F^{l-1}(v), \dots, F(v), v)$$

des Untervektorraums $Z := \text{Span}(\mathcal{B}) \subset V$ an. Dieses Z ist F -invariant, und offensichtlich ist $M_{\mathcal{B}}(F|_Z) = J_l$ eine JORDAN-Matrix. Wegen der speziellen Art der Operation von F auf \mathcal{B} nennt man Z einen **zyklischen** Unterraum.

Nun stehen alle Hilfsmittel bereit für das zentrale Theorem über die

Entscheidend sind nun die Eigenschaften

$$F|W_k \text{ ist injektiv und } F(W_k) \cap V_{k-2} = \{\mathbf{o}\}.$$

Das ist aber klar, denn ist $\mathbf{o} \neq w \in W_k$, so ist $w \notin V_{k-1}$, also folgt $\mathbf{o} \neq F^{k-1}(w) = F^{k-2}(F(w))$ und somit $F(w) \neq \mathbf{o}$, sowie $F(w) \notin V_{k-2}$.

In V_{k-1} betrachten wir die Untervektorräume $F(W_k)$ und V_{k-2} . Da $V_{k-2} \oplus F(W_k) \subsetneq V_{k-1}$ sein kann, wählt man einen weiteren geeigneten Untervektorraum $U_{k-1} \subset V_{k-2}$ derart, dass

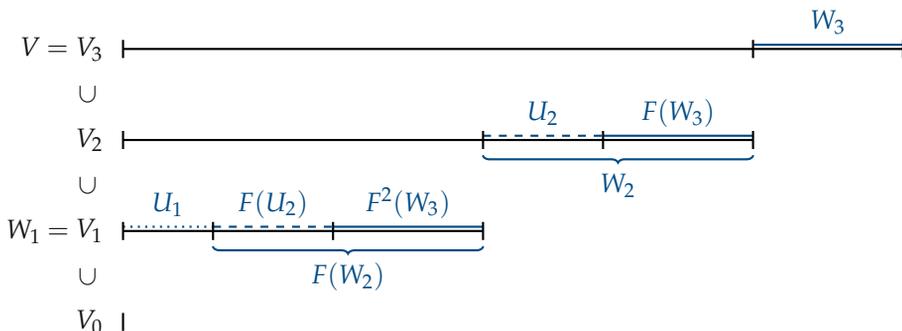
$$V_{k-1} = V_{k-2} \oplus U_{k-1} \oplus F(W_k).$$

Dann kann man $W_{k-1} := F(W_k) \oplus U_{k-1}$, insbesondere $W_1 := V_1$ wählen.

Durch Fortsetzung dieser Konstruktion erhält man analog für $l = 1, \dots, k-1$ Zerlegungen

$$V_l = V_{l+1} \oplus W_l \quad \text{mit} \quad W_l = U_l \oplus F(W_{l+1})$$

und injektive Abbildungen $F|W_{l+1} : W_{l+1} \rightarrow W_l$. Für $k = 3$ kann man das schematisch so skizzieren:



$$V = U_1 \oplus F(U_2) \oplus F^2(W_3) \oplus U_2 \oplus F(W_3) \oplus W_3 \quad .$$

Allgemein aufgeschrieben erhält man die Zerlegungen

$$V = V_k = V_{k-1} \oplus W_k = V_{k-2} \oplus W_{k-1} \oplus W_k = \dots = W_1 \oplus \dots \oplus W_k.$$

Um die gesuchten JORDAN-Stränge zu finden, betrachten wir die folgende Anordnung der Summen:

direkte Summe der zyklischen Unterräume. Ordnet man die JORDAN-Stränge aus dem Schema von unten nach oben, und ist \mathcal{B} die so aus den Strängen entstandene Basis von V , so folgt, dass $M_{\mathcal{B}}(F)$ die behauptete Gestalt hat.

Die Zahlen d_k, \dots, d_1 sind als Dimensionen von Unterräumen von V allein durch die Wirkung von F festgelegt, und damit eindeutig bestimmt. ■

Aus dem angegebenen Beweis kann man sofort ein praktisches Rechenverfahren ableiten. Dabei werden die passenden direkten Summanden durch Basisergänzungen konstruiert (vgl. 2.2.5).

Als Folgerung notieren wir noch das

Korollar Für einen Endomorphismus F von V mit $n = \dim V$ gilt:

$$F \text{ nilpotent} \Leftrightarrow P_F = \pm X^n.$$

Beweis „ \Rightarrow “ folgt sofort aus dem obigen Theorem, und „ \Leftarrow “ folgt aus der Hauptraum-Zerlegung in 4.2.5. ■

Beispiel 1 Wir betrachten die ganz einfache Matrix

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{mit} \quad A^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{und} \quad A^3 = \mathbf{o}.$$

In diesem Fall ist:

$$V_1 = \text{Ker}(A) = \text{Span}(e_1), \quad V_2 = \text{Ker}(A^2) = \text{Span}(e_1, e_2) \quad \text{und} \quad V_3 = \text{Span}(e_1, e_2, e_3) = K^3.$$

Als direkte Summanden passen

$$W_3 = \text{Span}(e_3), \quad W_2 = A(W_3) = \text{Span}(e_1 + e_2) \quad \text{und} \quad W_1 = A(W_2) = \text{Span}(e_1) = \text{Ker}(A),$$

also ist $U_2 = U_1 = \{0\}$. Als Ergebnis erhält man einen einzigen JORDAN-Strang

$$(e_3, \quad A \cdot e_3 = e_1 + e_2, \quad A^2(e_3) = e_1),$$

der schon eine Basis von K^3 ist. Daraus ergibt sich, in umgekehrter Reihenfolge als Spalten eingetragen,

$$S^{-1} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{also} \quad S = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{und} \quad S \cdot A \cdot S^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

ist eine JORDAN-Matrix.

Beispiel 2 Für

$$A := \begin{pmatrix} 2 & -1 & -1 & 0 \\ 8 & -3 & -5 & -4 \\ -4 & 1 & 3 & 4 \\ 3 & -1 & -2 & -2 \end{pmatrix} \in M(4 \times 4; \mathbb{R})$$

ist $A^2 = \mathbf{o}$. Dazu gehört das folgende Diagramm:

$$\mathbb{R}^4 = V = \text{Ker } A^2 = V_2 = V_1 \oplus W_2$$

$$\cup$$

$$\text{Ker } A = V_1 = \{\mathbf{o}\} \oplus W_1.$$

Da $\text{rang } A = 2$, folgt $\dim V_1 = \dim W_1 = \dim W_2 = 2$. Wegen $e_1, e_2 \notin V_1$, können wir

$$W_2 := \text{Span}(e_1, e_2)$$

setzen. Daraus erhalten wir zwei JORDAN-Stränge der Länge 2:

$$v_2 := e_1, \quad v_1 := A \cdot e_1 = {}^t(2, 8, -4, 3) \quad \text{und}$$

$$w_2 := e_2, \quad w_1 := A \cdot e_2 = {}^t(-1, -3, 1, -1).$$

Sie ergeben Basen (v_1, w_1) von W_1 und (v_1, v_2, w_1, w_2) von $V = W_1 \oplus W_2$. Trägt man die Basisvektoren von V als Spalten in eine Matrix ein, so erhält man

$$S^{-1} = \begin{pmatrix} 2 & 1 & -1 & 0 \\ 8 & 0 & -3 & 1 \\ -4 & 0 & 1 & 0 \\ 3 & 0 & -1 & 0 \end{pmatrix} \quad \text{und} \quad S = \begin{pmatrix} 0 & 0 & -1 & -1 \\ 1 & 0 & -1 & -2 \\ 0 & 0 & -3 & -4 \\ 0 & 1 & -1 & -4 \end{pmatrix}.$$

Daraus ergibt sich die JORDANSche Normalform

$$S \cdot A \cdot S^{-1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Beispiel 3 Für

$$A := \begin{pmatrix} 1 & 0 & 0 & -1 \\ 9 & -3 & -6 & -6 \\ -5 & 2 & 4 & 3 \\ 3 & -1 & -2 & -2 \end{pmatrix} \quad \text{ist} \quad A^2 := \begin{pmatrix} -2 & 1 & 2 & 1 \\ -6 & 3 & 6 & 3 \\ 2 & -1 & -2 & -1 \\ -2 & 1 & 2 & 1 \end{pmatrix} \quad \text{und} \quad A^3 = \mathbf{o}.$$

Dazu gehört das folgende Diagramm:

$$\mathbb{R}^4 = V = \text{Ker } A^3 = V_3 = V_2 \oplus W_3$$

$$\cup$$

$$\text{Ker } A^2 = V_2 = V_1 \oplus W_2$$

$$\cup$$

$$\text{Ker } A = V_1 = \{\mathbf{o}\} \oplus W_1.$$

Da $\text{rang } A^2 = 1$ und $\text{rang } A = 2$, folgt $\dim V_2 = 3$, $\dim W_3 = 1$, $\dim V_1 = 2$, $\dim W_2 = 1$ und $\dim W_1 = 2$. Nun erhält man einen JORDAN-Strang der Länge 3 aus $v_3 := e_1$; es ist

$$v_2 := A \cdot v_3 = {}^t(1, 9, -5, 3), v_1 := A^2 \cdot v_3 = {}^t(-2, -6, 2, -2), A^3 \cdot v_3 = \mathbf{o}.$$

Da $v_3 \notin V_2$ und $v_2 = A \cdot v_3 \notin V_1$, kann man

$$W_3 := \text{Span}(v_3) \quad \text{und} \quad W_2 := \text{Span}(v_2)$$

wählen. Weiter ist $v_1 \in W_1$, und wählt man etwa $w := {}^t(1, 1, 0, 1) \in W_1$, so ist (v_1, w) Basis von W_1 . Der Vektor w ist ein JORDAN-Strang der Länge 1, insgesamt erhält man eine Basis (v_1, v_2, v_3, w) von $V = W_1 \oplus W_2 \oplus W_3$; als Spalten in eine Matrix eingetragen ergibt das

$$S^{-1} := \begin{pmatrix} -2 & 1 & 1 & 1 \\ -6 & 9 & 0 & 1 \\ 2 & -5 & 0 & 0 \\ -2 & 3 & 0 & 1 \end{pmatrix} \quad \text{und} \quad S = \frac{1}{8} \cdot \begin{pmatrix} 0 & -5 & -6 & 5 \\ 0 & -2 & -4 & 2 \\ 8 & -4 & -8 & -4 \\ 0 & -4 & 0 & 12 \end{pmatrix}.$$

Schließlich ergibt sich die JORDANSche Normalform

$$S \cdot A \cdot S^{-1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

4.2.7 Die JORDANSche Normalform*

Durch Kombination der Ergebnisse aus 4.2.5 (Zerlegung in Haupträume) und 4.2.6 (Normalform nilpotenter Endomorphismen), kommt man schließlich zu folgendem Endergebnis:

JORDANSche Normalform Gegeben sei ein Endomorphismus F eines endlich-dimensionalen Vektorraums V über einem beliebigen Körper K . Falls das charakteristische Polynom P_F in Linearfaktoren zerfällt, d.h.

$$P_F = \pm (X - \lambda_1)^{r_1} \cdot \dots \cdot (X - \lambda_k)^{r_k}$$

mit paarweise verschiedenen $\lambda_1, \dots, \lambda_k \in K$, so gibt es eine Basis \mathcal{B} von V derart, dass

$$M_{\mathcal{B}}(F) = \begin{pmatrix} \boxed{\lambda_1 \cdot E_{r_1} + N_1} & & & 0 \\ & \ddots & & \\ & & \ddots & \\ 0 & & & \boxed{\lambda_k \cdot E_{r_k} + N_k} \end{pmatrix}$$

wobei die Matrizen N_1, \dots, N_k nilpotent und in der Normalform aus 4.2.6 sind. ■

Wir wenden dieses verbesserte Verfahren noch einmal an auf die Matrix

$$A := \begin{pmatrix} 9 & -1 & 9 & -5 \\ 26 & -2 & 32 & -18 \\ -7 & 1 & -7 & 5 \\ -4 & 1 & -5 & 6 \end{pmatrix}$$

aus Beispiel 2 in 4.2.5. Wir starten mit $w_1 = {}^t(0, -2, 0, 1) \in \text{Hau}(A; 1)$, und erhalten daraus

$$w'_1 := (A - 1 \cdot E_4) \cdot w_1 = {}^t(-3, -12, 3, 3) \in \text{Hau}(A; 1).$$

Analog erhält man aus $w_2 = {}^t(0, -7, 1, 4) \in \text{Hau}(A; 2)$

$$w'_2 := (A - 2 \cdot E_4) \cdot w_2 = {}^t(-4, -12, 4, 4) \in \text{Hau}(A; 2).$$

Die beiden JORDAN-Stränge (w_1, w'_1) bzw. (w_2, w'_2) sind Basen von $\text{Hau}(A; 1)$ bzw. $\text{Hau}(A; 2)$. In der passenden Reihenfolge in eine Matrix eingetragen erhält man

$$S^{-1} = \begin{pmatrix} -3 & 0 & -4 & 0 \\ -12 & -2 & -12 & -7 \\ 3 & 0 & 4 & 1 \\ 3 & 1 & 4 & 4 \end{pmatrix} \quad \text{und daraus} \quad S = \frac{1}{12} \cdot \begin{pmatrix} 8 & -4 & 4 & -8 \\ -36 & 0 & -48 & 12 \\ -9 & 3 & -3 & 6 \\ 12 & 0 & 12 & 0 \end{pmatrix}.$$

Daraus ergibt sich für A die JORDANSche Normalform

$$S \cdot A \cdot S^{-1} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

Zum Abschluss dieses Kapitels noch einige Bemerkungen zur Bedeutung der JORDANSchen Normalform. Vom Standpunkt der Theorie geht es um die **Klassifikation** von Endomorphismen. Aus der Sicht der darstellenden Matrizen kann man das so beschreiben: Zwei Matrizen $A, B \in M(n \times n; K)$ heißen **ähnlich**, wenn es ein $S \in GL(n; K)$ gibt derart, dass

$$B = S \cdot A \cdot S^{-1}.$$

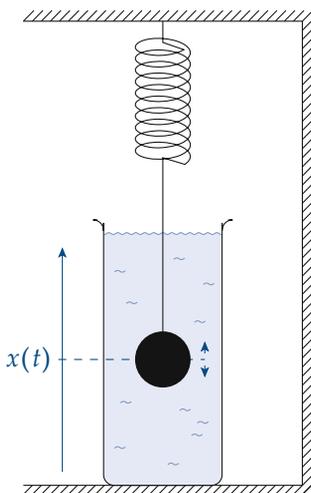
Es ist einfach zu sehen, dass die Ähnlichkeit in $M(n \times n; K)$ eine Äquivalenzrelation ergibt. Gesucht sind nun **Invarianten** einer Äquivalenzklasse, d.h. in diesem Fall Zahlen, die für alle Matrizen einer Äquivalenzklasse gleich sind, und **Normalformen**, d.h. besonders einfache Repräsentanten. Nach dem Lemma aus 4.1.4 haben ähnliche Matrizen das gleiche charakteristische Polynom, also sind die Eigenwerte und ihre Vielfachheiten Invarianten. Im Fall $K = \mathbb{C}$ zerfällt das charakteristische Polynom nach dem Fundamentalsatz der Algebra stets in Linearfaktoren, also kann man nach den Ergebnissen dieses Kapitels zu jeder Matrix $A \in M(n \times n; \mathbb{C})$ eine ähnliche Matrix B in JORDANScher Normalform finden. Diese Matrix B in Normalform hat nicht nur die gleichen Eigenwerte wie jede beliebige Matrix A aus der gleichen Äquivalenzklasse, sondern auch die Anzahlen und Längen der JORDAN-Stränge sind gleich. Das sieht man daran, dass diese

Zahlen nach den Konstruktionen von 4.2.5 und 4.2.6 durch Dimensionen von Untervektorräumen festgelegt sind, und nicht von der Auswahl einer Basis abhängen. Daher sind die Anzahlen und Längen der JORDAN-Stränge weitere Invarianten der Äquivalenzklasse. Man kann zeigen, dass zwei Matrizen A und B genau dann äquivalent sind, wenn die Invarianten – bis auf die Reihenfolge – gleich sind.

Vom Standpunkt numerischer Rechnungen ist die Situation ganz anders. Bei reellen oder komplexen Zahlen kann man nur endlich viele Dezimalstellen berücksichtigen, ein Ergebnis wird nie genau Null, sondern höchstens sehr klein sein. Dem entsprechend sind mehrfache Nullstellen eines Polynoms mehr in der Theorie als in der Praxis möglich, und fast alle Matrizen haben nur einfache Nullstellen, sind also nach dem Satz aus 4.2.1 diagonalisierbar. In diesem Fall reduzieren sich die Invarianten auf die n verschiedenen Eigenwerte.

Die in den letzten Abschnitten durchgerechneten Beispiele sollen nur zeigen, dass die Beweismethode für konkrete Matrizen anwendbar ist. Aber die angegebenen Matrizen sind für diesen Zweck in etwas schulmeisterlicher Art künstlich produziert worden.

4.2.8 Gedämpfte Schwingungen*



Der Verlauf der ungedämpften Schwingung eines Federpendels hängt ab von der Federkonstante c und der Masse m der Kugel. Ist die Position im Ruhezustand gegeben durch $x = 0$, so ergibt sich aus dem Gleichgewicht der Kräfte die Bedingung

$$m \cdot \ddot{x}(t) = -c \cdot x(t), \quad \text{also} \quad \ddot{x}(t) + \omega^2 \cdot x(t) = 0 \quad \text{mit} \quad \omega^2 := \frac{c}{m}.$$

Kommt eine linear von der Geschwindigkeit abhängige Reibungskraft hinzu, so gibt es eine Konstante $\mu \in \mathbb{R}_+$ derart, dass diese Kraft gleich $-2\mu\dot{x}(t)$ ist. Insgesamt ergibt sich die Differentialgleichung

$$\ddot{x} + 2\mu\dot{x} + \omega^2x = 0 \quad (*)$$

mit einer Anfangswertbedingung

$$x(0) = \alpha_1 \in \mathbb{R} \quad \text{und} \quad \dot{x}(0) = \alpha_2 \in \mathbb{R}.$$

Eine Variante der etwa in [FO₂, §14] ausgeführten Methode zur Lösung von (*) benutzt die Theorie der Eigenwerte. Dazu führt man zunächst die eine Gleichung (*) 2. Ordnung auf zwei Gleichungen 1. Ordnung zurück, indem man

$$x_0(t) = x(t) \quad \text{und} \quad x_1(t) = \dot{x}(t) = \dot{x}_0(t)$$

setzt. Die Gleichung (*) ist dann gleichwertig mit dem linearen System

$$\begin{aligned} \dot{x}_0 &= x_1 \\ \dot{x}_1 &= -\omega^2x_0 - 2\mu x_1 \end{aligned} \quad (**)$$

oder kürzer $\dot{\varphi} = A \cdot \varphi$, wobei

$$\varphi := \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \quad \text{und} \quad A := \begin{pmatrix} 0 & 1 \\ -\omega^2 & -2\mu \end{pmatrix}.$$

Für das charakteristische Polynom von A und seine Nullstellen erhält man

$$P_A = X^2 + 2\mu X + \omega^2 \quad \text{und} \quad \lambda_{1,2} = -\mu \pm \sqrt{\mu^2 - \omega^2}.$$

Nun sind drei Fälle zu unterscheiden:

1. Schwache Dämpfung, d.h. $\mu < \omega$, also $\mu^2 - \omega^2 < 0$.
2. Starke Dämpfung, d.h. $\mu > \omega$, also $\mu^2 - \omega^2 > 0$.
3. Aperiodischer Grenzfall, d.h. $\mu = \omega$, also $\mu^2 - \omega^2 = 0$.

Die Fälle 1 und 2 kann man weitgehend gemeinsam behandeln, denn da sind die beiden Eigenwerte verschieden. In Fall 2 sind sie beide reell, in Fall 1 nicht. Daher erweitern wir nun \mathbb{R} zu \mathbb{C} . In jedem der beiden Fälle erhält man als Eigenvektoren von A

$$v_1 = \begin{pmatrix} 1 \\ \lambda_1 \end{pmatrix} \quad \text{zu} \quad \lambda_1 \quad \text{und} \quad v_2 = \begin{pmatrix} 1 \\ \lambda_2 \end{pmatrix} \quad \text{zu} \quad \lambda_2.$$

Nun kann man A entsprechend 4.2.1 diagonalisieren. Mit

$$S^{-1} = \begin{pmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{pmatrix} \quad \text{ist} \quad S \cdot A \cdot S^{-1} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} =: D.$$

Das System (**) kann man entsprechend transformieren:

$$y := \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} = S \cdot \varphi \quad \text{und} \quad \varphi = \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = S^{-1} \cdot y.$$

Dann ist

$$\dot{y} = S \cdot \dot{\varphi} = S \cdot A \cdot \varphi = (S \cdot A \cdot S^{-1}) \cdot y = D \cdot y.$$

Das System $\dot{y} = D \cdot y$ hat die Fundamentallösungen

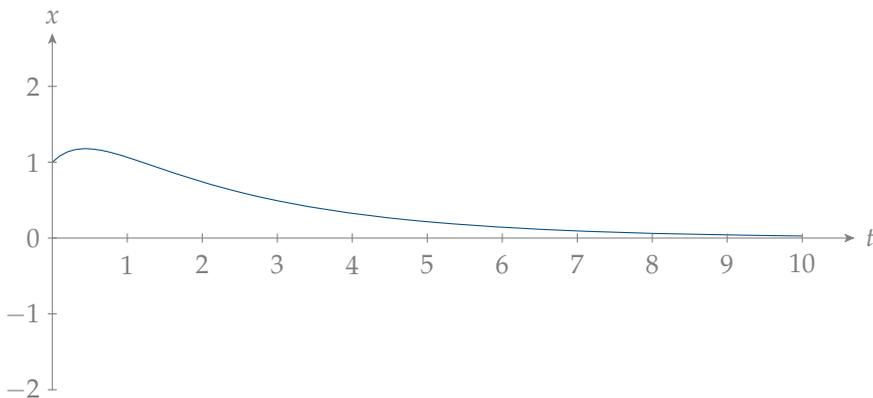
$$y_0(t) = e^{\lambda_1 t} \quad \text{und} \quad y_1(t) = e^{\lambda_2 t}.$$

Da $x = x_0 = y_0 + y_1$, erhält man daraus als allgemeine Lösung von (*)

$$x(t) = \beta_1 e^{\lambda_1 t} + \beta_2 e^{\lambda_2 t}.$$

In **Fall 2** ist $\sqrt{\mu^2 - \omega^2} < \mu$ reell, also folgt $\lambda_2 < \mu < \lambda_1 < 0$. Daher entsteht gar keine Schwingung mehr. Die Koeffizienten β_1 und β_2 sind reell und durch die Anfangswerte α_1, α_2 festgelegt, es gilt

$$\beta_1 = \frac{\lambda_2 \alpha_1 - \alpha_2}{\lambda_2 - \lambda_1} \quad \text{und} \quad \beta_2 = \frac{\alpha_2 - \lambda_1 \alpha_1}{\lambda_2 - \lambda_1}.$$



Starke Dämpfung: $\omega = 1$, $\mu = \sqrt{2}$, $\alpha_1 = \alpha_2 = 1$

In **Fall 1** ist $\omega' := \sqrt{\omega^2 - \mu^2} > 0$ reell und

$$\lambda_{1,2} = -\mu \pm i\omega'$$

nicht reell. Aus den komplexen Lösungen

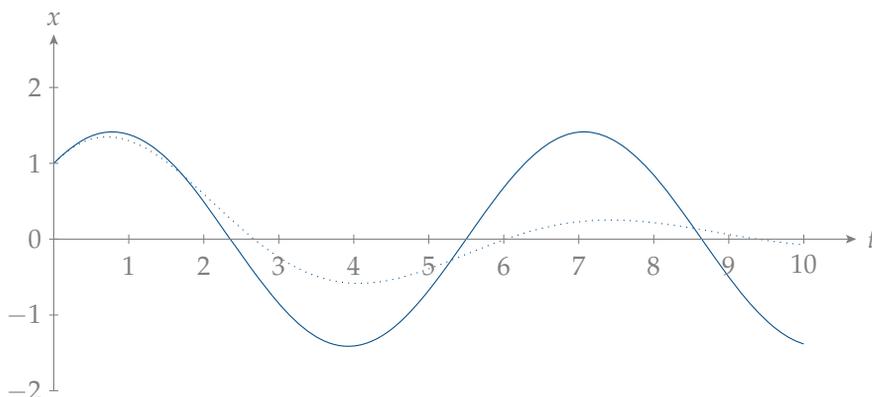
$$e^{\lambda_i t} = e^{(-\mu \pm i\omega')t} = e^{-\mu t} e^{\pm i\omega' t}$$

kann man nun die Real- und Imaginärteile linear kombinieren, daraus erhält man schließlich mit $\beta_1, \beta_2 \in \mathbb{R}$ die allgemeine reelle Lösung

$$x(t) = \beta_1 e^{-\mu t} \cos(\omega' t) + \beta_2 \cdot e^{-\mu t} \sin(\omega' t).$$

Das beschreibt gedämpfte Schwingung mit einer gegenüber ω verringerten Kreisfrequenz ω' , es gilt

$$\beta_1 = \alpha_1 \quad \text{und} \quad \beta_2 = \frac{\mu \alpha_1 + \alpha_2}{\omega'}.$$



Keine Dämpfung: $\omega = 1, \quad \mu = 0, \quad \alpha_1 = \alpha_2 = 1$ ———
 Schwache Dämpfung: $\omega = 1, \quad \mu = \frac{1}{4}, \quad \alpha_1 = \alpha_2 = 1$ ·····

In **Fall 3** ist $\mu = \omega$, also

$$A = \begin{pmatrix} 0 & 1 \\ -\omega^2 & -2\omega \end{pmatrix},$$

und $\lambda = -\omega$ ist der einzige Eigenwert. Der zugehörige Eigenraum

$$\text{Eig}(A; -\omega) = \mathbb{R} \cdot \begin{pmatrix} 1 \\ -\omega \end{pmatrix}$$

ist eindimensional, also ist A nicht diagonalisierbar. Ausweg ist eine Trigonalisierung von A nach der Methode aus 4.2.4: Man trägt die neue Basis als Spalten in eine Matrix ein, das ergibt

$$S^{-1} := \begin{pmatrix} 1 & 0 \\ -\omega & 1 \end{pmatrix}, \quad \text{und} \quad S \cdot A \cdot S^{-1} = \begin{pmatrix} -\omega & 1 \\ 0 & -\omega \end{pmatrix}$$

ist sogar in Jordanscher Normalform. Wie in den Fällen 1 und 2 kann man das System (***) mit Hilfe von

$$\begin{pmatrix} y_0 \\ y_1 \end{pmatrix} = S \cdot \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \omega & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}$$

transformieren auf

$$\begin{aligned} \dot{y}_0 &= -\omega y_0 + y_1 \\ \dot{y}_1 &= -\omega y_1 \end{aligned} \quad (***)$$

Dieses System löst man, wie üblich, von unten nach oben: Die allgemeine Lösung der zweiten und homogenen Gleichung ist

$$y_1 = \beta_2 \cdot e^{-\omega t} \quad \text{mit} \quad \beta_2 \in \mathbb{R} \quad \text{beliebig.}$$

Eingesetzt in die erste Gleichung erhält man

$$\dot{y}_0 = -\omega y_0 + \beta_2 e^{-\omega t}. \quad (+)$$

Diese inhomogene Gleichung kann man nach der Methode der „Variation der Konstanten“ mit Hilfe des Ansatzes

$$y_0 = u(t) \cdot e^{-\omega t} \quad (++)$$

lösen, wobei die unbekannte Funktion u noch zu finden ist. Durch Differenzieren von (++) und einen Vergleich mit (+) folgt

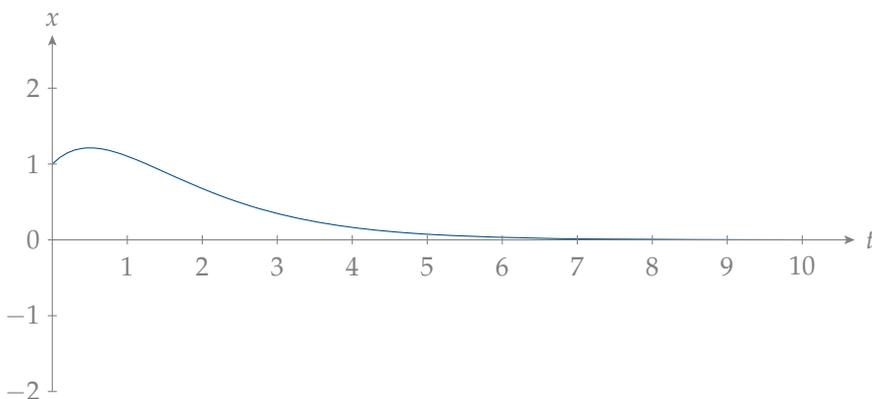
$$\dot{u}(t) = \beta_2 \quad \text{und somit} \quad u(t) = \beta_2 t + \beta_1$$

mit $\beta_1 \in \mathbb{R}$ beliebig. Das ergibt schließlich die allgemeine Lösung

$$x(t) = (\beta_2 t + \beta_1) e^{-\omega t}$$

von (*). Zunächst ist das die allgemeine Lösung für $y_0(t)$ aus (**). Wegen der speziellen Wahl von S^{-1} ist aber $y_0 = x_0 = x$. Weiter gilt

$$\beta_1 = \alpha_1 \quad \text{und} \quad \beta_2 = \omega \alpha_1 + \alpha_2.$$



Aperiodischer Grenzfall: $\omega = \mu = 1, \quad \alpha_1 = \alpha_2 = 1$

Dass es neben den oben ermittelten Lösungen keine weiteren gibt, folgt aus der allgemeinen Theorie der linearen Differentialgleichungen (vgl. etwa [FO₂, §13, Satz 5]). In unserem Beispiel hat der \mathbb{R} -Vektorraum der Lösungen von (*) die Dimension 2, dem entsprechen die jeweils frei wählbaren Parameter $\beta_1, \beta_2 \in \mathbb{R}$ in der allgemeinen Lösung. Die Werte dieser Parameter sind durch die Anfangsbedingungen festgelegt, unter diesen Bedingungen ist die Lösung eindeutig bestimmt.

... obschon sie vor den Genuß der Erkenntnisfrucht
den Schweiß des Tensorkalküls gesetzt hat.

HERMANN WEYL

Kapitel 5

Bilineare Algebra und Geometrie

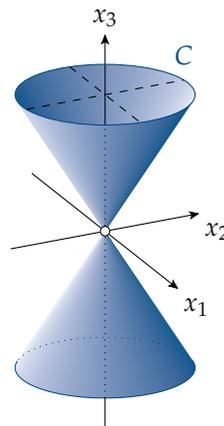
5.1 Kegelschnitte*

In den folgenden Abschnitten wollen wir zur Vorbereitung auf die bilineare Algebra zunächst an ein klassisches Thema der Geometrie erinnern, das aus den meisten Lehrplänen der Gymnasien gestrichen wurde, obwohl es viele elementare praktische Anwendungen hat. Eine ausführliche Darstellung findet man etwa in [FI₂, 1.4].

5.1.1 Die Gleichungen der ebenen Schnitte eines Kreiskegels

Wir starten im \mathbb{R}^3 mit einem *Kreiskegel*

$$C := \{(x_1, x_2, x_3) \in \mathbb{R}^3 : x_1^2 + x_2^2 = x_3^2\}.$$



Ein Schnitt mit der Ebene $x_3 = c$ ist gegeben durch die Gleichung

$$x_1^2 + x_2^2 = c^2,$$

das ist ein *Kreis* mit dem Radius $|c|$. Für $c = 0$ erhält man

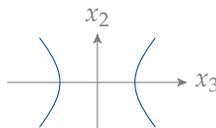
$$x_1^2 + x_2^2 = 0,$$

das ist ein Kreis vom Radius 0, also ein *Punkt*. Der Schnitt mit der Ebene $x_1 = 0$ ist gegeben durch die Gleichung

$$x_2^2 - x_3^2 = (x_2 + x_3)(x_2 - x_3) = 0,$$

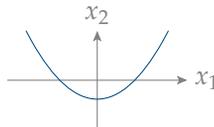
das ist ein *Paar von Geraden*. Schneidet man mit der Ebene $x_1 = 1$, so erhält man

$$x_3^2 - x_2^2 = 1,$$



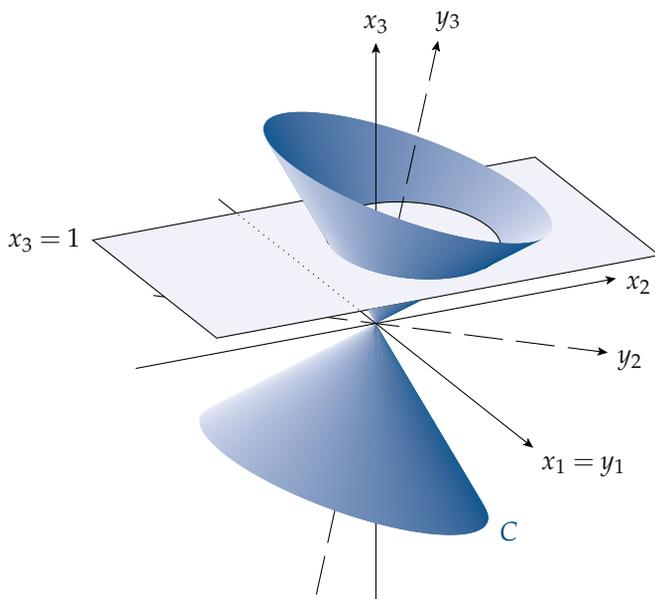
das ist eine *Hyperbel*. Schließlich ergibt der Schnitt mit der Ebene $x_3 = x_2 + 1$ die Gleichung

$$x_2 = \frac{1}{2}x_1^2 - \frac{1}{2},$$



das ist eine *Parabel*.

In diesen Beispielen hatten wir sehr spezielle Positionen der Ebene zum Kegel gewählt. Um allgemeinere Schnitte zu berechnen, halten wir die Ebene $x_3 = 1$ fest, und drehen den Kegel um die x_1 -Achse mit dem Winkel φ .



Diese Drehung wird beschrieben durch die Matrix

$$S := \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \varphi & -\sin \varphi \\ 0 & \sin \varphi & \cos \varphi \end{pmatrix}, \quad \text{es ist } S^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \varphi & \sin \varphi \\ 0 & -\sin \varphi & \cos \varphi \end{pmatrix}.$$

In Koordinaten bedeutet das mit $x = {}^t(x_1, x_2, x_3)$ und $y = {}^t(y_1, y_2, y_3)$

$$x = S \cdot y \quad \text{und} \quad y = S^{-1} \cdot x.$$

Der gedrehte Kegel hat in den y -Koordinaten die Gleichung $y_1^2 + y_2^2 = y_3^2$. Setzt man

$$y_1 = x_1, \quad y_2 = x_2 \cdot \cos \varphi + x_3 \cdot \sin \varphi, \quad y_3 = -x_2 \cdot \sin \varphi + x_3 \cdot \cos \varphi$$

ein, so erhält man als Gleichung des gedrehten Kegels in den x -Koordinaten

$$x_1^2 + \alpha \cdot x_2^2 + 4\beta \cdot x_2 x_3 = \alpha \cdot x_3^2 \quad \text{mit} \quad \alpha := \cos^2 \varphi - \sin^2 \varphi \quad \text{und} \quad \beta := \cos \varphi \cdot \sin \varphi.$$

Der Schnitt dieses gedrehten Kegels mit der Ebene $x_3 = 1$ wird dann beschrieben durch die Gleichung

$$x_1^2 + \alpha \cdot x_2^2 + 4\beta \cdot x_2 = \alpha. \quad (*)$$

Wir können uns auf den Winkelbereich $0 \leq \varphi \leq \frac{\pi}{2}$ beschränken, denn aus Gründen der Symmetrie passiert bei allen anderen Winkeln nichts Neues. In diesem Bereich ist $\alpha = 0$ genau dann, wenn $\varphi = \frac{\pi}{4}$. Dann ist $\beta = \frac{1}{2}$, und die Gleichung des Schnittes lautet

$$x_1^2 + 2 \cdot x_2 = 0,$$

das ist eine Parabel.

Für alle anderen Winkel, also $\alpha \neq 0$, wollen wir nun die Gleichung (*) durch eine Verschiebung der x_2 -Achse etwas einfacher schreiben. Das geht mit quadratischer Ergänzung der Terme, die x_2 enthalten:

$$\begin{aligned} \alpha \cdot x_2^2 + 4\beta \cdot x_2 &= \alpha \cdot \left(x_2^2 + \frac{4\beta}{\alpha} \cdot x_2 \right) = \alpha \cdot \left(x_2^2 + \frac{4\beta}{\alpha} \cdot x_2 + \left(\frac{2\beta}{\alpha} \right)^2 \right) - \frac{4\beta^2}{\alpha} \\ &= \alpha \cdot \left(x_2 + \frac{2\beta}{\alpha} \right)^2 - \frac{4\beta^2}{\alpha}. \end{aligned}$$

Setzt man $z_1 = x_2 + \frac{2\beta}{\alpha}$ und $z_2 = x_1$, so lautet die Gleichung des Kegelschnitts wegen $\alpha^2 + 4\beta^2 = 1$

$$\alpha^2 \cdot z_1^2 + \alpha \cdot z_2^2 = 1. \quad (**)$$

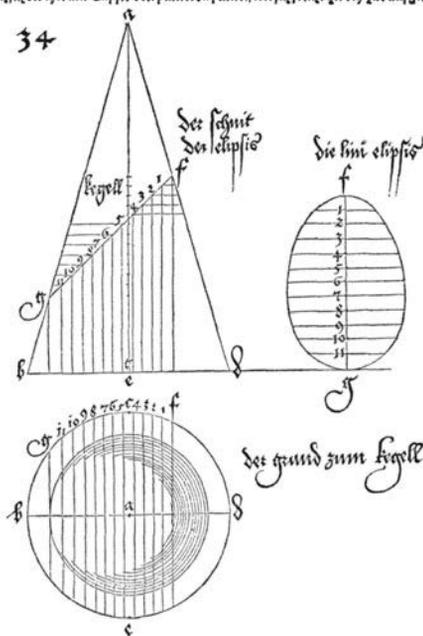
Für $0 \leq \varphi \leq \frac{\pi}{4}$ ist $\alpha > 0$. Setzt man $a = \frac{1}{\alpha}$ und $b = \frac{1}{\sqrt{\alpha}}$, so lautet die Gleichung

$$\frac{z_1^2}{a^2} + \frac{z_2^2}{b^2} = 1,$$

das ist eine Ellipse mit den **Hauptachsen** a und b .

Es ist geometrisch nicht offensichtlich – aber durch diese Rechnung nachgewiesen –, dass jeder solch schräge Schnitt eines Kegels mit einer Ebene zwei zueinander senkrechte Symmetrieachsen hat. Man würde eher einen eiförmigen Schnitt erwarten; dieser Fehler ist selbst ALBRECHT DÜRER [DÜ] unterlaufen, obwohl er „die eyer lini Ellipsis von punct zu punct ... aufgerissen“ hat.

Also thut ich im durch die gangen sal so dann die puncten zu rings herum gemacht sind/
daß zeich ich die eyer lini Ellipsis von punct zu punct, wie ich solche die bey hab aufgerissen.



Für $\frac{\pi}{4} < \varphi \leq \frac{\pi}{2}$ ist $\alpha < 0$. Setzt man in (**) $a = \frac{1}{\alpha}$ und $b = \frac{1}{\sqrt{-\alpha}}$, so lautet die Gleichung

$$\frac{z_1^2}{a^2} - \frac{z_2^2}{b^2} = 1,$$

das ist eine Hyperbel mit den **Hauptachsen** a und b . Für $\varphi = \frac{\pi}{2}$ ist $\alpha = -1$, also $a = b = 1$.

5.1.2 Geometrische Eigenschaften der Kegelschnitte*

In diesem Abschnitt soll nur kurz an einige elementare Eigenschaften der Kegelschnitte erinnert werden, in der Hoffnung, dass solch klassische Themen nicht ganz aus dem Mathematikunterricht verschwinden. Zur Vereinfachung bezeichnen wir die Koordinaten in der Ebene \mathbb{R}^2 mit x und y . Dann betrachten wir Kurven, die durch Gleichungen der folgenden Form definiert sind:

$$(1) \quad \frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

Ellipse

$$(2) \quad \frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$$

Hyperbel

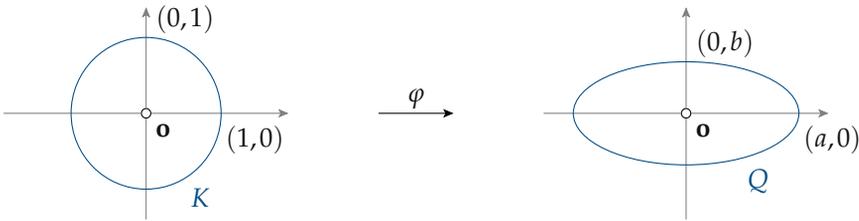
$$(3) \quad y = a \cdot x^2$$

Parabel

1. Ellipsen Der Einheitskreis $K \subset \mathbb{R}^2$ ist gegeben durch die Gleichung $x^2 + y^2 = 1$, sein Bild $Q = \varphi(K)$ bei der Abbildung

$$\varphi : \mathbb{R}^2 \rightarrow \mathbb{R}^2, (x, y) \mapsto (ax, by),$$

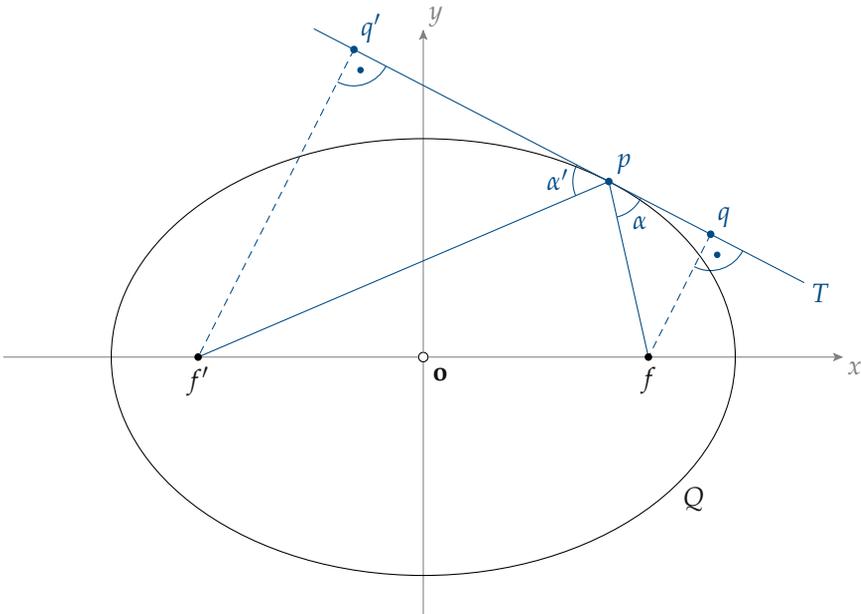
mit $a, b > 0$ hat die Gleichung $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$. Man kann $a \geq b$ annehmen, a und b sind die Längen der so genannten **Hauptachsen** der Ellipse Q .



Die Punkte $\pm(a, 0)$ und $\pm(0, b)$ heißen **Scheitelpunkte** der Ellipse. Nach der Voraussetzung $b \leq a$ ist

$$c := \sqrt{a^2 - b^2} \geq 0.$$

Die beiden Punkte $f := (c, 0)$ und $f' := (-c, 0)$ heißen **Brennpunkte** der Ellipse.



Um ihre besondere Bedeutung zu erklären, berechnen wir für jeden Punkt $p \in Q$ mit $p = (x_0, y_0)$ die Abstände

$$d(p, f) = a - \frac{c}{a} \cdot x_0 \quad \text{und} \quad d(p, f') = a + \frac{c}{a} \cdot x_0.$$

Daraus folgt sofort die Beziehung

$$d(p, f) + d(p, f') = 2a.$$

Sie ist Grundlage für die **Gärtnerkonstruktion** der Ellipse: Man befestigt eine Schnur der Länge $2a$ in den Brennpunkten und zeichnet mit gespanntem gleitendem Faden die Kurve.

Der Name „Brennpunkte“ erklärt sich aus einer physikalischen Eigenschaft: Ein von f ausgehender Lichtstrahl wird an Q so reflektiert, dass er durch f' geht. Um das zu begründen, muss man die Gleichung der Tangente T an Q im Punkt p bestimmen. Wie man in der Analysis lernt, steht der Gradient

$$2 \cdot \left(\frac{x_0}{a^2}, \frac{y_0}{b^2} \right)$$

der Gleichung von Q im Punkt p senkrecht auf T . Da auch $p \in T$ sein muss, erhält man als Gleichung von T

$$\frac{x_0}{a^2} \cdot x + \frac{y_0}{b^2} \cdot y = 1.$$

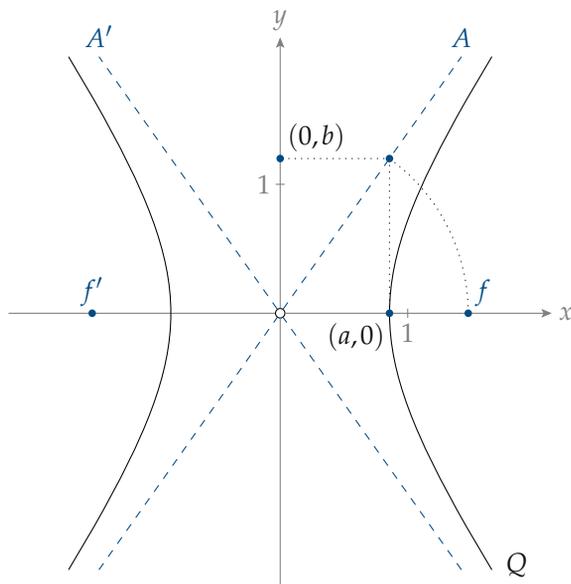
Um nachzuweisen, dass $\alpha = \alpha'$ gilt, genügt es zu zeigen, dass die Dreiecke p, q, f und p, q', f' ähnlich sind. Dazu kann man nachrechnen, dass

$$d(f, T) = d(f, q) = \beta \cdot d(f, p) \quad \text{und} \quad d(f', T) = d(f', q') = \beta \cdot d(f', p) \quad \text{mit einem } \beta \in \mathbb{R}_+.$$

2. Hyperbeln Die Gleichung der Hyperbel

$$Q = \left\{ (x, y) \in \mathbb{R}^2 : \frac{x^2}{a^2} - \frac{y^2}{b^2} = 1 \right\} \quad \text{mit } a, b > 0$$

unterscheidet sich „nur“ durch ein Vorzeichen von der Ellipsen-Gleichung, aber das Bild sieht ganz anders aus:



Die bei der Ellipse gemachte Voraussetzung $a > b$ ist hier überflüssig, man definiert

$$c := \sqrt{a^2 + b^2}, \quad \text{und} \quad f := (c, 0) \quad \text{sowie} \quad f' := (-c, 0)$$

heißen **Brennpunkte** der Hyperbel. Für die Abstände eines Punktes $p = (x_0, y_0) \in Q$ gilt

$$d(p, f) = \begin{cases} \frac{c}{a} \cdot x_0 - a & \text{für } x_0 > 0, \\ -\frac{c}{a} \cdot x_0 + a & \text{für } x_0 < 0, \end{cases} \quad \text{und} \quad d(p, f') = \begin{cases} \frac{c}{a} \cdot x_0 + a & \text{für } x_0 > 0, \\ -\frac{c}{a} \cdot x_0 - a & \text{für } x_0 < 0. \end{cases}$$

Also folgt für die Hyperbel die Abstandsbedingung

$$|d(p, f) - d(p, f')| = 2a.$$

Eine Besonderheit der Hyperbel sind die beiden Geraden A und A' mit den Gleichungen

$$y = \frac{b}{a} \cdot x \quad \text{und} \quad y = -\frac{b}{a} \cdot x,$$

sie heißen **Asymptoten** (d.h. „nicht zusammenfallende“ Geraden). Für großes $|x|$ nähert sich die Hyperbel den Asymptoten immer weiter an, ohne sie je zu treffen. Das sieht man am einfachsten, indem man die Hyperbelgleichung in folgender Form schreibt:

$$y = \pm \frac{b}{a} \cdot \sqrt{x^2 - a^2}.$$

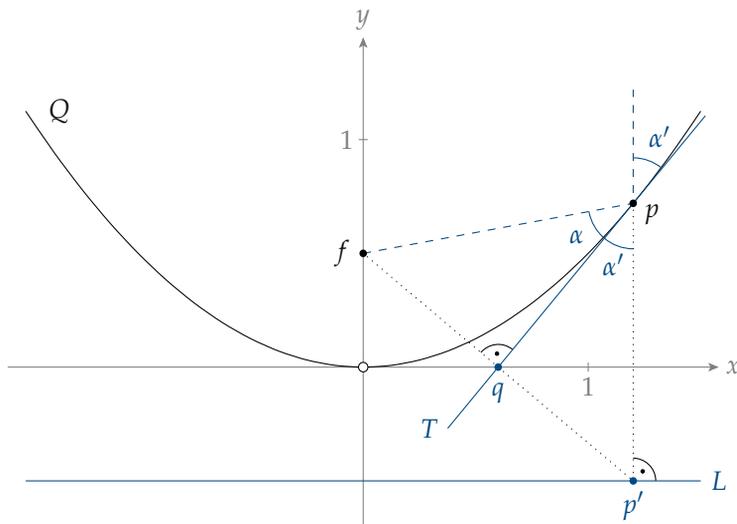
3. Parabeln Eine Parabel

$$Q = \left\{ (x, y) \in \mathbb{R}^2 : y = a \cdot x^2 \right\}, \quad a > 0,$$

kann als Grenzfall zwischen Ellipse und Hyperbel angesehen werden. Neben dem Scheitel o sind der **Brennpunkt**

$$f = (0, c) \quad \text{mit} \quad c = \frac{1}{4a}$$

und die **Leitgerade** L mit der Gleichung $y = -c$ von besonderer geometrischer Bedeutung. Ein Lichtstrahl, der vom Brennpunkt f ausgeht, wird an Q so reflektiert, dass er senkrecht nach oben geht; umgekehrt wird jeder senkrecht von oben kommende Strahl in den Brennpunkt reflektiert (das ist die mathematische Grundlage von Scheinwerfern und Antennenschüsseln). Um das nachzurechnen, betrachtet man die Tangente T an Q in $p = (x_0, y_0)$.



Für die Ableitung gilt $y' = 2a \cdot x$, also ist die Steigung der Tangente gleich

$$2a \cdot x_0 = \frac{2a \cdot x_0^2}{x_0} = \frac{y_0}{x_0/2}.$$

Daher geht T durch den Punkt $q = (\frac{x_0}{2}, 0)$, und mit elementargeometrischen Argumenten folgt, dass $\alpha = \alpha'$.

Eine Charakterisierung der Parabel durch eine Abstandseigenschaft ergibt sich sofort aus $d(f, p) = y_0 + c$. Demnach ist

$$Q = \left\{ p \in \mathbb{R}^2 : d(p, f) = d(p, L) \right\},$$

wobei $f = (0, c)$ und $L = \{(x, y) \in \mathbb{R}^2 : y = -c\}$ mit $c > 0$.

Bevor wir Kegelschnitte in allgemeiner Lage und ihre Verallgemeinerungen in höherer Dimension behandeln können, ist es hilfreich, die definierenden Gleichungen von einem abstrakteren Standpunkt zu betrachten und insbesondere mit symmetrischen Matrizen in Verbindung zu bringen. Das ist der Gegenstand der in 5.2 folgenden Abschnitte.

5.1.3 Kegelschnitte durch vorgegebene Punkte*

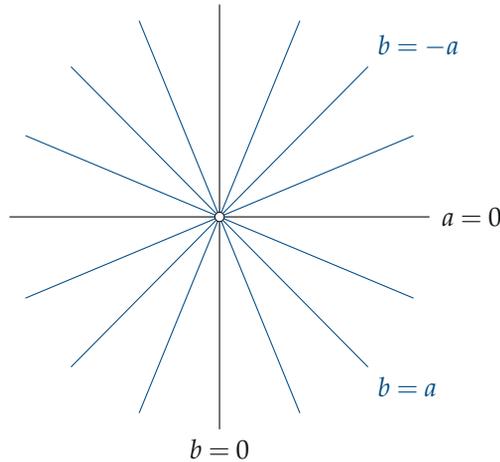
Eine Gerade ist bestimmt durch zwei Punkte; in der Ebene \mathbb{R}^2 ist sie definiert durch eine Gleichung

$$ax + by = c \quad \text{mit} \quad (a, b) \neq (0, 0),$$

wobei die drei Koeffizienten a, b, c nur bis auf einen Faktor festgelegt sind (Bemerkung in 0.2.3). Durch einen einzigen Punkt p gibt es ein ganzes *Büschel* von Geraden. Im einfachsten Fall der Ebene und $p = (0, 0)$ ist es gegeben durch die Gleichungen

$$ax + by = 0,$$

wobei $-a : b$ für $b \neq 0$ die Steigung der Geraden angibt; für $b = 0$ erhält man die Gerade $x = 0$ mit unendlicher Steigung.



Durch jeden Punkt außerhalb des Ursprungs geht genau eine Gerade des Büschels.

Nach diesen ganz einfachen Vorbemerkungen über Geraden nun zu den Kegelschnitten. Wie wir in 5.2.7 genauer erläutern werden, nennt man eine Teilmenge

$$Q = \{(x, y) \in \mathbb{R}^2 : f(x, y) = 0\} \subset \mathbb{R}^2$$

einen Kegelschnitt, wenn

$$f(x, y) = a_1x^2 + a_2xy + a_3y^2 + a_4x + a_5y + a_6,$$

wobei $a_1, \dots, a_6 \in \mathbb{R}$ und $(a_1, a_2, a_3) \neq (0, 0, 0)$. Typische Beispiele sind in 5.1.1 und 5.1.2 beschrieben. Wir wollen nun die folgende Frage behandeln:

Durch wie viele Punkte ist ein Kegelschnitt bestimmt?

Ist $p = (x, y) \in \mathbb{R}^2$, so ergibt die Bedingung $p \in Q$ eine lineare Gleichung für die sechs Koeffizienten a_1, \dots, a_6 . Sind Punkte p_1, \dots, p_n gegeben, so ergeben die Bedingungen $p_i \in Q$ für $i = 1, \dots, n$ ein homogenes System von n Gleichungen für die Koeffizienten a_1, \dots, a_6 . Da die Multiplikation von f mit einem Faktor $\neq 0$ die Nullstellenmenge Q nicht ändert, ist $n = 5$ die kritische Grenze für die sechs Koeffizienten. Das führt zu folgender

Definition Seien Punkte $p_i = (x_i, y_i) \in \mathbb{R}^2$, $i = 1, \dots, 5$, gegeben und sei $A \in M(5 \times 6; \mathbb{R})$ die Koeffizientenmatrix des homogenen linearen Gleichungssystems für die Unbekannten a_1, \dots, a_6 , das aus den Bedingungen

$$f(x_i, y_i) = 0 \quad \text{für } i = 1, \dots, 5$$

entsteht. Dann sagt man, p_1, \dots, p_5 befinden sich in **allgemeiner Lage**, wenn $\text{rang } A = 5$.

Um den geometrischen Hintergrund dieser algebraischen Bedingung besser zu verstehen, geben wir ganz einfache aber charakteristische Beispiele.

Beispiel 1 Es seien $p_1 = (1, 0)$, $p_2 = (-1, 0)$, $p_3 = (0, 0)$. Diese auf einer Geraden gelegenen Punkte ergeben eine Koeffizientenmatrix

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

und man sieht leicht, dass $\text{rang } A'' = 3$. Als Lösung des Gleichungssystems erhält man

$$a_2 = \lambda_1, a_3 = \lambda_2, a_5 = \lambda_3, a_1 = a_4 = a_6 = 0$$

mit $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$. Daraus ergeben sich die zulässigen Gleichungen

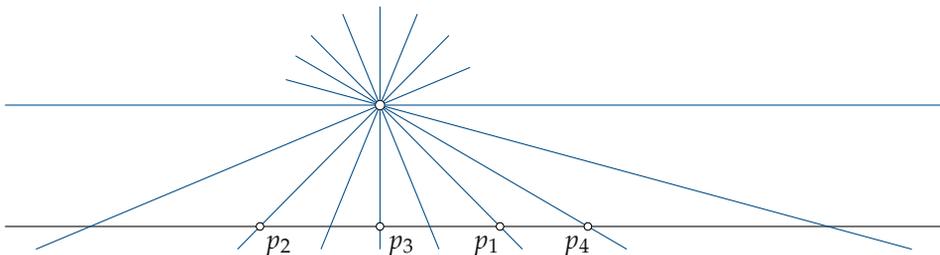
$$f(x, y) = y \cdot (\lambda_1 x + \lambda_2 y + \lambda_3) \quad \text{mit } (\lambda_1, \lambda_2) \neq (0, 0).$$

Die entsprechenden Kegelschnitte bestehen aus der Geraden $y = 0$, zusammen mit einer beliebigen weiteren Geraden.

Nimmt man zu p_1, p_2, p_3 einen vierten auf der Geraden $y = 0$ gelegenen Punkt, etwa $p_4 = (2, 0)$, dazu, so erhält man

$$A' = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 4 & 0 & 0 & 2 & 0 & 1 \end{pmatrix}$$

mit $\text{rang } A' = 3$. Man kann also keinen Punkt p_5 mehr finden, so dass p_1, \dots, p_5 in allgemeiner Lage sind. Ist etwa $p_5 = (0, 1)$, so gibt es durch p_1, \dots, p_5 unendlich viele Kegelschnitte. Sie bestehen aus der Geraden $y = 0$, zusammen mit einer Geraden durch p_5 .



Wählt man auch noch p_5 auf der Geraden $y = 0$, etwa $p_5 = (-2, 0)$, so ist

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

und $\text{rang } A = 3$. In diesem Fall ist die Gerade $y = 0$ zusammen mit einer beliebigen anderen Geraden ein Kegelschnitt durch p_1, \dots, p_5 .

Nimmt man zu den oben angegebenen Punkten p_1, p_2, p_3 noch zwei weitere Punkte p_4, p_5 außerhalb der Geraden $y = 0$ dazu, etwa $p_4 = (0, 1)$ und $p_5 = (0, -1)$, so erhält man

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

mit $\text{rang } A = 5$. Das entsprechende Gleichungssystem ist leicht zu lösen, das Ergebnis ist

$$a_2 = \lambda, \quad a_1 = a_3 = a_4 = a_5 = a_6 = 0 \quad \text{mit } \lambda \in \mathbb{R} \text{ beliebig.}$$

Für $\lambda = 1$ erhält man die Funktion $f(x, y) = x \cdot y$ und den aus zwei Geraden bestehenden Kegelschnitt

$$Q = \{(x, y) \in \mathbb{R}^2 : x \cdot y = 0\}.$$

Etwas allgemeiner gilt die folgende

Bemerkung Angenommen, p_1, \dots, p_5 liegen auf einer Geraden. Dann ist $\text{rang } A \leq 3$.

Beweis Angenommen, p_1, \dots, p_5 liegen auf der Geraden mit der Gleichung

$$g(x, y) := \alpha x + \beta y + \gamma = 0 \quad \text{mit } (\alpha, \beta) \neq (0, 0).$$

Dann liegen sie auch auf den Kegelschnitten mit den Gleichungen

$$x \cdot g(x, y) = 0, \quad y \cdot g(x, y) = 0 \quad \text{und} \quad (x + 1) \cdot g(x, y) = 0.$$

Das ergibt die Lösungen

$$(\alpha, \beta, 0, \gamma, 0, 0), \quad (0, \alpha, \beta, 0, \gamma, 0) \quad \text{und} \quad (\alpha, \beta, 0, \alpha + \gamma, \beta, \gamma)$$

des durch A gegebenen homogenen Gleichungssystems. Da sie linear unabhängig sind, ist $\dim \text{Lös}(A, \mathbf{0}) \geq 3$, also $\text{rang } A \leq 3$. ■

Beispiel 2 Nach der obligaten Diskussion der Ausnahmefälle kommen wir zu interessanteren Ergebnissen. Wählen wir

$$p_1 = (1,0), p_2 = (0,1), p_3 = (-1,0), p_4 = (0,-1),$$

so ergibt sich die Koeffizientenmatrix

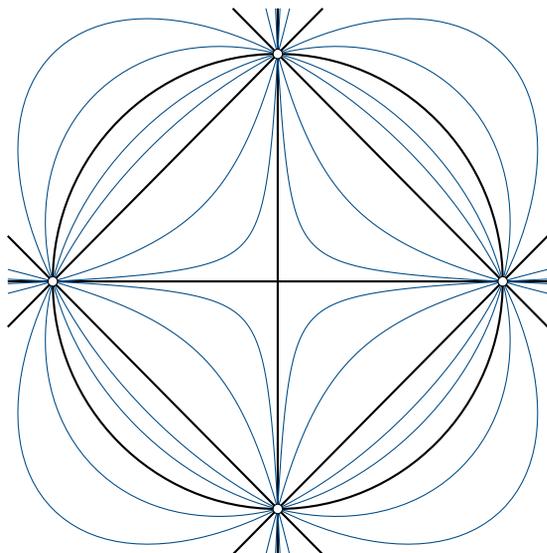
$$A' = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & 0 & -1 & 1 \end{pmatrix}, \quad \text{umgeformt zu} \quad \tilde{A}' = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 & 0 \end{pmatrix},$$

also die Lösung $a_2 = \lambda, a_6 = \mu, a_1 = a_3 = -\mu, a_4 = a_5 = 0$ mit den Parametern λ, μ . Da die Gleichung $f(x,y) = -\mu x^2 + \lambda xy - \mu y^2 + \mu$ nur bis auf einen Faktor $\neq 0$ festgelegt ist, genügt es die Fälle $\mu = 0$ und $\lambda = 1$, sowie $\mu = -1$ und λ beliebig zu betrachten. Wir erhalten

$$f(x,y) = xy, \quad \text{oder} \quad (1)$$

$$f(x,y) = x^2 + \lambda xy + y^2 - 1. \quad (2)$$

Gleichung (1) beschreibt ein Geradenpaar. Bei Gleichung (2) hängt der beschriebene Kegelschnitt Q_λ von λ ab. Wie in 5.2.7 auch theoretisch begründet wird, erhält man das im Bild zu sehende Ergebnis:



Für $-2 < \lambda < 2$ ist Q_λ eine Ellipse, Q_0 ist ein Kreis.

Für $\lambda = \pm 2$ erhält man ein Paar paralleler Geraden, denn

$$x^2 \pm 2xy + y^2 - 1 = (y \pm x + 1)(y \pm x - 1).$$

Für $\lambda < -2$ und $\lambda > 2$ ist Q_λ eine Hyperbel.

An dem Bild sieht man auch, dass es für jeden von p_1, \dots, p_4 verschiedenen Punkt p_5 genau einen der Kegelschnitte gibt, der durch p_1, \dots, p_5 geht. Man kann auch durch Rechnung beweisen, dass jede der entsprechenden Koeffizientenmatrizen A den Rang 5 hat. Allgemein gilt der

Satz Durch fünf Punkte p_1, \dots, p_5 in der Ebene \mathbb{R}^2 gibt es immer mindestens einen Kegelschnitt Q . Er ist genau dann eindeutig bestimmt, wenn sich die fünf Punkte in allgemeiner Lage befinden.

Beweis Es sei $A \in M(5 \times 6; \mathbb{R})$ die oben beschriebene Koeffizientenmatrix des aus den Punkten $p_1, \dots, p_5 \in \mathbb{R}^2$ erhaltenen linearen Gleichungssystems. Da $\text{rang } A \leq 5$, gibt es immer mindestens eine Lösung

$$(a_1, \dots, a_6) \in \mathbb{R}^6 \setminus \{\mathbf{0}\}.$$

Sei $f(x, y)$ die zu a_1, \dots, a_6 gehörende Funktion und

$$Q := \{(x, y) \in \mathbb{R}^2 : f(x, y) = 0\}.$$

Q ist nur dann ein Kegelschnitt im Sinne der Definition, wenn $(a_1, a_2, a_3) \neq (0, 0, 0)$.

Im Fall $a_1 = a_2 = a_3 = 0$ ist Q eine Gerade. Ist $L \subset \mathbb{R}^2$ eine beliebige weitere Gerade, so ist $Q' := Q \cup L$ ein Kegelschnitt durch p_1, \dots, p_5 . Durch Rechnung kann man das so sehen. Die Gerade Q ist beschrieben durch die Gleichung

$$a_4x + a_5y + a_6 = 0 \quad \text{mit} \quad (a_4, a_5) \neq (0, 0).$$

Dann ist etwa

$$Q' := \{(x, y) \in \mathbb{R}^2 : x \cdot (a_4x + a_5y + a_6) = 0\}$$

ein Kegelschnitt durch p_1, \dots, p_5 .

Q ist genau dann eindeutig bestimmt, wenn $\dim \text{Lös}(A, \mathbf{0}) = 1$, das ist gleichwertig mit $\text{rang } A = 5$. ■

Beispiele mit beliebig vorgegebenen fünf Punkten kann man bei *MatheVital* betrachten.

Die allgemeine Lage von fünf Punkten in der Ebene hatten wir dadurch erklärt, dass der Rang der so erhaltenen Matrix A maximal sein muss. Der geometrische Hintergrund dieser algebraischen Bedingung ist nicht direkt einsichtig, daher wollen wir noch etwas einfachere Bedingungen an die fünf Punkte betrachten.

Zunächst ist es hilfreich, zwei Arten von Kegelschnitten zu unterscheiden: Ein Kegelschnitt heißt *reduzibel*, wenn er eine Gerade enthält, und *irreduzibel*, wenn er keine

Gerade enthält. Typische Beispiele für reduzible Kegelschnitte sind gegeben durch die Gleichungen

$$x \cdot y = 0, \quad x \cdot (x - 1) = 0, \quad x^2 = 0.$$

Geometrisch gesehen sind das zwei sich schneidende Geraden, zwei parallele Geraden oder eine „Doppelgerade“. Dagegen sind Ellipsen, Hyperbeln und Parabeln irreduzibel.

Wie wir in 5.2.7 nachweisen werden, besteht jeder reduzible Kegelschnitt aus zwei Geraden, die auch zusammenfallen können. Das wird im Folgenden schon benutzt.

Ganz entscheidend sind die folgenden Schnitt-Eigenschaften:

- 1) Ist Q ein Kegelschnitt und L eine Gerade, so ist entweder $L \subset Q$, oder $Q \cap L$ besteht aus höchstens zwei Punkten.
- 2) Zwei verschiedene irreduzible Kegelschnitte schneiden sich in höchstens vier Punkten.

Der Beweis von 1) ist ganz elementar. Ist Q gegeben durch $f(x, y) = 0$ und geht die Gerade L durch die verschiedenen Punkte (x_1, y_1) und (x_2, y_2) , so kann man zur Bestimmung der Schnittpunkte von Q mit L die Werte

$$x = x_1 + \lambda \cdot (x_2 - x_1) \quad \text{und} \quad y = y_1 + \lambda \cdot (y_2 - y_1)$$

in f einsetzen, das ergibt ein Polynom $\varphi(\lambda)$ vom Grad höchstens 2. Ist φ das Nullpolynom, so folgt $L \subset Q$. In diesem Fall muss Q reduzibel sein. Ist φ nicht das Nullpolynom, so hat es nach Korollar 1 aus 1.4.4 höchstens zwei Nullstellen, also gibt es höchstens zwei Schnittpunkte.

Teil 2) ist ein einfacher Spezialfall des allgemeinen Satzes von BÉZOUT über algebraische Kurven. Einen Beweis findet man etwa in [FI₄, 2.7]. ■

Als Folgerung der Schnitt-Eigenschaft 2) erhalten wir das

Korollar Durch fünf Punkte p_1, \dots, p_5 im \mathbb{R}^2 , von denen keine drei auf einer Geraden liegen, geht genau ein Kegelschnitt Q , und dieser ist irreduzibel.

Beweis Wäre Q reduzibel, so müssten von p_1, \dots, p_5 mindestens drei auf einer Geraden liegen. Angenommen es gäbe zwei verschiedene irreduzible Kegelschnitte Q_1 und Q_2 die durch die fünf Punkte gehen; das wäre ein Widerspruch zur Schnitt-Eigenschaft 2) ■

Einen Beweis dieses Korollars, der die allgemeine Schnitteigenschaft durch ein direkteres Argument ersetzt, findet man etwa in [R-O, Satz 5.3].

Die Ergebnisse dieses Abschnitts fassen wir noch einmal zusammen.

Gegeben $p_1, \dots, p_5 \in \mathbb{R}^2$. Dann gilt für die Kegelschnitte Q durch p_1, \dots, p_5 :

- a) Es gibt immer mindestens ein Q .
- b) Sind keine drei Punkte kollinear, so gibt es genau ein irreduzibles Q .
- c) Sind genau drei Punkte kollinear, so ist Q reduzibel und eindeutig.
- d) Sind mindestens vier Punkte kollinear, so ist Q reduzibel und nicht eindeutig.

5.1.4 Pol und Polare*

Ein weiterer Zusammenhang mit der linearen Algebra ergibt sich, indem man Tangenten an einen Kegelschnitt betrachtet. Im einfachsten Fall haben wir einen Einheitskreis um den Ursprung, also

$$Q = \{(x_1, x_2) \in \mathbb{R}^2 : x_1^2 + x_2^2 = 1\}.$$

Um die Gleichung der Tangente T_q an Q im Punkt $q = (q_1, q_2) \in Q$ zu bestimmen, benutzen wir die Tatsache, dass der Vektor q auf T_q senkrecht steht und dass $q \in T_q$. Also ist

$$T_q = \{(x_1, x_2) \in \mathbb{R}^2 : q_1 x_1 + q_2 x_2 = 1\}.$$

Ist $q' = (q'_1, q'_2) \in Q$ ein weiterer Punkt, so kann man den Schnittpunkt

$$p = (p_1, p_2) = T_q \cap T_{q'}$$

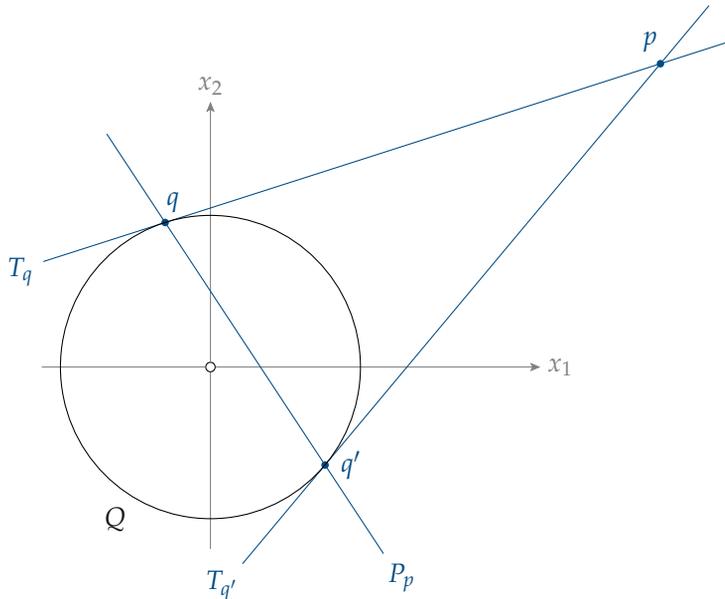
etwa mit Hilfe der CRAMERSchen Regel berechnen als

$$p_1 = \frac{q'_2 - q_2}{q_1 q'_2 - q_2 q'_1}, \quad p_2 = \frac{q_1 - q'_1}{q_1 q'_2 - q_2 q'_1},$$

falls die Vektoren q, q' linear unabhängig sind. In diesem Fall betrachten wir die Gerade

$$P_p := \{(x_1, x_2) \in \mathbb{R}^2 : p_1 x_1 + p_2 x_2 = 1\}.$$

Wie man ganz leicht nachrechnet, liegen die Punkte q und q' auf P_p , also ist P_p die Verbindungsgerade von q und q' . Man nennt die Gerade P_p die **Polare** zum **Pol** p relativ zum Kreis Q .



Mit Hilfe der Polaren kann man nun für einen Punkt $p = (a, b)$ außerhalb des Kreises, d.h. $a^2 + b^2 > 1$, die durch p gehenden Tangenten an den Kreis finden: Die Koordinaten der Berührungspunkte müssen die beiden Gleichungen

$$x_1^2 + x_2^2 = 1 \quad \text{und} \quad ax_1 + bx_2 = 1$$

erfüllen. Ist etwa $b \neq 0$, so kann man

$$x_2 = \frac{1}{b}(1 - ax_1)$$

in die quadratische Gleichung einsetzen, das ergibt

$$(a^2 + b^2)x_1^2 - 2ax_1 + (1 - b^2) = 0. \quad (*)$$

Die Diskriminante dieser Gleichung ist

$$4a^2 - 4(a^2 + b^2)(1 - b^2) = 4b^2(a^2 + b^2 - 1),$$

daraus erhält man die Lösungen

$$x_1 = \frac{a \pm b \cdot \sqrt{a^2 + b^2 - 1}}{a^2 + b^2}.$$

Liegt der Punkt $p = (a, b)$ auf dem Kreis, d.h. $a^2 + b^2 = 1$, so ist die Polare P_p gleich der Tangente T_p und $p \in P_p$.

Liegt der Punkt $p = (a, b)$ im Inneren des Kreises und ist vom Ursprung verschieden, so ist $0 < a^2 + b^2 < 1$. Auch in diesem Fall kann man eine Polare

$$P_p := \{(x_1, x_2) \in \mathbb{R}^2 : ax_1 + bx_2 = 1\}$$

erklären, aber von diesen Punkten kann man keine Tangente mehr an den Kreis legen; in der Gleichung (*) wird die Diskriminante negativ. In diesem Fall betrachten wir den Punkt

$$q := \frac{1}{a^2 + b^2}(a, b).$$

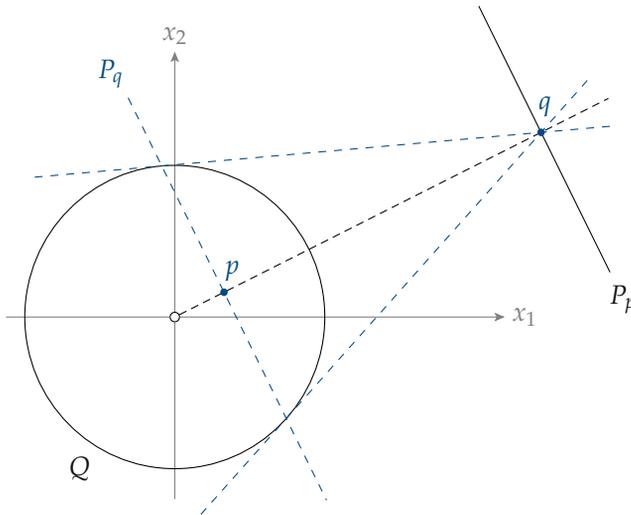
Offensichtlich ist $q \in P_p$, und für den Abstand von P_p zum Ursprung gilt

$$d(\mathbf{o}, P_p) = \|q\| = \frac{1}{\|p\|^2} \cdot \|p\| = \frac{1}{\|p\|}.$$

Die Abbildung

$$\mathbb{R}^2 \setminus \{\mathbf{o}\} \rightarrow \mathbb{R}^2 \setminus \{\mathbf{o}\}, p = (a, b) \mapsto q = \frac{1}{\|p\|^2} \cdot p,$$

kann man als eine Spiegelung am Einheitskreis ansehen. Es gilt nicht nur $q \in P_p$, sondern auch umgekehrt $p \in P_q$.



Den Zusammenhang zwischen Pol und Polare bezüglich des Kreises kann man auch etwas abstrakter durch das kanonische Skalarprodukt im \mathbb{R}^2 beschreiben: Ist der Pol gegeben durch $y = (y_1, y_2)$, so ist die Polare gleich

$$P_y = \{x \in \mathbb{R}^2 : \langle x, y \rangle = 1\}.$$

Diese Beschreibung kann man leicht auf beliebige Kegelschnitte verallgemeinern.

5.2 Bilinearformen

5.2.1 Definitionen und beschreibende Matrix

In 0.3.1 hatten wir die grundlegenden Rechenregeln für das Skalarprodukt im \mathbb{R}^n vermerkt. In einer allgemeineren Situation führt das zu folgenden Begriffen.

Definition Sei K ein Körper und V ein K -Vektorraum. Eine Abbildung

$$s : V \times V \rightarrow K$$

heißt **bilinear** (oder **Bilinearform**), wenn für alle $v, v', w, w' \in V$ und $\lambda \in K$ folgendes gilt:

B1 $s(v + v', w) = s(v, w) + s(v', w), \quad s(\lambda \cdot v, w) = \lambda \cdot s(v, w).$

B2 $s(v, w + w') = s(v, w) + s(v, w'), \quad s(v, \lambda \cdot w) = \lambda \cdot s(v, w).$

Eine Bilinearform s heißt **symmetrisch**, wenn für alle $v, w \in V$

$$s(w, v) = s(v, w)$$

gilt, und **alternierend** (oder **schiefssymmetrisch**), wenn

$$s(w, v) = -s(v, w)$$

gilt.

Standardbeispiel für eine symmetrische Bilinearform ist das kanonische Skalarprodukt im \mathbb{R}^n , wobei

$$s(x, y) = \langle x, y \rangle = {}^t x \cdot y = \sum_{i=1}^n x_i y_i \quad \text{für} \quad x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \quad \text{und} \quad y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Es gibt aber auch ganz andersartige Beispiele, etwa im unendlich-dimensionalen Vektorraum $V = \mathcal{C}(I; \mathbb{R})$ der stetigen Funktionen auf einem Intervall $I = [a, b] \subset \mathbb{R}$. Da stetige Funktionen auf I integrierbar sind, hat man eine Abbildung

$$V \times V \rightarrow \mathbb{R}, (f, g) \mapsto \int_a^b f(t) \cdot g(t) dt.$$

Nach den Rechenregeln für Integrale ist diese Abbildung bilinear. Sie wird etwa in der Theorie der **FOURIER-Reihen** entscheidend benutzt (vgl. etwa [FO₁, §23]).

Lineare Abbildungen zwischen endlich-dimensionalen Vektorräumen kann man mit Hilfe von Basen durch Matrizen beschreiben. Ähnlich – aber doch etwas anders – geht das mit Bilinearformen. Sei also V ein Vektorraum, s eine Bilinearform auf V und

$\mathcal{B} = (v_1, \dots, v_n)$ eine Basis von V . Dann kann man die speziellen Werte $a_{ij} = s(v_i, v_j)$ in einer Matrix A zusammenfassen, und

$$M_{\mathcal{B}}(s) := (s(v_i, v_j)) = A \in M(n \times n; K)$$

heißt die **darstellende Matrix** der Bilinearform s bezüglich der Basis \mathcal{B} .

Mit Hilfe der darstellenden Matrix kann man die Werte $s(v, w)$ leicht ausrechnen. Das sieht man besonders einfach im Fall $\dim V = 2$. Sei also $\mathcal{B} = (v_1, v_2)$ eine Basis von V und

$$v = x_1 v_1 + x_2 v_2, \quad w = y_1 v_1 + y_2 v_2, \quad x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \quad y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}.$$

Dann ist wegen B1 und B2

$$\begin{aligned} s(v, w) &= s(x_1 v_1 + x_2 v_2, y_1 v_1 + y_2 v_2) \\ &= x_1 y_1 \cdot s(v_1, v_1) + x_1 y_2 \cdot s(v_1, v_2) + x_2 y_1 \cdot s(v_2, v_1) + x_2 y_2 \cdot s(v_2, v_2) \\ &= a_{11} \cdot x_1 y_1 + a_{12} \cdot x_1 y_2 + a_{21} \cdot x_2 y_1 + a_{22} \cdot x_2 y_2 \\ &= (x_1, x_2) \cdot \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = {}^t x \cdot A \cdot y. \end{aligned}$$

Ist s symmetrisch, so ist $s(v_2, v_1) = s(v_1, v_2)$, also $a_{21} = a_{12}$, d.h. A ist symmetrisch. Ist umgekehrt $a_{21} = a_{12}$, so folgt

$$s(w, v) = (y_1, y_2) \cdot \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = s(v, w).$$

Das ist ein Spezialfall von folgendem allgemeinen

Lemma Sei s eine Bilinearform auf V , $\mathcal{B} = (v_1, \dots, v_n)$ eine Basis von V und $A = M_{\mathcal{B}}(s)$ die darstellende Matrix. Ist

$$v = \sum_{i=1}^n x_i v_i \quad \text{und} \quad w = \sum_{i=1}^n y_i v_i, \quad \text{so folgt} \quad s(v, w) = \sum_{i,j=1}^n a_{ij} \cdot x_i y_j.$$

Diese Beziehung kann man auch in Matrizen schreiben:

$$\text{Ist } x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \quad \text{und} \quad y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}, \quad \text{so folgt} \quad s(v, w) = {}^t x \cdot A \cdot y.$$

Weiter gilt: s symmetrisch $\Leftrightarrow M_{\mathcal{B}}(s)$ symmetrisch.

Beweis Man rechnet wie im Spezialfall $n = 2$, nun aber mit Summenzeichen:

$$s(v, w) = s\left(\sum_{i=1}^n x_i v_i, \sum_{j=1}^n y_j v_j\right) = \sum_{i,j=1}^n x_i y_j \cdot s(v_i, v_j) = \sum_{i,j=1}^n a_{ij} \cdot x_i y_j.$$

Ist s symmetrisch, so ist $a_{ij} = s(v_i, v_j) = s(v_j, v_i) = a_{ji}$. Ist umgekehrt A symmetrisch, also $A = {}^tA$, so folgt nach den Rechenregeln für Matrizen

$$s(v, w) = {}^t(s(v, w)) = {}^t({}^tx \cdot A \cdot y) = {}^ty \cdot {}^tA \cdot x = {}^ty \cdot A \cdot x = s(w, v). \quad \blacksquare$$

Obiges Lemma zeigt insbesondere, dass im Fall $V = \mathbb{R}^n$ jede beliebige Bilinearform s in engem Zusammenhang steht mit dem kanonischen Skalarprodukt $\langle \cdot, \cdot \rangle$, denn für Spaltenvektoren $x, y \in \mathbb{R}^n$ ist

$$s(x, y) = {}^tx \cdot A \cdot y = \langle x, A \cdot y \rangle = \langle {}^tA \cdot x, y \rangle,$$

denn $\langle {}^tA \cdot x, y \rangle = ({}^tA \cdot x) \cdot y = {}^tx \cdot A \cdot y$. Ist A symmetrisch, so gilt insbesondere

$$\langle x, A \cdot y \rangle = \langle A \cdot x, y \rangle.$$

In diesem Fall kann man also die Matrix A in der Klammer nach vorne „wälzen“. Der einfachste Fall ist $A = E_n$, dann gilt

$$s(x, y) = \langle x, E_n \cdot y \rangle = \langle x, y \rangle.$$

Zu einer symmetrischen Bilinearform $s : V \times V \rightarrow K$ kann man eine neue Abbildung

$$q_s : V \rightarrow K, \quad q_s(v) := s(v, v),$$

erklären. q_s heißt die zu s gehörige **quadratische Form** auf V .

Ist $V = K^n$, und s gegeben durch die symmetrische Matrix $A = (a_{ij})$, so ist

$$q_s(x) = {}^tx \cdot A \cdot x = \sum_{i,j=1}^n a_{ij} \cdot x_i x_j = \sum_{i=1}^n a_{ii} \cdot x_i^2 + 2 \cdot \sum_{1 \leq i < j \leq n} a_{ij} \cdot x_i x_j.$$

Ist $\text{char}(K) \neq 2$, so kann man eine symmetrische Bilinearform s aus q_s rekonstruieren, denn $q_s(v+w) = s(v+w, v+w) = q_s(v) + q_s(w) + 2 \cdot s(v, w)$, also

$$s(v, w) = \frac{1}{2} \cdot (q_s(v+w) - q_s(v) - q_s(w)).$$

Dieses Verfahren nennt man **Polarisierung** (vgl. dazu 5.1.4).

Beispiel Im Polynomring $\mathbb{R}[X]$ betrachten wir für beliebiges $n \in \mathbb{N}$ die linear unabhängige Familie

$$\mathcal{B} := (1, X, X^2, \dots, X^n).$$

Auf $V := \text{Span}_{\mathbb{R}}(\mathcal{B})$ ist durch

$$s(f, g) := \int_0^1 f(t) \cdot g(t) dt$$

eine symmetrische Bilinearform gegeben. Da

$$\int_0^1 t^k t^l dt = \frac{1}{k+l+1}, \quad \text{ist} \quad M_{\mathcal{B}}(s) = \begin{pmatrix} 1 & \frac{1}{2} & \cdots & \frac{1}{1+n} \\ \frac{1}{2} & \frac{1}{3} & \cdots & \frac{1}{n+2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{n+1} & \frac{1}{n+2} & \cdots & \frac{1}{2n+1} \end{pmatrix}.$$

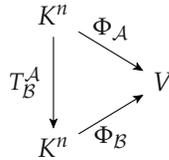
Das ist die tückische **HILBERT-Matrix**.

5.2.2 Transformationsformel für darstellende Matrizen

In 2.5.2 hatten wir für einen Endomorphismus $F : V \rightarrow V$ die darstellenden Matrizen $A = M_{\mathcal{A}}(F)$ und $B = M_{\mathcal{B}}(F)$ mit Hilfe der Transformationsmatrix $S = T_{\mathcal{B}}^{\mathcal{A}}$ umgerechnet:

$$M_{\mathcal{B}}(F) = T_{\mathcal{B}}^{\mathcal{A}} \cdot M_{\mathcal{A}}(F) \cdot T_{\mathcal{A}}^{\mathcal{B}}, \quad \text{kurz} \quad B = S \cdot A \cdot S^{-1}.$$

Will man für eine Bilinearform s auf V eine Basis finden, bezüglich derer die darstellende Matrix besonders einfach wird, muss man die Regel für die Umrechnung kennen. Sind auf V Basen \mathcal{A} und \mathcal{B} gegeben, so hat man ein Diagramm



mit den Koordinatensystemen $\Phi_{\mathcal{A}}$ und $\Phi_{\mathcal{B}}$, sowie der Koordinatentransformation $S = T_{\mathcal{B}}^{\mathcal{A}}$. Für $v, w \in V$ gibt es eindeutig bestimmte

$$\begin{array}{l}
 x, x' \in K^n \\
 y, y' \in K^n
 \end{array}
 \quad \text{mit} \quad
 \begin{array}{l}
 v = \Phi_{\mathcal{A}}(x) = \Phi_{\mathcal{B}}(x') \\
 w = \Phi_{\mathcal{A}}(y) = \Phi_{\mathcal{B}}(y')
 \end{array}
 \quad \text{also} \quad
 \begin{array}{l}
 x' = S \cdot x \\
 y' = S \cdot y.
 \end{array}$$

Ist $A := M_{\mathcal{A}}(s)$ und $B := M_{\mathcal{B}}(s)$, so hat man nach dem Lemma aus 5.2.1 die zwei möglichen Darstellungen

$${}^t x \cdot A \cdot y = s(v, w) = {}^t x' \cdot B \cdot y' = {}^t(S \cdot x) \cdot B \cdot (S \cdot y) = {}^t x \cdot ({}^t S \cdot B \cdot S) \cdot y.$$

Da diese Beziehung für alle $x, y \in K^n$ gilt, folgt

$$A = {}^t S \cdot B \cdot S \quad \text{und somit} \quad B = {}^t S^{-1} \cdot A \cdot S^{-1}.$$

Denn ist allgemein ${}^t x \cdot A \cdot y = {}^t x \cdot C \cdot y$ für alle $x, y \in K^n$, so folgt durch Einsetzen von $x = e_i$ und $y = e_j$, dass $a_{ij} = c_{ij}$. Damit haben wir folgendes bewiesen:

Transformationsformel für Bilinearformen *Ist in einem K -Vektorraum V eine Bilinearform s durch zwei Basen \mathcal{A} und \mathcal{B} dargestellt, so gilt*

$$M_{\mathcal{A}}(s) = {}^t T_{\mathcal{B}}^{\mathcal{A}} \cdot M_{\mathcal{B}}(s) \cdot T_{\mathcal{B}}^{\mathcal{A}}. \quad \blacksquare$$

Die beiden Transformationsformeln kann man noch einmal vergleichen: Ist $S := T_{\mathcal{B}}^{\mathcal{A}}$, so gilt

$$\begin{array}{ll}
 A = S^{-1} \cdot B \cdot S & \text{und} \quad B = S \cdot A \cdot S^{-1} & \text{bei Endomorphismen,} \\
 A = {}^t S \cdot B \cdot S & \text{und} \quad B = {}^t S^{-1} \cdot A \cdot S^{-1} = {}^t T A T & \text{mit } T = S^{-1} \text{ bei Bilinearformen.}
 \end{array}$$

Daran erkennt man, dass der Fall $S^{-1} = {}^t S$ besonders interessant ist. Solche Matrizen heißen im Fall $K = \mathbb{R}$ „orthogonal“ (vgl. 5.3.4).

5.2.3 Entartung und Rang einer Bilinearform

Endomorphismen und Bilinearformen eines Vektorraums V sind verschiedenartige Abbildungen, sie können aber beide bezüglich einer Basis von V durch eine quadratische Matrix A beschrieben werden. Bei Endomorphismen ist der Rang von A gleich der Dimension des Bildes, das ist nach der Dimensionsformel aus 2.3.4 durch die Dimension des Kerns bestimmt. Für eine Bilinearform

$$s : V \times V \rightarrow K$$

kann man ein Analogon zum Kern eines Endomorphismus erklären. Dabei ist zu bedenken, dass die Teilmenge

$$\{v \in V : s(v, v) = 0\} \subset V$$

im Allgemeinen kein Untervektorraum ist. Etwa für $V = \mathbb{R}^2$ und

$$s(x, y) = {}^t x \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot y \quad \text{ist} \quad s(x, x) = x_1^2 - x_2^2,$$

und $\{x \in \mathbb{R}^2 : x_1^2 - x_2^2 = 0\}$ ist ein Paar von Geraden. Besser geht es so:

Definition Für eine symmetrische Bilinearform s auf V sei

$$V_0(s) := \{v \in V : s(v, w) = 0 \text{ für alle } w \in V\}.$$

$V_0(s)$ heißt *Ausartungsraum* von s in V .

Man beachte, dass V_0 wegen der vorausgesetzten Symmetrie von s nicht von der Reihenfolge der Argumente v und w abhängt.

Aus der Bilinearität von s folgt unmittelbar, dass $V_0(s) \subset V$ ein Untervektorraum ist, also kann man

$$\text{rang}(s) := \dim V - \dim V_0(s)$$

als *Rang* der symmetrischen Bilinearform s erklären.

Beispiel Ist $V = \mathbb{R}^3$ und

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

so sei $s(x, y) := {}^t x \cdot A \cdot y$. Da ${}^t x \cdot A = (x_1, -x_2, 0)$, ist

$$x \in V_0 \Leftrightarrow x_1 y_1 - x_2 y_2 = 0 \text{ für alle } y \in \mathbb{R}^3.$$

Setzt man $y = e_1$, so folgt $x_1 = 0$, mit $y = e_2$ folgt $x_2 = 0$. Also ist in diesem Fall

$$V_0(s) = \mathbb{R} \cdot e_3, \quad \text{rang}(s) = 2 = \text{rang} A.$$

Das ist ein Spezialfall von folgendem

Lemma Ist s eine symmetrische Bilinearform auf V und \mathcal{B} eine Basis, so gilt

$$\text{rang}(s) = \text{rang } M_{\mathcal{B}}(s).$$

Genauer gilt: Ist $A := M_{\mathcal{B}}(s)$, $\Phi_{\mathcal{B}} : K^n \rightarrow V$ das zu \mathcal{B} gehörende Koordinatensystem und

$$L := \{x \in K^n : A \cdot x = \mathbf{o}\}$$

der Lösungsraum des homogenen linearen Gleichungssystems, so gilt

$$V_0(s) = \Phi_{\mathcal{B}}(L).$$

Beweis Ist $v = \Phi_{\mathcal{B}}(x)$ und $w = \Phi_{\mathcal{B}}(y)$, so gilt $s(v, w) = {}^t x \cdot A \cdot y$.

Ist $x' = {}^t x \cdot A = (x'_1, \dots, x'_n) \in K^n$, so gilt

$$x'_1 y_1 + \dots + x'_n y_n = 0 \text{ für alle } y \in K^n \Leftrightarrow x'_1 = \dots = x'_n = 0.$$

Das sieht man leicht, indem man $y = e_i$ für $i = 1, \dots, n$ einsetzt. Also folgt

$$v \in V_0(s) \Leftrightarrow {}^t x \cdot A = \mathbf{o} \Leftrightarrow {}^t A \cdot x = \mathbf{o} \Leftrightarrow A \cdot x = \mathbf{o} \Leftrightarrow x \in L,$$

da $A = {}^t A$. ■

Schließlich nennt man eine symmetrische Bilinearform s **nicht entartet**, wenn

$$V_0(s) = \{\mathbf{o}\}.$$

Nach dem obigen Lemma ist das gleichwertig mit

$$\text{rang } M_{\mathcal{B}}(s) = \dim V$$

für eine – und damit auch für jede – Basis \mathcal{B} von V .

Das einfachste Beispiel für eine nicht entartete symmetrische Bilinearform ist das kanonische Skalarprodukt im \mathbb{R}^n . Ist $x \in \mathbb{R}^n$ mit $\langle x, y \rangle = 0$ für alle $y \in \mathbb{R}^n$, so steht x senkrecht auf allen y ; das geht nur für $x = \mathbf{o}$.

5.2.4 Diagonalisierung einer symmetrischen Bilinearform

Wie wir in 4.2.2 gesehen hatten, gibt es für die Diagonalisierung eines Endomorphismus markante Hindernisse. Im Fall einer symmetrischen Bilinearform $s : V \times V \rightarrow K$ ist das viel einfacher. Hier ist eine Basis $\mathcal{B} = (v_1, \dots, v_n)$ von V gesucht, derart dass

$$s(v_i, v_j) = 0 \text{ für } i \neq j.$$

Eine derartige Basis von V nennt man **orthogonal** für s . In Matrizen ausgedrückt ist zu einer symmetrischen Matrix $A \in M(n \times n; K)$ ein $T \in GL(n; K)$ gesucht, so dass

$${}^tT \cdot A \cdot T = D = \begin{pmatrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_n \end{pmatrix}$$

eine Diagonalmatrix ist. In diesem Fall bilden die Spaltenvektoren von T eine orthogonale Basis des K^n für A , denn

$${}^t(T \cdot e_i) \cdot A \cdot (T \cdot e_j) = {}^t e_i \cdot ({}^tT \cdot A \cdot T) \cdot e_j = {}^t e_i \cdot D \cdot e_j = 0 \quad \text{für } i \neq j.$$

Man beachte, dass diese sehr allgemeine Art von „Orthogonalität“ nur in Analogie zum kanonischen Skalarprodukt im \mathbb{R}^n erklärt ist, aber nichts mit einem „Winkel“ zu tun hat.

Gegen die Diagonalisierung einer Bilinearform gibt es zwei ziemlich offensichtliche Hindernisse.

Beispiel 1 Die Matrix

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

ist nicht symmetrisch. Für eine beliebige Matrix

$$T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{ist} \quad {}^tTAT = \begin{pmatrix} ac & ad \\ bc & bd \end{pmatrix}.$$

Soll $ad = bc = 0$ sein, so folgt $\det T = 0$; also kann T nicht invertierbar sein.

Beispiel 2 Ist $\text{char}(K) = 2$, so betrachten wir

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

Für eine beliebige Matrix

$$T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{ist} \quad {}^tTAT = \begin{pmatrix} ac + ca & ad + cb \\ bc + da & bd + db \end{pmatrix} =: B.$$

Da $ac + ca = 0$ und $bd + db = 0$ gilt, muss die Diagonale von B Null sein; da $ad + cb = bc + da = \det T$, kann B keine Diagonalmatrix sein.

Zum Glück gibt es keine weiteren Hindernisse:

Diagonalisierungssatz Sei K ein Körper mit $\text{char}(K) \neq 2$, V ein n -dimensionaler K -Vektorraum und s eine symmetrische Bilinearform auf V . Dann gibt es für s eine orthogonale Basis $\mathcal{B} = (v_1, \dots, v_n)$ von V , d.h. $M_{\mathcal{B}}(s)$ ist eine Diagonalmatrix.

Ist $q_s : V \rightarrow K$ die zu s gehörige quadratische Form, und $\alpha_i := q_s(v_i) = s(v_i, v_i)$, so gilt

$$q_s(v) = \alpha_1 x_1^2 + \dots + \alpha_n x_n^2 \quad \text{für } v = x_1 v_1 + \dots + x_n v_n.$$

Die quadratische Form ist also in diesen Koordinaten frei von „gemischten Termen“ $x_i x_j$ ($i \neq j$).

Zusammen mit der Transformationsformel aus 5.2.2 folgt das

Korollar Ist \mathcal{A} eine beliebige Basis von V , und $A := M_{\mathcal{A}}(s)$, so gibt es ein $T \in \text{GL}(n; K)$ mit

$${}^tT \cdot A \cdot T = D := \begin{pmatrix} \alpha_1 & & & & & \\ & \ddots & & & & \\ & & \alpha_r & & & \\ & & & 0 & & \\ & 0 & & & \ddots & \\ & & & & & 0 \end{pmatrix},$$

wobei $r = \text{rang}(s)$ und $\alpha_1, \dots, \alpha_r \in K^*$. ■

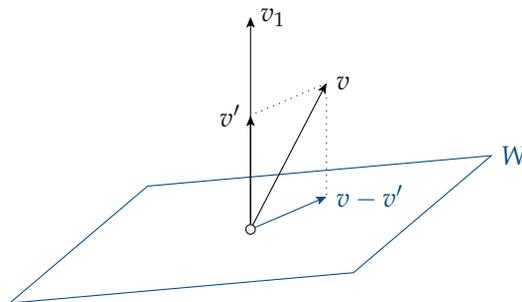
Beweis des Satzes Wir führen Induktion über $n = \dim V$. Für $n = 1$ ist nichts zu beweisen. Ist $q_s(v) = 0$ für alle $v \in V$, so ist nach der wegen $\text{char}(K) \neq 2$ möglichen Polarisierung aus 5.2.1 auch $s(v, w) = 0$ für alle Vektoren $v, w \in V$. Andernfalls gibt es ein $v_1 \in V$ mit $q_s(v_1) = s(v_1, v_1) \neq 0$; dazu betrachten wir den Untervektorraum

$$W := \{w \in V : s(v_1, w) = 0\} \subset V.$$

Wir behaupten, dass $V = K \cdot v_1 \oplus W$, d.h.

$$V = K \cdot v_1 + W \quad \text{und} \quad K \cdot v_1 \cap W = \{\mathbf{0}\}.$$

Zum Nachweis der ersten Bedingung müssen wir jedes $v \in V$ geeignet zerlegen. Dazu suchen wir ein $\alpha \in K$ derart, dass $v - v' \in W$ für $v' = \alpha \cdot v_1$.



Die Bedingung für $v - v' \in W$ lautet

$$0 = s(v_1, v - v') = s(v_1, v) - s(v_1, v') = s(v_1, v) - \alpha \cdot s(v_1, v_1).$$

Also hat man $\alpha = \frac{s(v_1, v)}{s(v_1, v_1)}$ zu wählen.

Zum Nachweis der zweiten Bedingung nehmen wir an, dass $v \in K \cdot v_1 \cap W$. Dann ist $v = \lambda \cdot v_1$ und

$$0 = s(v_1, v) = s(v_1, \lambda \cdot v_1) = \lambda \cdot s(v_1, v_1),$$

also $\lambda = 0$, und damit auch $v = \mathbf{o}$. Insbesondere ist $\dim W = n - 1$. Nun kann man s ohne Probleme auf W beschränken zu

$$s' : W \times W \rightarrow K, s'(v, w) = s(v, w).$$

Nach der Induktionsannahme gibt es eine Basis $\mathcal{B}' = (v_2, \dots, v_n)$ von W , so dass

$$s'(v_i, v_j) = s(v_i, v_j) = 0 \quad \text{für } i, j = 2, \dots, n \quad \text{und } i \neq j.$$

Da $v_i \in W$ für $i = 2, \dots, n$, folgt $s(v_1, v_i) = 0$. Die Vektoren v_1, v_2, \dots, v_n sind linear unabhängig, das folgt aus den Eigenschaften einer direkten Summe. Man kann es aber noch einmal direkt nachrechnen: Aus $\lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_n v_n = \mathbf{o}$ folgt $\lambda_1 v_1 \in K v_1 \cap W$, also $\lambda_1 = 0$. Da \mathcal{B}' Basis von W ist, folgt auch $\lambda_2 = \dots = \lambda_n = 0$. Also erhält man schließlich die gesuchte Basis $\mathcal{B} = (v_1, v_2, \dots, v_n)$ von V . ■

Der Leser wird erfreut festgestellt haben, dass diese „Diagonalisierung“ einer symmetrischen Bilinearform viel einfacher ist, als die mit Hindernissen gepflasterte Diagonalisierung eines Endomorphismus. Im Gegensatz zu den Eigenwerten sind die Einträge $\alpha_1, \dots, \alpha_n$ in der Diagonalen auch nicht eindeutig. Im folgenden Abschnitt werden wir sehen, dass im Fall $K = \mathbb{R}$ wenigstens die Verteilung der Vorzeichen der α_i eindeutig ist.

Ist eine symmetrische Matrix $A \in M(n \times n; K)$ gegeben, so gibt es ein einfaches Rechenverfahren durch *symmetrische Umformungen* zur Bestimmung einer Matrix $T \in GL(n; K)$ derart, dass ${}^t T A T$ eine Diagonalmatrix ist. Dabei wird an A in jedem Schritt zunächst eine Zeilenumformung und dann die entsprechende Spaltenumformung gemacht. Parallel dazu werden an E_n nur die Spaltenumformungen vorgenommen. Schematisch kann man das mit Hilfe von Elementarmatrizen C_1, \dots, C_k so beschreiben, wobei die Pfeile die Reihenfolge der Umformungen angeben.

$$\begin{array}{ccc}
 & & A & E_n \\
 & & & \swarrow \\
 {}^t C_1 \cdot A & \begin{array}{c} \leftarrow \\ \rightarrow \end{array} & {}^t C_1 \cdot A \cdot C_1 & E_n \cdot C_1 \\
 & & & \swarrow \\
 {}^t C_2 \cdot {}^t C_1 \cdot A \cdot C_1 & \begin{array}{c} \leftarrow \\ \rightarrow \end{array} & {}^t C_2 \cdot {}^t C_1 \cdot A \cdot C_1 \cdot C_2 & E_n \cdot C_1 \cdot C_2 \\
 & & \vdots & \vdots \\
 {}^t C_k \cdot \dots \cdot {}^t C_1 \cdot A \cdot C_1 \cdot \dots \cdot C_{k-1} & \rightarrow & {}^t C_k \cdot \dots \cdot {}^t C_1 \cdot A \cdot C_1 \cdot \dots \cdot C_k & E_n \cdot C_1 \cdot \dots \cdot C_k
 \end{array}$$

Ziel der Umformungen ist es, dass ${}^t C_k \cdot \dots \cdot {}^t C_1 \cdot A \cdot C_1 \cdot \dots \cdot C_k = D$ eine Diagonalmatrix wird. Dann hat man rechts mit $T := C_1 \cdot \dots \cdot C_k$ eine Transformationsmatrix erhalten. Eine Strategie für die Umformungen erkennt man an den folgenden Beispielen. Die Art der jeweiligen Umformung ist rechts vermerkt.

Beispiel 1

	A	E_2	
	0 1	1 0	
	1 0	0 1	
			(1) + 1 · (2)
1 1	2 1	1 0	
1 0	1 0	1 1	
			(2) - $\frac{1}{2}$ · (1)
2 1	2 0	1 - $\frac{1}{2}$	
0 - $\frac{1}{2}$	0 - $\frac{1}{2}$	1 $\frac{1}{2}$	
	D	T	

Zur Kontrolle kann man ${}^tT \cdot A \cdot T = D$ prüfen.

Beispiel 2

	A	E_3	
	-1 -2 1	1 0 0	
	-2 -3 -2	0 1 0	
	1 -2 15	0 0 1	
			(2) - 2 · (1)
-1 -2 1	-1 0 1	1 -2 0	
0 1 -4	0 1 -4	0 1 0	
1 -2 15	1 -4 15	0 0 1	
			(3) + 1 · (1)
-1 0 1	-1 0 0	1 -2 1	
0 1 -4	0 1 -4	0 1 0	
0 -4 16	0 -4 16	0 0 1	
			(3) + 4 · (2)
-1 0 0	-1 0 0	1 -2 -7	
0 1 -4	0 1 0	0 1 4	
0 0 0	0 0 0	0 0 1	
	D	T	

5.2.5 Das Trägheitsgesetz von SYLVESTER*

Ist ein Endomorphismus F von V durch eine Diagonalmatrix beschrieben, so müssen in der Diagonalen die Eigenwerte stehen; die sind bis auf die Reihenfolge eindeutig bestimmt. Ist eine symmetrische Bilinearform s bezüglich einer Basis $\mathcal{B} = (v_1, \dots, v_n)$ von V durch eine Diagonalmatrix beschrieben, und $s(v_i, v_i) = \alpha_i$ für $i = 1, \dots, n$, so erhält man mit Hilfe von $\mu_1, \dots, \mu_n \in K^*$ eine neue Basis $\mathcal{B}' := (\mu_1 v_1, \dots, \mu_n v_n)$. Dann ist

$$s(\mu_i v_i, \mu_i v_i) = \mu_i^2 \cdot s(v_i, v_i) = \mu_i^2 \cdot \alpha_i.$$

Die Diagonalmatrix $M_{\mathcal{B}'}(s)$ entsteht also aus $M_{\mathcal{B}}(s)$, indem die Einträge α_i mit μ_i^2 multipliziert werden. Daher kann man für die beschreibende Diagonalmatrix keine Eindeutigkeit erwarten.

Im Fall $K = \mathbb{R}$ ist jedoch stets $\mu_i^2 > 0$, also haben α_i und $\mu_i^2 \cdot \alpha_i$ das gleiche Vorzeichen. Das ist der Schlüssel zum Verständnis des Trägheitsgesetzes. Bevor wir es formulieren, noch eine Folgerung aus dem Diagonalisierungssatz in 5.2.4.

Im Fall einer symmetrischen Bilinearform auf einem reellen Vektorraum V wählen wir eine Basis $\mathcal{B}' = (v'_1, \dots, v'_n)$ von V so, dass $s(v'_i, v'_j) = 0$ für $i \neq j$. Ist $\alpha_i := s(v'_i, v'_i) \neq 0$, so ersetzen wir

$$v'_i \quad \text{durch} \quad v_i := |\alpha_i|^{-\frac{1}{2}} \cdot v'_i.$$

Im Fall $\alpha_i = 0$ setzen wir $v_i := v'_i$. Dann gilt für die quadratische Form q_s zu s bei geeigneter Anordnung der Basis

$$\begin{aligned} q_s(v_i) &= +1 & \text{für } i = 1, \dots, k, \\ q_s(v_i) &= -1 & \text{für } i = k+1, \dots, r, \\ q_s(v_i) &= 0 & \text{für } i = r+1, \dots, n, \end{aligned}$$

und mit $\mathcal{B} := (v_1, \dots, v_n)$ ist $M_{\mathcal{B}}(s) = \begin{pmatrix} E_k & & 0 \\ & -E_{r-k} & \\ 0 & & 0 \end{pmatrix}$.

Dem entsprechend erklären wir Untervektorräume

$$\begin{aligned} V_+ &:= \text{Span}(v_1, \dots, v_k) \subset V, \\ V_- &:= \text{Span}(v_{k+1}, \dots, v_r) \subset V, \\ V_0 &:= \text{Span}(v_{r+1}, \dots, v_n) \subset V. \end{aligned}$$

Ist $v = \sum_{i=1}^n \lambda_i v_i$, so folgt wegen $s(v_i, v_j) = 0$ für $i \neq j$, dass

$$q_s(v) = s(v, v) = \sum_{i=1}^k \lambda_i^2 - \sum_{i=k+1}^r \lambda_i^2.$$

Daher ist

$$\begin{aligned} q_s(v) &> 0 && \text{für alle } v \in V_+ \setminus \{\mathbf{o}\}, \\ q_s(v) &< 0 && \text{für alle } v \in V_- \setminus \{\mathbf{o}\}, \\ q_s(v) &= 0 && \text{für alle } v \in V_0. \end{aligned}$$

Nach Definition der Untervektorräume mit Hilfe der Basen gilt

$$V = V_+ \oplus V_- \oplus V_0,$$

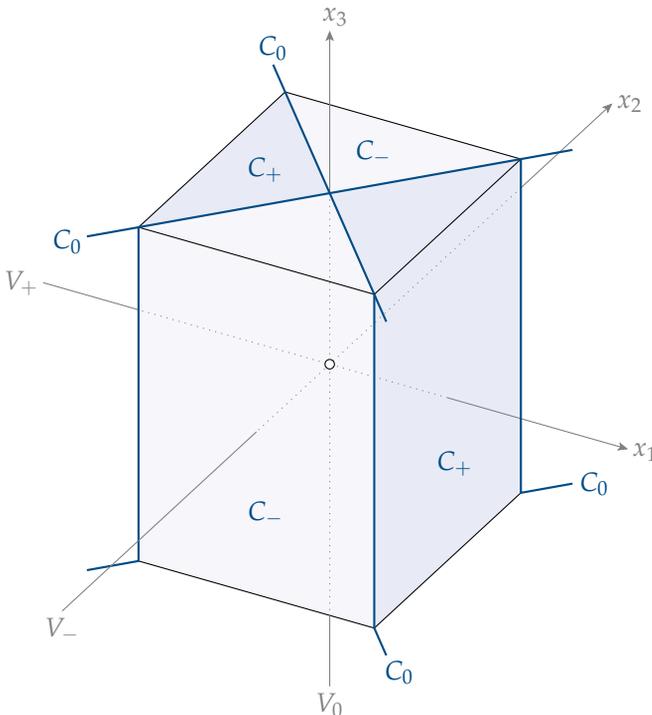
und nach dem Lemma aus 5.2.3 ist $V_0 = V_0(s)$ der Ausartungsraum von s .

Man beachte, dass von diesen drei direkten Summanden nur V_0 durch s eindeutig bestimmt ist. Betrachtet man die Mengen

$$\begin{aligned} C_+ &:= \{v \in V : q_s(v) > 0\}, \\ C_- &:= \{v \in V : q_s(v) < 0\} \quad \text{und} \\ C_0 &:= \{v \in V : q_s(v) = 0\}, \end{aligned}$$

so ist $V_+ \setminus \{\mathbf{o}\} \subset C_+$, $V_- \subset C_- \setminus \{\mathbf{o}\}$ und $V_0 \subset C_0$. Die Mengen C_+ , C_- und C_0 sind jedoch fast nie Untervektorräume. Das sieht man am einfachsten im \mathbb{R}^3 mit

$$s(x, y) = x_1y_1 - x_2y_2, \quad \text{also} \quad q_s(x) = x_1^2 - x_2^2.$$



Hier ist C_0 das Paar von Ebenen $x_1 + x_2 = 0$ und $x_1 - x_2 = 0$, $V_0 = \mathbb{R} \cdot e_3$. C_+ und C_- sind die markierten Bereiche. Entsprechend der obigen Definition ist

$$V_+ = \mathbb{R} \cdot e_1 \quad \text{und} \quad V_- = \mathbb{R} \cdot e_2.$$

Anstelle von V_+ kann man jedoch jeden in C_+ gelegenen Untervektorraum V'_+ von \mathbb{R}^3 also

$$V'_+ \subset C_+ \cup \{0\} \subset \mathbb{R}^2 \quad \text{und analog} \quad V'_- \subset C_- \cup \{0\} \subset \mathbb{R}^2$$

wählen. Dann ist stets

$$q_s(v) > 0 \quad \text{für} \quad v \in V'_+ \setminus \{\mathbf{o}\} \quad \text{und} \quad q_s(v) < 0 \quad \text{für} \quad v \in V'_- \setminus \{\mathbf{o}\}.$$

Will man erreichen, dass $\mathbb{R}^3 = V'_+ \oplus V'_- \oplus V_0$, so müssen V'_+ und V'_- Geraden durch \mathbf{o} sein. Allgemein gilt das

Trägheitsgesetz von SYLVESTER *Hat man für eine quadratische Form q auf einem reellen Vektorraum V zwei Zerlegungen*

$$V = V_+ \oplus V_- \oplus V_0 = V'_+ \oplus V'_- \oplus V_0,$$

wobei V_0 den Ausartungsraum der zugehörigen symmetrischen Bilinearform bezeichnet, und

$$\begin{aligned} q(v) > 0 & \quad \text{für alle} \quad v \in V_+ \setminus \{\mathbf{o}\} \quad \text{und alle} \quad v \in V'_+ \setminus \{\mathbf{o}\}, \\ q(v) < 0 & \quad \text{für alle} \quad v \in V_- \setminus \{\mathbf{o}\} \quad \text{und alle} \quad v \in V'_- \setminus \{\mathbf{o}\}, \end{aligned}$$

so folgt $\dim V'_+ = \dim V_+$ und $\dim V'_- = \dim V_-$.

Die Zahlen $r_+(q) := \dim V_+$ und $r_-(q) := \dim V_-$ sind also wohldefiniert und Invarianten der quadratischen Form q , ebenso wie der Rang $r(q) = \text{rang}(s)$, das ist der Rang der zugehörigen Bilinearform s . Offensichtlich ist

$$r_+(q) + r_-(q) = r(q) \quad \text{und} \quad \dim V_0 = \dim V - r(q).$$

Die Zahl $r_+(q)$ heißt **Positivitäts-Index** von q .

Korollar *Sei s eine symmetrische Bilinearform auf einem reellen Vektorraum V . Angenommen man hat zwei Basen \mathcal{B} und \mathcal{B}' von V derart, dass $M_{\mathcal{B}}(s)$ und $M_{\mathcal{B}'}(s)$ Diagonalmatrizen sind. Dann sind für $M_{\mathcal{B}}(s)$ und $M_{\mathcal{B}'}(s)$ die folgenden Zahlen gleich:*

- Die Zahlen der positiven Diagonalelemente.
- Die Zahlen der negativen Diagonalelemente.
- Die Ränge. ■

Beweis des Trägheitsgesetzes Es genügt, folgendes zu zeigen:

Ist $W \subset V$ ein Untervektorraum mit $q(v) > 0$ für alle $v \in W \setminus \{\mathbf{o}\}$,
so folgt $\dim W \leq \dim V_+$. (*)

Da V_+ und V'_+ gleichberechtigt sind, folgt daraus $\dim V_+ = \dim V'_+$. Wegen

$$\dim V_+ + \dim V_- = \dim V'_+ + \dim V'_- = r,$$

folgt auch $\dim V'_- = \dim V_-$.

Nun zum Beweis von (*). Angenommen $\dim W > \dim V_+$. Aus der Dimensionsformel in 2.2.5 folgt

$$\dim(W \cap (V_- \oplus V_0)) = \dim W + \dim(V_- \oplus V_0) - \dim(W + V_- \oplus V_0) > 0,$$

da die Summe der beiden ersten Terme der rechten Seite nach Annahme $> \dim V$, und der dritte Term in jedem Fall $\leq \dim V$ ist. Also gibt es ein $w \in W \cap (V_- \oplus V_0)$ mit $w \neq \mathbf{o}$. Aus $w \in W$ folgt $q(w) > 0$. Aus $w \in V_- \oplus V_0$ folgt

$$w = v_- + v_0 \quad \text{mit} \quad v_- \in V_- \quad \text{und} \quad v_0 \in V_0.$$

Dann ist aber

$$q(w) = s(v_- + v_0, v_- + v_0) = s(v_-, v_-) \leq 0,$$

im Widerspruch zu $q(w) > 0$. ■

Die in den vorhergehenden Abschnitten bewiesenen Tatsachen über quadratische Formen haben Anwendungen in der Geometrie, besonders der Theorie der Quadriken. Das ist der Gegenstand der folgenden Abschnitte.

5.2.6 Exkurs über affine Geometrie*

Bei linearen Abbildungen zwischen Vektorräumen bleibt der Ursprung \mathbf{o} immer fest. In vielen geometrischen Situationen ist es angebracht, auch etwas allgemeinere Abbildungen zu benutzen, etwa dann, wenn man einen Kegelschnitt durch eine möglichst einfache Gleichung beschreiben will.

Wir erinnern zunächst an die Definition eines affinen Unterraums $L \subset V$ in einem K -Vektorraum V : Es muss ein $p \in V$ und einen Untervektorraum $L_0 \subset V$ derart geben, dass

$$L = p + L_0.$$

Dabei kann man $p \in L$ beliebig wählen, L_0 ist eindeutig bestimmt als

$$L_0 = \{p' - p : p, p' \in L\},$$

die Differenzen aus L . Dabei ist die suggestive Bezeichnung

$$\overrightarrow{pp'} := p' - p \in L_0$$

üblich. Der Vektor $\overrightarrow{pp'}$ verschiebt p nach p' :

$$p + \overrightarrow{pp'} = p'.$$

Insgesamt wird durch jeden Vektor $v \in L_0$ eine Abbildung

$$\tau_v : L \rightarrow L, q \mapsto q + v$$

bewirkt, sie heißt **Translation**.

Als **Dimension** eines affinen Raumes $L \subset V$ hatten wir die Dimension des Untervektorraums $L_0 \subset V$ erklärt, in Zeichen

$$\dim L := \dim L_0.$$

Ist $\dim L_0 = k$, so heißt ein $(k+1)$ -Tupel (p_0, p_1, \dots, p_k) von Punkten $p_0, \dots, p_k \in L$ **affine Basis** von L , wenn $(\overrightarrow{p_0 p_1}, \dots, \overrightarrow{p_0 p_k})$ eine Vektorraum-Basis von L_0 ist.

Eine Abbildung $f : V \rightarrow W$ zwischen K -Vektorräumen heißt **affin**, wenn es eine lineare Abbildung $F : V \rightarrow W$ gibt derart, dass

$$f(v) = f(\mathbf{o}) + F(v) \quad \text{für alle } v \in V.$$

Offenbar ist f genau dann linear, wenn $f(\mathbf{o}) = \mathbf{o}$. Im Spezialfall $V = K^n$ und $W = K^m$ ist $f : K^n \rightarrow K^m$ genau dann affin, wenn es eine Matrix $A \in M(m \times n; K)$ und ein $b \in K^m$ gibt derart, dass

$$f(x) = b + A \cdot x \quad \text{für alle } x \in K^n.$$

Schließlich nennt man eine Abbildung $f : V \rightarrow V$ **Affinität**, wenn f affin und bijektiv ist.

Für den Umgang mit Affinitäten benötigen wir einige Regeln:

Lemma a) Eine affine Abbildung $f : V \rightarrow V$ ist genau dann eine Affinität, wenn die zugehörige lineare Abbildung F ein Isomorphismus ist.

b) Ist $f : V \rightarrow V$ eine Affinität, so ist die Umkehrabbildung $f^{-1} : V \rightarrow V$ gegeben durch

$$f^{-1}(w) = -F^{-1}(f(\mathbf{o})) + F^{-1}(w) \quad \text{für alle } w \in V,$$

also ist auch f^{-1} eine Affinität.

c) Sind (p_0, p_1, \dots, p_n) und (q_0, q_1, \dots, q_n) affine Basen von V , so gibt es genau eine Affinität $f : V \rightarrow V$ mit

$$f(p_i) = q_i \quad \text{für } i = 0, \dots, n.$$

Beweis Ad a). Ist F kein Isomorphismus, so gibt es ein $\mathbf{o} \neq v \in \text{Ker } F$, also ist

$$f(v) = f(\mathbf{o}) + F(v) = f(\mathbf{o}),$$

und f ist daher nicht injektiv. Ist F Isomorphismus, so behaupten wir, dass durch

$$g(w) := -F^{-1}(f(\mathbf{o})) + F^{-1}(w)$$

eine affine Umkehrabbildung von f gegeben ist. Setzen wir $w = f(v) = f(\mathbf{o}) + F(v)$ ein, so ergibt sich wegen der Linearität von F^{-1}

$$g(w) = -F^{-1}(f(\mathbf{o})) + F^{-1}(f(\mathbf{o}) + F(v)) = -F^{-1}(f(\mathbf{o})) + F^{-1}(f(\mathbf{o})) + F^{-1}(F(v)) = v.$$

Analog folgt $f \circ g = \text{id}_V$. Damit ist a) und auch b) bewiesen.

Ad c). Nach 2.4.1 gibt es genau eine lineare Abbildung

$$F: V \rightarrow V \quad \text{mit} \quad F(\overrightarrow{p_0 p_i}) = \overrightarrow{q_0 q_i} \quad \text{für} \quad i = 1, \dots, n,$$

und dieses F ist ein Isomorphismus. Aus $f(p_0) = q_0$ und aus $f(p_0) = f(\mathbf{o}) + F(p_0)$ folgt, dass $f(\mathbf{o}) = q_0 - F(p_0)$ sein muss. Also hat $f: V \rightarrow V$ mit

$$f(v) = (q_0 - F(p_0)) + F(v)$$

die verlangten Eigenschaften, denn dann ist für $i = 1, \dots, n$

$$f(p_i) = q_0 - F(p_0) + F(p_i) = q_0 + F(\overrightarrow{p_0 p_i}) = q_0 + \overrightarrow{q_0 q_i} = q_i.$$

Die Eindeutigkeit von f folgt aus der Eindeutigkeit von F . ■

Beispiel Im \mathbb{R}^2 seien die Punkte

$$p_0 = {}^t(1, 1), p_1 = {}^t(1, 2), p_2 = {}^t(0, 1) \quad \text{und} \quad q_0 = {}^t(-2, -1), q_1 = {}^t(0, -1), q_2 = {}^t(-2, -2)$$

gegeben. Gesucht ist eine Affinität $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ mit $f(p_i) = q_i$ für $i = 0, 1, 2$. Dazu berechnet man zunächst die Vektoren

$$\overrightarrow{p_0 p_1} = {}^t(0, 1), \overrightarrow{p_0 p_2} = {}^t(-1, 0) \quad \text{und} \quad \overrightarrow{q_0 q_1} = {}^t(2, 0), \overrightarrow{q_0 q_2} = {}^t(0, -1).$$

Die lineare Abbildung $F: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ mit $F(\overrightarrow{p_0 p_i}) = \overrightarrow{q_0 q_i}$ für $i = 1, 2$ ist gegeben durch die Matrix

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

Also ist $f(\mathbf{o}) = q_0 - F(p_0) = {}^t(-4, -2)$, und für ein beliebiges $x = {}^t(x_1, x_2) \in \mathbb{R}^2$ ist

$$f(x) = \begin{pmatrix} -4 \\ -2 \end{pmatrix} + \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

Zur Kontrolle kann man noch $f(p_i) = q_i$ für $i = 1, 2$ nachrechnen. Die Umkehrung von f ist gegeben durch

$$f^{-1}(y) = \begin{pmatrix} 2 \\ 2 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ \frac{1}{2} & 0 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}.$$

Wie wir in 2.4.2 gesehen hatten, gibt es zu jeder linearen Abbildung $F : K^n \rightarrow K^m$ eine Matrix $A \in M(m \times n; K)$ derart, dass

$$F(x) = A \cdot x \quad \text{für } x = {}^t(x_1, \dots, x_n).$$

Wir werden nun sehen, dass sich jede affine Abbildung $f : K^n \rightarrow K^m$ durch eine Matrix $A' \in M((m+1) \times (n+1); K)$ beschreiben lässt. Ist

$$f(x) = b + A \cdot x \quad \text{mit } b = {}^t(b_1, \dots, b_m) \in K^m,$$

so erklären wir die *erweiterte Matrix*

$$A' := \left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline b_1 & & & \\ \vdots & & & \\ b_m & & & A \end{array} \right), \quad x' := \begin{pmatrix} 1 \\ x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^{n+1}, \quad y' := \begin{pmatrix} 1 \\ y_1 \\ \vdots \\ y_m \end{pmatrix} \in K^{m+1}.$$

Ist dann $y' = A' \cdot x'$, so folgt ${}^t(y_1, \dots, y_m) = f(x)$. Das kann man ganz explizit nachrechnen:

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ b_1 & a_{11} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ b_m & a_{m1} & \cdots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 1 \\ b_1 + a_{11}x_1 + \cdots + a_{1n}x_n \\ \vdots \\ b_m + a_{m1}x_1 + \cdots + a_{mn}x_n \end{pmatrix} = \begin{pmatrix} 1 \\ y_1 \\ \vdots \\ y_m \end{pmatrix}.$$

Offensichtlich ist f genau dann linear, wenn $b_1 = \dots = b_m = 0$, genau dann eine Affinität, wenn $n = m$ und $A \in GL(n; K)$, und genau dann eine Translation, wenn $A = E_n$.

Ist f eine durch A' beschriebene Affinität, so wird f^{-1} beschrieben durch

$$(A')^{-1} = \left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline c_1 & & & \\ \vdots & & & \\ c_n & & & A^{-1} \end{array} \right), \quad \text{wobei } \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = -A^{-1} \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}.$$

In dem oben angegebenen Beispiel ist

$$A' = \begin{pmatrix} 1 & 0 & 0 \\ -4 & 0 & 2 \\ -2 & 1 & 0 \end{pmatrix} \quad \text{und} \quad (A')^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 0 & 1 \\ 2 & \frac{1}{2} & 0 \end{pmatrix}.$$

5.2.7 Quadriken*

Die Gleichung eines Kreises in der Ebene \mathbb{R}^2 mit Mittelpunkt \mathbf{o} und Radius 1 lautet

$$x_1^2 + x_2^2 - 1 = 0.$$

Ist ${}^t(a_1, a_2)$ der Mittelpunkt und r der Radius, so wird es schon komplizierter:

$$(x_1 - a_1)^2 + (x_2 - a_2)^2 - r^2 = x_1^2 + x_2^2 - 2a_1x_1 - 2a_2x_2 + a_1^2 + a_2^2 - r^2 = 0.$$

Das ist eine quadratische Gleichung für die Koordinaten x_1, x_2 . Die allgemeine Form solch einer quadratischen Gleichung ist

$$\alpha_1 x_1^2 + \alpha_2 x_2^2 + \alpha_3 x_1 x_2 + \beta_1 x_1 + \beta_2 x_2 + \gamma = 0, \quad (*)$$

wobei die Koeffizienten $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \gamma \in \mathbb{R}$ beliebig gewählt werden können. Der Zusammenhang mit der bilinearen Algebra ist leicht herzustellen, indem man eine Gleichung der Form (*) mit Hilfe einer symmetrischen Matrix $A' \in M(3 \times 3; K)$ beschreibt. Dabei muss $\text{char}(K) \neq 2$ sein, der geometrisch einfachste Fall ist $K = \mathbb{R}$. Für

$$x = {}^t(x_1, x_2) \in \mathbb{R}^2 \quad \text{setzen wir wieder} \quad x' := {}^t(1, x_1, x_2) \in \mathbb{R}^3.$$

Dann ist

$$\begin{aligned} {}^t x' \cdot A' \cdot x' &= (1, x_1, x_2) \cdot \begin{pmatrix} a_{00} & a_{01} & a_{02} \\ a_{01} & a_{11} & a_{12} \\ a_{02} & a_{12} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ x_1 \\ x_2 \end{pmatrix} \\ &= a_{00} + 2a_{01}x_1 + 2a_{02}x_2 + 2a_{12}x_1x_2 + a_{11}x_1^2 + a_{22}x_2^2. \end{aligned}$$

Ganz analog erhält man für $A' = {}^t A' \in M((n+1) \times (n+1); \mathbb{R})$ und $x \in \mathbb{R}^n, x' \in \mathbb{R}^{n+1}$

$${}^t x' \cdot A' \cdot x' = a_{00} + 2 \cdot \sum_{i=1}^n a_{0i} x_i + 2 \cdot \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j + \sum_{i=1}^n a_{ii} x_i^2.$$

Die Koeffizienten der Terme zweiter Ordnung sind enthalten in der Teilmatrix

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{1n} & \cdots & a_{nn} \end{pmatrix} \in M(n \times n; \mathbb{R}).$$

Ist $A = \mathbf{o}$, so wird ${}^t x' \cdot A' \cdot x' = 0$ eine lineare Gleichung, die Menge der Nullstellen im \mathbb{R}^n ist ein affiner Untervektorraum. Diesen Fall kann man durch die Voraussetzung $\text{rang } A \geq 1$ ausschließen. Damit sind wir vorbereitet für die ganz allgemeine

Definition Eine Teilmenge $Q \subset \mathbb{R}^n$ heißt **Quadrik**, wenn es eine symmetrische Matrix $A' \in M((n+1) \times (n+1); \mathbb{R})$ gibt mit $\text{rang } A \geq 1$ derart, dass

$$Q = \{x \in \mathbb{R}^n : {}^t x' \cdot A' \cdot x' = 0\}.$$

Im Fall $n = 2$ nennt man eine Quadrik auch **Kegelschnitt**.

Vorsicht! In dieser Allgemeinheit sind Extremfälle wie die Gleichung

$$x_1^2 + \dots + x_n^2 + 1 = 0, \quad \text{also } Q = \emptyset$$

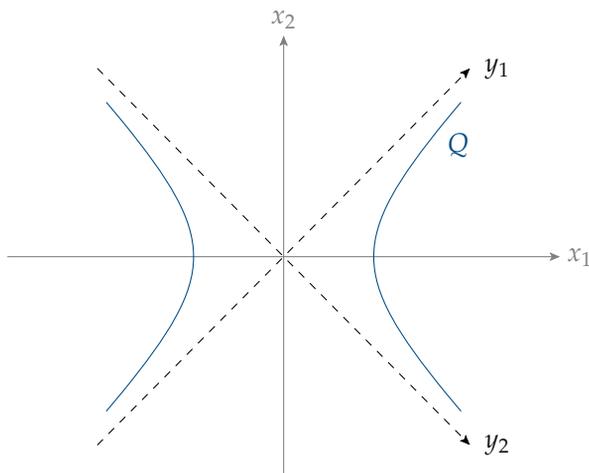
nicht ausgeschlossen.

Wir wollen nun die Frage in Angriff nehmen, wie man an der durch die Matrix A' bestimmten Gleichung einer Quadrik die geometrischen Eigenschaften erkennen kann. Im Fall $n = 2$ bedeutet das, ob es sich um eine Ellipse, eine Parabel oder eine Hyperbel handelt. Wesentliches Hilfsmittel dabei werden Koordinatentransformationen sein, mit deren Hilfe man die Gleichungen verändern, insbesondere vereinfachen kann. Wir illustrieren das zunächst an einem ganz einfachen

Beispiel Die Quadrik

$$Q := \{(x_1, x_2) \in \mathbb{R}^2 : x_1^2 - x_2^2 - 1 = 0\}$$

ist eine Hyperbel, in diesem Fall ist $A' = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$.



Um die Asymptoten als neue Koordinatenachsen einzuführen, betrachtet man den linearen Isomorphismus

$$F: \mathbb{R}^2 \rightarrow \mathbb{R}^2, \quad \text{gegeben durch } S = \frac{1}{2} \cdot \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.$$

Nach den Regeln für Koordinatentransformationen aus 2.5.1 gilt dann

$$x_1 = \frac{1}{2} \cdot (y_1 + y_2) \quad \text{und} \quad x_2 = \frac{1}{2} \cdot (-y_1 + y_2).$$

In die Hyperbelgleichung eingesetzt erhält man

$$x_1^2 - x_2^2 - 1 = \frac{1}{4} \cdot (y_1 + y_2)^2 - \frac{1}{4} \cdot (-y_1 + y_2)^2 - 1 = y_1 y_2 - 1 = 0.$$

In den neuen y -Koordinaten ist Q also der Graph der Funktion $y_2 = y_1^{-1}$. Zur neuen Gleichung von Q gehört die Matrix

$$B' = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & 0 \end{pmatrix}.$$

Um auf die alte Gleichung mit der Diagonalmatrix A' zurückzukommen, kann man B' nach einer Variante des Verfahrens aus 5.2.4 durch symmetrische Umformungen diagonalisieren, und daneben bei E_3 nur die Spalten umformen. Im Gegensatz zu 5.2.4 darf in der ganz rechts stehenden Matrix die erste Zeile nicht verändert werden. Das Ergebnis sieht so aus:

	B'	E_3	
	-1 0 0	1 0 0	
	0 0 $\frac{1}{2}$	0 1 0	
	0 $\frac{1}{2}$ 0	0 0 1	
			(2) + 1 · (3)
-1 0 0	-1 0 0	1 0 0	
0 $\frac{1}{2}$ $\frac{1}{2}$	0 1 $\frac{1}{2}$	0 1 0	
0 $\frac{1}{2}$ 0	0 $\frac{1}{2}$ 0	0 1 1	
			(3) - $\frac{1}{2}$ · (2)
-1 0 0	-1 0 0	1 0 0	
0 1 $\frac{1}{2}$	0 1 0	0 1 - $\frac{1}{2}$	
0 0 - $\frac{1}{4}$	0 0 - $\frac{1}{4}$	0 1 $\frac{1}{2}$	
			2 · (3)
-1 0 0	-1 0 0	1 0 0	
0 1 0	0 1 0	0 1 -1	
0 0 - $\frac{1}{2}$	0 0 -1	0 1 1	
	A'	T'	

Nach den Rechenregeln für symmetrische Matrizen aus 5.2.4 ist

$$A' = {}^t T' \cdot B' \cdot T'.$$

Wie wir gleich sehen werden, kann man an T' die lineare Transformation der Koordinaten ablesen:

$$y_1 = x_1 - x_2 \quad \text{und} \quad y_2 = x_1 + x_2.$$

Eingesetzt in die Gleichung für Q ergibt das die alte Gleichung:

$$y_1 y_2 - 1 = (x_1 - x_2)(x_1 + x_2) - 1 = x_1^2 - x_2^2 - 1 = 0.$$

Bevor wir versuchen, die Gleichung einer Quadrik durch eine Affinität zu vereinfachen, muss überlegt werden, wie sich die Gleichung verändert.

Transformationsformel Sei $Q \subset \mathbb{R}^n$ eine Quadrik, beschrieben durch die symmetrische Matrix A' . Ist $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$ eine Affinität beschrieben durch $S' \in \text{GL}(n+1, \mathbb{R})$, so ist $f(Q) \subset \mathbb{R}^n$ eine Quadrik, beschrieben durch die Matrix

$$B' = {}^t T' \cdot A' \cdot T', \quad \text{wobei} \quad T' = S'^{-1}.$$

Beweis Ist $x \in \mathbb{R}^n$ und $y = f(x) \in \mathbb{R}^n$, so gilt nach 5.2.6

$$y' = S' \cdot x' \quad \text{und} \quad x' = T' \cdot y'.$$

Daraus folgt

$$\begin{aligned} y \in f(Q) &\Leftrightarrow x = f^{-1}(y) \in Q \Leftrightarrow {}^t x' \cdot A' \cdot x' = 0 \\ &\Leftrightarrow 0 = {}^t (T' \cdot y') \cdot A' \cdot (T' \cdot y') = {}^t y' \cdot ({}^t T' \cdot A' \cdot T') \cdot y'. \end{aligned}$$

■

Das Problem einer „Normalform“ für die Gleichung einer Quadrik behandeln wir zunächst im Spezialfall $n = 2$. Hier ist

$$A' = \left(\begin{array}{c|cc} a_{00} & a_{01} & a_{02} \\ \hline a_{01} & & A \\ a_{02} & & \end{array} \right).$$

Setzt man $r = \text{rang } A$ und $r' := \text{rang } A'$, so gelten die Ungleichungen

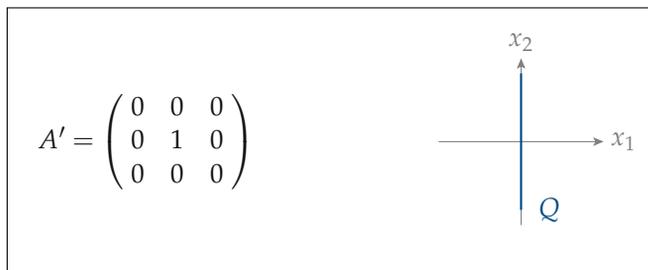
$$1 \leq r \leq 2, \quad r \leq r' \quad \text{und} \quad 1 \leq r' \leq 3.$$

Dadurch wird eine grobe Einteilung in fünf verschiedene Typen von Gleichungen möglich:

r	r'	Typ
1	1	(a)
1	2	(b)
1	3	(c)
2	2	(d)
2	3	(e)

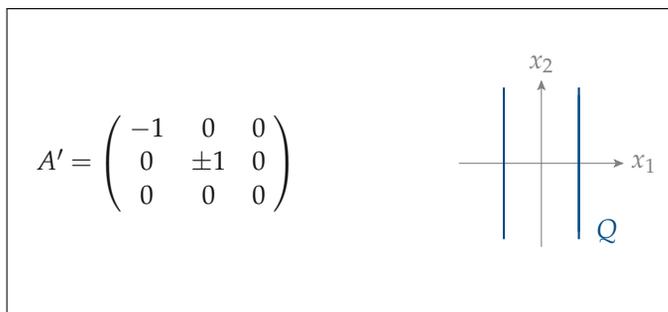
Für jeden der Typen kann man möglichst einfache Gleichungen als *Normalformen* auswählen.

Typ (a)



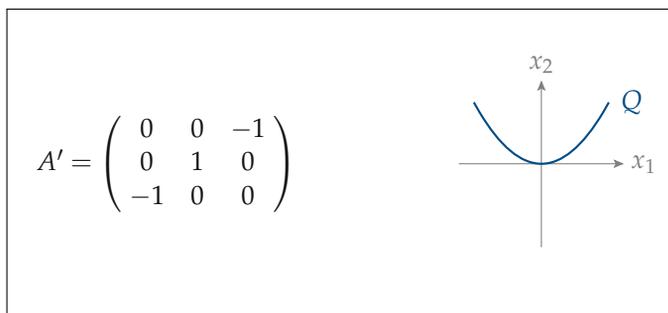
Die zugehörige Gleichung $x_1^2 = 0$ beschreibt eine Gerade Q , die man mit Vielfachheit 2 zählen kann. Sie entsteht, wenn ein Kegel von einer Ebene in einer „Mantellinie“ tangiert wird.

Typ (b)



Die beiden möglichen Gleichungen sind $x_1^2 = 1$ und $x_1^2 = -1$. Im zweiten Fall hat man $Q = \emptyset$, im ersten besteht Q aus den beiden Geraden $x_1 = 1$ und $x_1 = -1$. Sie entstehen, wenn man statt eines Kegels einen Zylinder mit einer geeigneten Ebene schneidet.

Typ (c)



Die Gleichung $x_1^2 - 2x_2 = 0$ beschreibt eine Parabel.

Typ (d)

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

Die Gleichung $x_1^2 + x_2^2 = 0$ beschreibt den Ursprung, $x_1^2 - x_2^2 = 0$ zwei Geraden. Beide können entstehen, wenn man einen Kegel mit einer geeigneten Ebene durch die Spitze schneidet.

Typ (e)

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

In diesem Fall gibt es drei wesentlich verschiedene Möglichkeiten für die Gleichungen:

- (1) $-x_1^2 - x_2^2 = 1$, $Q = \emptyset$,
- (2) $x_1^2 - x_2^2 = 1$, Q ist eine Hyperbel,
- (3) $x_1^2 + x_2^2 = 1$, Q ist ein Kreis.

Die Typen (a) bis (d) kann man als Ausnahmen ansehen, „im Allgemeinen“ wird $r = 2$ und $r' = 3$ sein. Aber welcher der Fälle (1) bis (3) auftritt, kann nicht durch die Ränge entschieden werden. Nun können wir folgendes zeigen:

Affine Normalform der Gleichung eines Kegelschnitts Ist $Q \subset \mathbb{R}^2$ ein Kegelschnitt, so kann man seine Gleichung durch eine affine Transformation auf genau eine der oben angegebenen Normalformen bringen.

Man beachte dabei, dass nur $Q = \emptyset$ als Teilmenge von \mathbb{R}^2 durch zwei verschiedene Typen von Gleichungen beschrieben werden kann, nämlich

$$x_1^2 = -1 \quad \text{vom Typ (b) und} \quad x_1^2 + x_2^2 = -1 \quad \text{vom Typ (e).}$$

Beweis Sei $Q = \{x \in \mathbb{R}^2 : {}^t x' \cdot A' \cdot x' = 0\}$. Nach der obigen Transformationsformel ist eine Matrix

$$T' = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline c_1 & & \\ c_2 & & T \end{array} \right) \in \text{GL}(3; \mathbb{R})$$

gesucht, derart dass $B' = {}^t T' \cdot A' \cdot T'$ Normalform hat. Wir geben ein konstruktives Verfahren an, wie man T' schrittweise aufbauen kann.

Wir starten mit

$$A' = \left(\begin{array}{c|cc} a_{00} & a_{01} & a_{02} \\ \hline a_{01} & & A \\ a_{02} & & \end{array} \right).$$

In der ersten Etappe wird A nach dem Verfahren aus 5.2.4 diagonalisiert: Man findet ein $T_1 \in \text{GL}(2; \mathbb{R})$ so, dass

$${}^t T_1 \cdot A \cdot T_1 = \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} =: B_1.$$

Nach der Voraussetzung $\text{rang } A \geq 1$ können wir $\alpha_1 \neq 0$ annehmen. Wir setzen

$$T'_1 := \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & & T_1 \\ 0 & & \end{array} \right) \quad \text{und} \quad B'_1 := {}^t T'_1 \cdot A' \cdot T'_1 = \left(\begin{array}{c|cc} a_{00} & c_{01} & c_{02} \\ \hline c_{01} & \alpha_1 & 0 \\ c_{02} & 0 & \alpha_2 \end{array} \right).$$

In der zweiten Etappe wird die erste Zeile und Spalte von B'_1 bearbeitet. Dazu ist eine Fallunterscheidung nötig.

Fall 1: $\text{rang } A = 1$; dann ist $\alpha_2 = 0$. Mit Hilfe von $\alpha_1 \neq 0$ kann man c_{01} zu Null machen: Es gibt ein $T'_2 \in \text{GL}(3; \mathbb{R})$ so, dass

$${}^t T'_2 \cdot B'_1 \cdot T'_2 = \begin{pmatrix} c_{00} & 0 & c_{02} \\ 0 & \alpha_1 & 0 \\ c_{02} & 0 & 0 \end{pmatrix} =: B'_2.$$

Ist $c_{02} = 0$, so hat man die Fälle $c_{00} = 0$ und $c_{00} \neq 0$. Im ersten Fall kann man die Gleichung $\alpha_1 x_1^2 = 0$ ohne Veränderung der Nullstellen durch α_1 dividieren, das ergibt Typ (a). Im zweiten Fall erhält man durch Multiplikation der Gleichung mit $-(1/c_{00})$

$$\beta_1 x_1^2 - 1 = 0 \quad \text{mit} \quad \beta_1 = -\frac{\alpha_1}{c_{00}} \neq 0.$$

Durch Multiplikation der zweiten Zeile und Spalte von

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & \beta_1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

mit $|\beta_1|^{-\frac{1}{2}}$ kommt man bei Typ (b) an.

Ist $c_{02} \neq 0$, so gibt es ein $T'_3 \in GL(3; \mathbb{R})$ derart, dass

$${}^t T'_3 \cdot B'_2 \cdot T'_3 = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix},$$

das ergibt Typ (c).

Fall 2: $\text{rang } A = 2$; dann ist $\alpha_2 \neq 0$. Somit kann man ein $T'_2 \in GL(3; \mathbb{R})$ finden derart, dass

$${}^t T'_2 \cdot B'_1 \cdot T'_2 = \begin{pmatrix} c_{00} & 0 & 0 \\ 0 & \alpha_1 & 0 \\ 0 & 0 & \alpha_2 \end{pmatrix} =: B'_2.$$

Im Fall $c_{00} = 0$ kann man α_1 auf 1, und α_2 auf ± 1 transformieren, das ergibt Typ (d).

Ist $c_{00} \neq 0$, so kann man die ganze Gleichung durch Multiplikation mit $-(1/c_{00})$ ohne Veränderung der Nullstellen auf die Form

$$\beta_1 x_1^2 + \beta_2 x_2^2 - 1 = 0$$

bringen. Durch Multiplikation der zweiten und dritten Zeile und Spalte der Matrix mit einem geeigneten Faktor kommt man bei Typ (e) an.

Da die verschiedenen Typen der Normalformen durch die Ränge von Matrizen bestimmt sind, folgt die Eindeutigkeit. ■

Ein praktisches Rechenverfahren verläuft nach einer Variante des Verfahrens aus 5.2.4. Man startet mit A' und E_3 , und endet mit

$${}^t C_k \cdot \dots \cdot {}^t C_1 \cdot A' \cdot C_1 \cdot \dots \cdot C_k \quad \text{und} \quad E_n \cdot C_1 \cdot \dots \cdot C_k,$$

wobei die $C_i \in GL(3; \mathbb{R})$ Elementarmatrizen sind. Die entstandene Transformationsmatrix $T' = C_1 \cdot \dots \cdot C_k$ muss aber von der Form

$$T' := \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline c_1 & & \\ c_2 & & T \end{array} \right)$$

sein. Daher darf man keine Umformungen vornehmen, bei der Vielfache der ersten Zeile und Spalte zu anderen addiert werden. Weiterhin hat eine Multiplikation der ganzen Matrix links keinen Einfluss auf die Nullstellen, sie muss rechts bei der entstehenden Transformationsmatrix nicht berücksichtigt werden.

Beispiel 1 Wir starten mit dem Kegelschnitt

$$Q := \{(x_1, x_2) \in \mathbb{R}^2 : x_1^2 + 2x_1x_2 + x_2^2 + 2x_2 + 2 = 0\}.$$

In diesem Fall ist $\text{rang } A = 1$ und $\text{rang } A' = 3$. Die Umformung verläuft nach folgendem Schema:

	A'	E_3	
	2 0 1	1 0 0	
	0 1 1	0 1 0	
	1 1 1	0 0 1	
			(3) - 1 · (2)
2 0 1	2 0 1	1 0 0	
0 1 1	0 1 0	0 1 -1	
1 0 0	1 0 0	0 0 1	
			(1) - 1 · (3)
1 0 1	0 0 1	1 0 0	
0 1 0	0 1 0	1 1 -1	
1 0 0	1 0 0	-1 0 1	
			-1 · (3)
0 0 1	0 0 -1	1 0 0	
0 1 0	0 1 0	1 1 1	
-1 0 0	-1 0 0	-1 0 -1	
	B'	T'	

Weiter berechnet man

$$S' := (T')^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ -1 & 0 & -1 \end{pmatrix}.$$

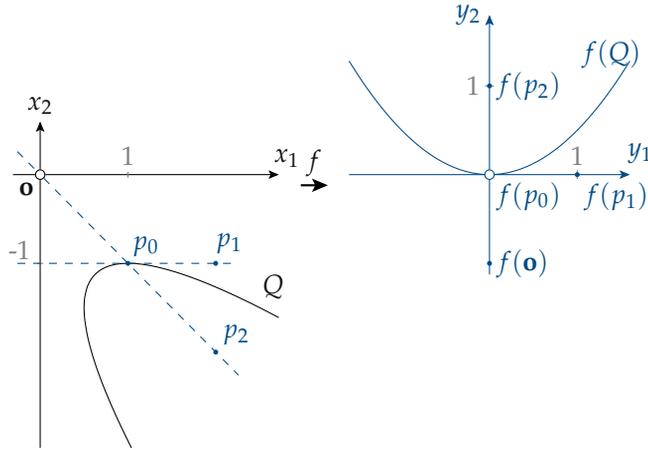
Ist dann $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ beschrieben durch S' , so wird f^{-1} beschrieben durch T' , und

$$f(Q) = \{y \in \mathbb{R}^2 : {}^t y' \cdot B' \cdot y' = 0\} = \{(y_1, y_2) \in \mathbb{R}^2 : y_1^2 - 2y_2 = 0\},$$

also ist $f(Q)$ und damit auch Q eine Parabel. Das kann man noch einmal direkt nachrechnen, indem man

$$y_1 = x_1 + x_2 \quad \text{und} \quad y_2 = -1 - x_2$$

in die Gleichung von $f(Q)$ einsetzt.



Beispiel 2 Bei $Q := \{(x_1, x_2) \in \mathbb{R}^2 : 5x_1^2 - 2x_1x_2 + 2x_2^2 + 8x_1 + 2x_2 + 4 = 0\}$ ist $r = 2$ und $r' = 3$, die Umformung verlauft so:

			A'				E_3			
			4	4	1	1	0	0	0	
			4	5	-1	0	1	0	0	
			1	-1	2	0	0	1	1	
										$(2) + \frac{1}{2} \cdot (3)$
4	4	1	4	$\frac{9}{2}$	1	1	0	0	0	
$\frac{9}{2}$	$\frac{9}{2}$	0	$\frac{9}{2}$	$\frac{9}{2}$	0	0	1	0	0	
1	-1	2	1	0	2	0	$\frac{1}{2}$	1	1	
										$(1) - (2)$
$-\frac{1}{2}$	0	1	$-\frac{1}{2}$	0	1	1	0	0	0	
$\frac{9}{2}$	$\frac{9}{2}$	0	0	$\frac{9}{2}$	0	-1	1	0	0	
1	0	2	1	0	2	$-\frac{1}{2}$	$\frac{1}{2}$	1	1	
										$(1) - \frac{1}{2} \cdot (3)$
-1	0	0	-1	0	0	1	0	0	0	
0	$\frac{9}{2}$	0	0	$\frac{9}{2}$	0	-1	1	0	0	
1	0	2	0	0	2	-1	$\frac{1}{2}$	1	1	
										$\frac{1}{3}\sqrt{2} \cdot (2), \frac{1}{2}\sqrt{2} \cdot (3)$
-1	0	0	-1	0	0	1	0	0	0	
0	$\frac{3}{2}\sqrt{2}$	0	0	1	0	-1	$\frac{1}{3}\sqrt{2}$	0	0	
0	0	$\sqrt{2}$	0	0	1	-1	$\frac{1}{6}\sqrt{2}$	$\frac{1}{2}\sqrt{2}$	$\frac{1}{2}\sqrt{2}$	
			B'				T'			

Ist dann $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ beschrieben durch

$$S' = (T')^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ \frac{3}{2}\sqrt{2} & \frac{3}{2}\sqrt{2} & 0 \\ \frac{1}{2}\sqrt{2} & -\frac{1}{2}\sqrt{2} & \sqrt{2} \end{pmatrix},$$

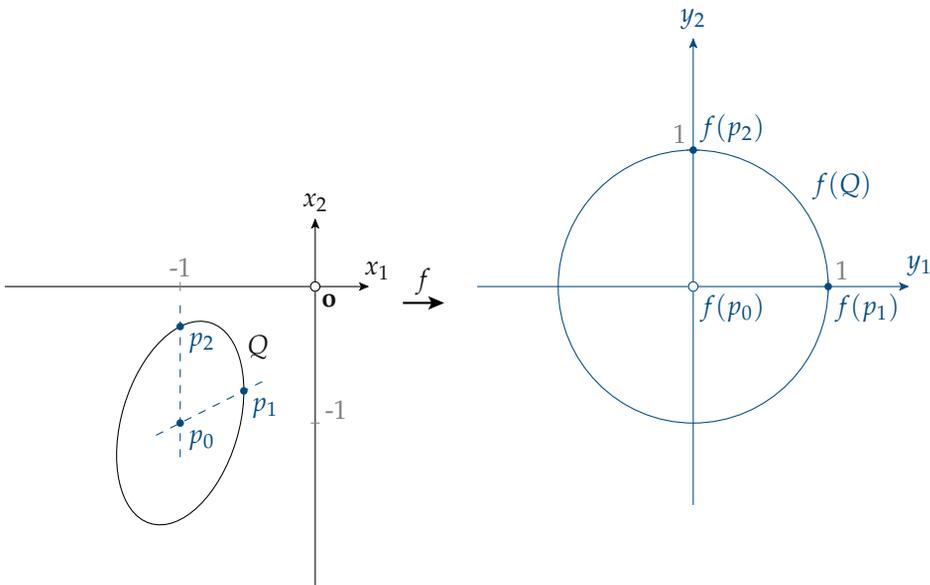
so ist

$$f(Q) = \{(y_1, y_2) \in \mathbb{R}^2 : y_1^2 + y_2^2 - 1 = 0\},$$

also ein Kreis. Das kann man noch einmal direkt nachrechnen, indem man

$$y_1 = \frac{3}{2}\sqrt{2}x_1 + \frac{3}{2}\sqrt{2} \quad \text{und} \quad y_2 = -\frac{1}{2}\sqrt{2}x_1 + \sqrt{2}x_2 + \frac{1}{2}\sqrt{2}$$

in die Gleichung von $f(Q)$ einsetzt.



Wie man an den Beispielen sieht, kann man mit Hilfe der Affinität f den Typ und die Lage des Kegelschnitts Q erkennen. Aber f verändert Längen und Winkel. Das wird verbessert durch die „Hauptachsentransformation“ in 5.3.6.

Die Normalformen von Quadriken im \mathbb{R}^n haben wir nur im Fall von Kegelschnitten, d.h. $n = 2$ ausführlich beschrieben. Der allgemeine Fall verläuft ganz analog, es sind aber mehr Buchstaben und Indizes nötig. Hier soll nur das Ergebnis festgehalten werden.

Ist $A' \in M((n + 1) \times (n + 1); \mathbb{R})$ die symmetrische Koeffizientenmatrix der Quadrik $Q \subset \mathbb{R}^n$ und $A \in M(n \times n; \mathbb{R})$ die oben beschriebene Teilmatrix, so beweist man zunächst ganz einfach die Ungleichung

$$\text{rang } A \leq \text{rang } A' \leq \text{rang } A + 2.$$

Setzt man zur Abkürzung $r := \text{rang } A$ und $r' := \text{rang } A'$, so erhält man folgendes Ergebnis:

Affine Normalform der Gleichung einer Quadrik *Ist*

$$Q = \{x \in \mathbb{R}^n : {}^t x' \cdot A' \cdot x' = 0\} \subset \mathbb{R}^n,$$

so gibt es eine Affinität $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ derart, dass $f(Q) \subset \mathbb{R}^n$ durch eine der folgenden Gleichungen beschrieben wird:

$$y_1^2 + \dots + y_k^2 - y_{k+1}^2 - \dots - y_r^2 = \begin{cases} 0 & \text{falls } r' = r, & (0) \\ 1 & \text{falls } r' = r + 1, & (1) \\ 2y_{r+1} & \text{falls } r' = r + 2. & (2) \end{cases}$$

In jedem der drei Fälle sind alle k mit $0 \leq k \leq r$ möglich. Nach dem Trägheitsgesetz aus 5.2.5 ist die Zahl k durch die Matrix A' eindeutig festgelegt. Bilder dazu im Fall $n = 3$ findet man in 5.3.6. Hinter dieser Aussage ist ein ernsthaftes Problem versteckt. Sind Q und Q' durch verschiedene Gleichungen erklärt, so könnte man hoffen, dass es dann keine Affinität $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ gibt derart, dass $f(Q) = Q'$. Das ist nicht der Fall: Ist bei Typ (1) der Rang $r \geq 1$ beliebig, und $k = 0$, so wird durch jede Gleichung

$$-y_1^2 - \dots - y_r^2 = 1$$

stets die leere Quadrik beschrieben. Weiter kann man die Gleichung von Typ (0) ohne Änderung der Nullstellen mit -1 multiplizieren. Die Quadriken vom Typ (0) sind **Kegel**, d.h. für jedes $y \in Q$ und $\lambda \in \mathbb{R}$ ist auch $\lambda y \in Q$.

Man kann nun mit etwas Mühe beweisen, dass diese extremen Fälle im wesentlichen die einzigen Ausnahmen sind (vgl. etwa [F1₂, 1.4.5]). Wie man an den Bildern sieht, werden bei den affinen Transformationen Winkel und Abstände verändert. In 5.3.7 werden bessere Transformationen angegeben.

5.3 Euklidische und unitäre Vektorräume

Wenn eine Quadrik durch eine affine Transformation auf Normalform gebracht wird, so ändern sich dabei im Allgemeinen Längen und Winkel. Etwa bei einer Ellipse kann man dabei die Lage und die Länge der Hauptachsen nicht feststellen. Das ist einer der vielen Gründe dafür, Abbildungen zu untersuchen, die Längen und Winkel erhalten. Weiterhin sei an die schon in 4.2.1 bewiesene Aussage erinnert, dass jede reelle symmetrische 2×2 -Matrix diagonalisierbar ist. Auch eine Verallgemeinerung dieses Ergebnisses auf beliebig große quadratische symmetrische Matrizen ist für die Theorie der Quadriken und andere Anwendungen von Bedeutung. Wie so oft hilft dabei der Übergang von den reellen zu den komplexen Zahlen.

5.3.1 Hermitesche Formen

Das kanonische Skalarprodukt im \mathbb{R}^n hatten wir schon in 0.3.1 erklärt durch

$$\langle x, y \rangle := \sum_{i=1}^n x_i y_i.$$

Dadurch erhält man eine Norm

$$\|x\| := \sqrt{\langle x, x \rangle},$$

denn $\langle x, x \rangle \geq 0$ für alle $x \in \mathbb{R}^n$. Im \mathbb{C}^n ist eine solche Definition schon im Fall $n = 1$ nicht mehr sinnvoll, denn für jedes $z \in \mathbb{C}$ hat z^2 im Fall $z \neq 0$ zwei verschiedene komplexe Wurzeln, und von „positiv“ kann man in \mathbb{C} nicht reden (vgl. 1.3.6). Als Ersatz hat man

$$|z| = \sqrt{z \cdot \bar{z}} = \sqrt{x^2 + y^2} \quad \text{für } z = x + iy \quad \text{mit } x, y \in \mathbb{R}$$

als Betrag einer komplexen Zahl. Ganz analog kann man im \mathbb{C}^n ein *kanonisches Skalarprodukt* erklären durch

$$\langle z, w \rangle := \sum_{i=1}^n z_i \bar{w}_i \quad \text{für } z = (z_1, \dots, z_n) \in \mathbb{C}^n \quad \text{und } w = (w_1, \dots, w_n) \in \mathbb{C}^n.$$

Im Gegensatz zu einer symmetrischen Bilinearform auf \mathbb{C}^n ist dann für $\lambda \in \mathbb{C}$

$$\langle z, \lambda \cdot w \rangle = \bar{\lambda} \cdot \langle z, w \rangle \quad \text{und} \quad \langle w, z \rangle = \overline{\langle z, w \rangle}.$$

Das ist die Grundlage für folgende allgemeine

Definition Sei V ein \mathbb{C} -Vektorraum. Eine Abbildung

$$s : V \times V \rightarrow \mathbb{C}$$

heißt **hermitesche Form**, wenn für $v, v', w, w' \in V$ und $\lambda \in \mathbb{C}$ folgende Bedingungen erfüllt sind.

H1 $s(v + v', w) = s(v, w) + s(v', w)$ und $s(\lambda \cdot v, w) = \lambda \cdot s(v, w)$.

H2 $s(v, w + w') = s(v, w) + s(v, w')$ und $s(v, \lambda \cdot w) = \bar{\lambda} \cdot s(v, w)$.

H3 $s(w, v) = \overline{s(v, w)}$.

Sind nur die Bedingungen H1 und H2 erfüllt, so spricht man von einer **Sesquilinearform** („sesqui“ bedeutet $1\frac{1}{2}$).

Aus H3 folgt insbesondere, dass $s(v, v) \in \mathbb{R}$ für alle $v \in V$.

Ganz analog zu 5.2.1, nur an den erforderlichen Stellen komplex konjugiert, kann man eine hermitesche Form s durch eine **hermitesche Matrix** beschreiben, d.h.

$$A \in M(n \times n; \mathbb{C}) \quad \text{mit} \quad {}^t A = \bar{A}.$$

Ist $\mathcal{B} = (v_1, \dots, v_n)$ eine Basis von V , so ist die darstellende Matrix von s bezüglich \mathcal{B} erklärt durch

$$M_{\mathcal{B}}(s) := (s(v_i, v_j)).$$

Ist umgekehrt A eine hermitesche Matrix, so erklärt $A = (a_{ij})$ eine hermitesche Form s_A durch

$$s_A(v, w) := \sum_{i,j=1}^n a_{ij} \lambda_i \bar{\mu}_j, \quad \text{wenn} \quad v = \sum_{i=1}^n \lambda_i v_i \quad \text{und} \quad w = \sum_{i=1}^n \mu_i v_i.$$

Sind \mathcal{A} und \mathcal{B} zwei Basen von V , so erhält man (wie in 5.2.2) für hermitesche Formen eine **Transformationsformel**

$$M_{\mathcal{A}}(s) = {}^t T_{\mathcal{B}}^{\mathcal{A}} \cdot M_{\mathcal{B}}(s) \cdot \overline{T_{\mathcal{B}}^{\mathcal{A}}}, \quad \text{kurz} \quad A = {}^t S \cdot B \cdot \bar{S}.$$

5.3.2 Definitheit

Bezeichnet $\langle \cdot, \cdot \rangle$ das kanonische Skalarprodukt im \mathbb{R}^n oder \mathbb{C}^n , so ist

$$\langle x, x \rangle = x_1^2 + \dots + x_n^2 \geq 0 \quad \text{für} \quad x = (x_1, \dots, x_n) \in \mathbb{R}^n \quad \text{und}$$

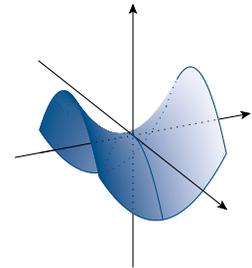
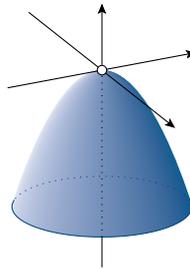
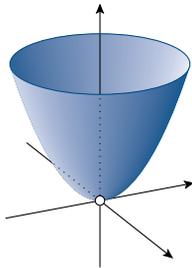
$$\langle z, z \rangle = z_1 \bar{z}_1 + \dots + z_n \bar{z}_n \geq 0 \quad \text{für} \quad z = (z_1, \dots, z_n) \in \mathbb{C}^n.$$

von f in einem Punkt entscheidend (vgl. [FO₂, §7]). Ist etwa $n = 2$ und

$$f(x_1, x_2) = ax_1^2 + bx_2^2, \quad \text{so ist } H := 2 \cdot \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

die HESSE-Matrix im Punkt $\mathbf{o} = (0,0)$, und es gilt

$$\begin{aligned} f \text{ hat in } \mathbf{o} \text{ ein striktes lokales Minimum} &\Leftrightarrow a, b > 0 \Leftrightarrow H \text{ positiv definit,} \\ f \text{ hat in } \mathbf{o} \text{ ein striktes lokales Maximum} &\Leftrightarrow a, b < 0 \Leftrightarrow H \text{ negativ definit,} \\ f \text{ hat in } \mathbf{o} \text{ kein lokales Extremum} &\Leftrightarrow H \text{ indefinit.} \end{aligned}$$



Für Anwendungen ist es nützlich, wenn man mit möglichst wenig Rechenaufwand feststellen kann, ob eine Matrix definit ist oder nicht. Wir beschränken und dabei auf den reellen Fall.

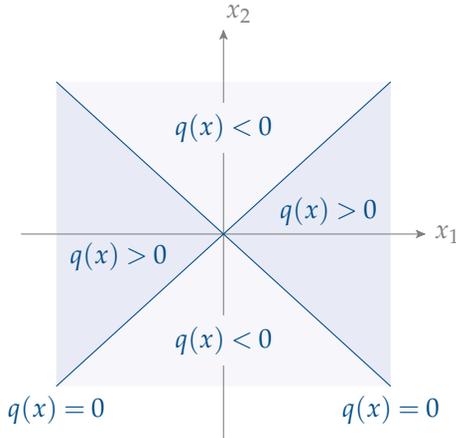
Zunächst eine Warnung: Man hüte sich vor der Vermutung („don't even dream of...“), eine Matrix $A = {}^tA \in M(n \times n; \mathbb{R})$ wäre schon dann positiv definit, wenn es eine Basis (v_1, \dots, v_n) von \mathbb{R}^n gibt, so dass

$${}^t v_i \cdot A \cdot v_i > 0 \quad \text{für } i = 1, \dots, n.$$

Gegenbeispiele gibt es schon ab $n = 2$, etwa

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \text{also } q(x) = {}^t x \cdot A \cdot x = x_1^2 - x_2^2.$$

Die Vorzeichen von $q(x)$ sind wie folgt verteilt:



Offensichtlich kann man eine Basis aus dem positiven Bereich wählen, etwa

$$B = (e_1, v) \quad \text{mit} \quad v = {}^t(2, 1).$$

Dann ist ${}^t e_1 \cdot A \cdot e_1 = 1 > 0$ und ${}^t v \cdot A \cdot v = 3 > 0$, aber ${}^t e_1 \cdot A \cdot v = 2 \neq 0$. In der neuen Basis B wird die durch A erklärte Bilinearform somit beschrieben durch die Matrix

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

Sie hat positive Einträge in der Diagonalen, ist aber nicht diagonal. Eine symmetrische Diagonalisierung von B nach der Methode aus 5.2.4 ergibt

$${}^t T \cdot B \cdot T = A \quad \text{mit} \quad T = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}.$$

Nach diesen Vorbemerkungen ist klar, wie man die Definitheit einer Matrix testen kann: Man diagonalisiert sie symmetrisch und betrachtet die entstandene Diagonale.

Diagonalisierungs-Kriterium für Definitheit Sei V ein \mathbb{R} -Vektorraum und $s : V \times V \rightarrow \mathbb{R}$ eine symmetrische Bilinearform. Hat man eine Basis B von V gefunden, derart dass

$$M_B(s) = \begin{pmatrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_n \end{pmatrix}$$

eine Diagonalmatrix ist, so gilt

- s positiv definit $\Leftrightarrow \alpha_1, \dots, \alpha_n > 0$
- s negativ definit $\Leftrightarrow \alpha_1, \dots, \alpha_n < 0$
- s indefinit \Leftrightarrow es gibt ein $\alpha_i > 0$ und ein $\alpha_j < 0$

Beweis Die Einträge $\alpha_1, \dots, \alpha_n$ in der Diagonale seien so nummeriert, dass

$$\alpha_1, \dots, \alpha_k > 0, \quad \alpha_{k+1}, \dots, \alpha_r < 0, \quad \alpha_{r+1} = \dots = \alpha_n = 0.$$

Ist $\mathcal{B} = (v_1, \dots, v_n)$ und $v = \mu_1 v_1 + \dots + \mu_n v_n \in V$, so folgt

$$s(v, v) = \alpha_1 \cdot \mu_1^2 + \dots + \alpha_k \cdot \mu_k^2 + \alpha_{k+1} \cdot \mu_{k+1}^2 + \dots + \alpha_r \cdot \mu_r^2.$$

Daraus ergibt sich sofort die Behauptung. ■

Beispiel

$$\begin{array}{l}
 A = \begin{array}{|ccc|} \hline 17 & -32 & 29 \\ -32 & 63 & -58 \\ 29 & -58 & 59 \\ \hline \end{array} \\
 \begin{array}{l} (2) + \frac{32}{17} \cdot (1) \\ (3) - \frac{29}{17} \cdot (1) \\ (3) + \frac{58}{47} \cdot (2) \end{array} \\
 D = \begin{array}{|ccc|} \hline 17 & 0 & 29 \\ 0 & \frac{47}{17} & \frac{-58}{17} \\ 29 & \frac{-58}{17} & 59 \\ \hline \end{array} \\
 \begin{array}{|ccc|} \hline 17 & 0 & 0 \\ 0 & \frac{47}{17} & \frac{-58}{17} \\ 0 & \frac{-58}{17} & \frac{162}{17} \\ \hline \end{array} \\
 \begin{array}{|ccc|} \hline 17 & 0 & 0 \\ 0 & \frac{47}{17} & 0 \\ 0 & 0 & \frac{250}{17} \\ \hline \end{array}
 \end{array}$$

Also ist A positiv definit. Wie man sieht, ist der Rechenaufwand auch kaum größer als bei der Berechnung von $\det A$ mit Hilfe von Zeilenumformungen. Man muss in jedem Schritt nur noch die entsprechende Spaltenumformung anschließen. Da

$$D = {}^t T \cdot A \cdot T \quad \text{ist} \quad \det A = \det D = 250.$$

Das folgt ganz allgemein aus der speziellen Form von T : Wenn nur Umformungen vom Typ (1) und (2) vorgenommen werden, ist $\det T = \pm 1$.

Eine reelle Zahl ist genau dann positiv, wenn sie Quadrat einer Zahl ungleich Null ist. Als Folgerung aus obigem Satz erhält man ein analoges Ergebnis für Matrizen.

Korollar Eine symmetrische Matrix $A \in M(n \times n; \mathbb{R})$ ist genau dann positiv definit, wenn es ein $C \in GL(n; \mathbb{R})$ gibt derart, dass

$$A = {}^t C \cdot C.$$

Beweis Ist $A = {}^tC \cdot C$ und $y = C \cdot x$ für $x \in \mathbb{R}^n$, so folgt

$${}^tAx = {}^tx{}^tCCx = {}^tyy = y_1^2 + \dots + y_n^2 > 0$$

für $x \neq \mathbf{o}$, also $y \neq \mathbf{o}$.

Ist A positiv definit, so gibt es ein $S \in \text{GL}(n; \mathbb{R})$ mit $A = {}^tSDS$, wobei D eine Diagonalmatrix ist, mit Einträgen $\alpha_1, \dots, \alpha_n > 0$. Bezeichnet D' die Diagonalmatrix mit Einträgen $\sqrt{\alpha_1}, \dots, \sqrt{\alpha_n}$, so folgt

$$A = {}^tSD' \cdot D'S = {}^tC \cdot C \quad \text{mit} \quad C := D'S.$$

■

Es gibt andere klassische Kriterien für Definitheit, die nicht die symmetrische Diagonalisierung, sondern Determinanten nutzen. Auch hier beschränken wir uns auf den reellen Fall.

Bemerkung 1 *Ist die symmetrische Matrix $A = (a_{ij})$ positiv definit, so gilt*

$$a_{ii} > 0 \quad \text{für alle } i \quad \text{und} \quad \det A > 0.$$

Beweis Da $a_{ii} = {}^te_i \cdot A \cdot e_i$, muss $a_{ii} > 0$ sein. Nach 5.2.4 gibt es ein $T \in \text{GL}(n; \mathbb{R})$ derart, dass

$${}^tT \cdot A \cdot T = \begin{pmatrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_n \end{pmatrix} =: D.$$

D beschreibt die durch A gegebene Bilinearform bezüglich einer transformierten Basis des \mathbb{R}^n . Weiter gilt

$$0 < \alpha_1 \cdot \dots \cdot \alpha_n = \det D = (\det T)^2 \cdot \det A,$$

also muss auch $\det A > 0$ sein. ■

Für $n = 2$ sind die notwendigen Bedingungen aus Bemerkung 1 auch hinreichend:

Bemerkung 2 *Ist*

$$A = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \in \text{M}(2 \times 2; \mathbb{R})$$

mit $a > 0$ und $\det A > 0$, so ist A positiv definit.

Beweis Sei $x = {}^t(x_1, x_2) \in \mathbb{R}^2$. Dann erhält man durch quadratische Ergänzung

$$\begin{aligned} a \cdot ({}^t x \cdot A \cdot x) &= a \cdot (ax_1^2 + 2bx_1x_2 + cx_2^2) = (a^2x_1^2 + 2abx_1x_2 + b^2x_2^2) + (ac - b^2)x_2^2 \\ &= (ax_1 + bx_2)^2 + (\det A)x_2^2. \end{aligned}$$

Also ist $a \cdot ({}^t x \cdot A \cdot x) > 0$ für $x \neq \mathbf{o}$. Wegen $a > 0$ ist auch ${}^t x \cdot A \cdot x > 0$. ■

Die beiden Bemerkungen 1 und 2 kann man wie folgt verallgemeinern. Zu einer Matrix $A = (a_{ij}) \in M(n \times n; \mathbb{R})$ betrachten wir für $k = 1, \dots, n$ die Teilmatrix

$$A_k := \begin{pmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & & \vdots \\ a_{k1} & \cdots & a_{kk} \end{pmatrix}.$$

Die Determinante $\det A_k$ nennt man einen **Haupt-Minor** von A .

Haupt-Minoren-Kriterium für Definitheit Für eine symmetrische Matrix $A \in M(n \times n; \mathbb{R})$ gilt:

$$\begin{aligned} A \text{ positiv definit} &\Leftrightarrow \det A_k > 0 \text{ für } k = 1, \dots, n, \\ A \text{ negativ definit} &\Leftrightarrow \det(-A_k) > 0 \text{ für } k = 1, \dots, n. \end{aligned}$$

Vorsicht! $A = -E_n$ ist negativ definit, aber

$$\det A_k = \det(-E_k) = (-1)^k \cdot \det E_k = (-1)^k.$$

Offensichtlich gilt: A negativ definit $\Leftrightarrow -A$ positiv definit

$$\Leftrightarrow \det A_k < 0 \text{ für } k \text{ ungerade und } \det A_k > 0 \text{ für } k \text{ gerade.}$$

Beweis Nach der Vorbemerkung genügt es, die erste Äquivalenz zu zeigen.

„ \Rightarrow “ Die Teilmatrix beschreibt eine symmetrische Bilinearform auf dem zu \mathbb{R}^k isomorphen Untervektorraum

$$V := \{(x_1, \dots, x_n) \in \mathbb{R}^n : x_{k+1} = \dots = x_n = 0\}.$$

Also folgt $\det A_k > 0$ aus der obigen Bemerkung 1.

„ \Leftarrow “ Für $n = 2$ ging das durch eine einfache Rechnung mit quadratischer Ergänzung; im allgemeinen Fall ist es formal übersichtlicher, eine Induktion und den Matrizenkalkül zu verwenden.

Der Fall $n = 1$ ist klar. Sei also die Implikation „ \Leftarrow “ schon für $n - 1$ bewiesen, dann ist A_{n-1} positiv definit. Nach 5.2.4, angewandt im Fall $K = \mathbb{R}$, gibt es ein $S' \in GL(n - 1; \mathbb{R})$ derart, dass

$${}^t S' \cdot A_{n-1} \cdot S' = E_{n-1}.$$

Wir erweitern die Transformationsmatrix S zu

$$S := \left(\begin{array}{ccc|c} & & & 0 \\ & S' & & \vdots \\ & & & 0 \\ \hline 0 & \cdots & 0 & 1 \end{array} \right) \in \text{GL}(n; \mathbb{R})$$

und definieren die transformierte Matrix

$$B := {}^tS \cdot A \cdot S = \left(\begin{array}{ccc|c} & & & \beta_1 \\ & E_{n-1} & & \vdots \\ & & & \beta_{n-1} \\ \hline \beta_1 & \cdots & \beta_{n-1} & \beta_n \end{array} \right).$$

Mit der neuen Transformationsmatrix

$$T := \left(\begin{array}{ccc|c} & & & -\beta_1 \\ & E_{n-1} & & \vdots \\ & & & -\beta_{n-1} \\ \hline 0 & \cdots & 0 & 1 \end{array} \right) \text{ erh\u00e4lt man } {}^tT \cdot B \cdot T = \left(\begin{array}{ccc|c} & & & 0 \\ & E_{n-1} & & \vdots \\ & & & 0 \\ \hline 0 & \cdots & 0 & \gamma \end{array} \right) =: D,$$

wobei $\gamma = \beta_n - \beta_1^2 - \dots - \beta_{n-1}^2 = \det B$. Da $\det T = 1$, folgt

$$\gamma = \det D = \det B = \det({}^tSAS) = \det A(\det S)^2.$$

Da $\det A > 0$, ist $\gamma > 0$ und somit ist A positiv definit. ■

Der Leser m\u00f6ge zur \u00dcbung diesen Beweis im Fall $n = 2$ mit dem Beweis von Bemerkung 2 vergleichen!

Im schon oben angegeben Beispiel

$$A = \begin{pmatrix} 17 & -32 & 29 \\ -32 & 63 & -58 \\ 29 & -58 & 59 \end{pmatrix}$$

ist $\det A_1 = 17$, $\det A_2 = 47$ und $\det A = 250$. Also ist das Haupt-Minoren-Kriterium f\u00fcr positive Definitheit erf\u00fcllt. Offensichtlich kann man die Werte der Haupt-Minoren wegen der speziellen Art der Umformungen direkt an der oben berechneten Diagonalmatrix D ablesen.

Nach diesen Vor\u00fcberlegungen zur Definitheit ben\u00fctzen wir f\u00fcr den Rest dieses Kapitels zur Vereinfachung folgende Namen:

Definition Ein **Skalarprodukt** in einem reellen bzw. komplexen Vektorraum ist eine positiv definite symmetrische Bilinearform bzw. eine positiv definite hermitesche Form.

Ein **euklidischer** bzw. **unitärer** Vektorraum ist ein reeller bzw. komplexer Vektorraum zusammen mit einem Skalarprodukt.

Beispiel 1 Standardbeispiele sind die Vektorräume \mathbb{R}^n und \mathbb{C}^n mit dem kanonischen Skalarprodukt

$$\langle x, y \rangle = {}^t x \cdot y = \sum_{i=1}^n x_i y_i \quad \text{bzw.} \quad \langle z, w \rangle = {}^t z \cdot \bar{w} = \sum_{i=1}^n z_i \bar{w}_i.$$

Ist $A = (a_{ij})$ eine positiv definite symmetrische bzw. hermitesche Matrix, so wird dadurch auf \mathbb{R}^n bzw. \mathbb{C}^n ein Skalarprodukt

$$\langle x, y \rangle_A := {}^t x \cdot A \cdot y = \sum_{i,j=1}^n a_{ij} x_i y_j \quad \text{bzw.} \quad \langle z, w \rangle_A := {}^t z \cdot A \cdot \bar{w} = \sum_{i,j=1}^n a_{ij} z_i \bar{w}_j$$

erklärt. Es steht in engem Zusammenhang mit dem kanonischen Skalarprodukt:

$$\langle x, y \rangle_A = \langle A \cdot x, y \rangle = \langle x, A \cdot y \rangle \quad \text{bzw.} \quad \langle z, w \rangle_A = \langle A \cdot z, w \rangle = \langle z, A \cdot w \rangle.$$

Dabei ist zu bedenken, dass ${}^t A = A$ bzw. ${}^t A = \bar{A}$. Eine derartige Matrix kann man aus jedem $B \in \text{GL}(n; \mathbb{R})$ bzw. $B \in \text{GL}(n; \mathbb{C})$ erhalten, indem man

$$A := {}^t B \cdot B \quad \text{bzw.} \quad A := {}^t \bar{B} \cdot B$$

setzt. Dann ist A positiv definit und symmetrisch bzw. hermitesch, wie man leicht sieht.

Beispiel 2 Ein ganz anderes Beispiel kommt aus der Analysis. Ist V der \mathbb{R} -Vektorraum der auf einem Intervall $[a, b] \subset \mathbb{R}$ stetigen Funktionen, so kann man

$$\langle f, g \rangle := \int_a^b f(t) \cdot g(t) dt \quad \text{für} \quad f, g \in V$$

erklären. Nach den Rechenregeln für Integrale ist das eine symmetrische Bilinearform auf V , und ist

$$\langle f, f \rangle = \int_a^b f(t)^2 dt = 0,$$

so muss wegen der vorausgesetzten Stetigkeit $f = \mathbf{0}$ sein. Also ist $\langle \cdot, \cdot \rangle$ positiv definit. Man beachte dabei, dass V unendliche Dimension hat, und $\langle \cdot, \cdot \rangle$ ohne Benutzung einer Basis erklärt ist.

5.3.3 Orthogonalität

Gegeben sei ein euklidischer bzw. unitärer Vektorraum V mit Skalarprodukt

$$\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{K}, (v, w) \mapsto \langle v, w \rangle,$$

wobei $\mathbb{K} = \mathbb{R}$ bzw. $\mathbb{K} = \mathbb{C}$. Für jedes $v \in V$ ist dann eine *Norm* erklärt durch

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

Man nennt zwei Vektoren $v, w \in V$ *orthogonal*, wenn

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

Ein m -Tupel (v_1, \dots, v_m) von Vektoren aus V heißt

$$\begin{aligned} \textit{orthogonal} &\Leftrightarrow \langle v_i, v_j \rangle = 0 \quad \text{für } i \neq j \text{ und} \\ \textit{orthonormal} &\Leftrightarrow \textit{orthogonal} \text{ und } \|v_i\| = 1 \text{ für alle } i. \end{aligned}$$

Ist $\mathcal{B} = (v_1, \dots, v_n)$ eine orthogonale Basis von V , so erhält man daraus eine *Orthonormalbasis* (d.h. orthonormale Basis) $\tilde{\mathcal{B}} = (w_1, \dots, w_n)$, indem man

$$w_i := \frac{1}{\|v_i\|} \cdot v_i \quad \text{für } i = 1, \dots, n$$

setzt.

Beispiel 1 Im \mathbb{R}^n bzw. \mathbb{C}^n ist die kanonische Basis (e_1, \dots, e_n) orthonormal bezüglich dem kanonischen Skalarprodukt. Es gibt jedoch viele andere orthonormale Basen. Darauf kommen wir beim Satz von GRAM-SCHMIDT zurück.

Beispiel 2 Im Vektorraum V der auf $[0, 2\pi] \subset \mathbb{R}$ stetigen reellwertigen Funktionen ist durch

$$\langle f, g \rangle := \frac{1}{\pi} \cdot \int_0^{2\pi} f(t) \cdot g(t) dt$$

ein Skalarprodukt gegeben. Die Funktionen

$$\cos(kx) \quad \text{und} \quad \sin(kx)$$

sind für alle $k \in \mathbb{N}$ in V enthalten. Diese unendliche Familie ist orthogonal, denn wie man in der Analysis lernt ([FO₁, §23]), ist

$$\begin{aligned} \langle \cos(kx), \sin(lx) \rangle &= 0 \quad \text{für alle } k, l \in \mathbb{N} \text{ und} \\ \langle \cos(kx), \cos(lx) \rangle &= \langle \sin(kx), \sin(lx) \rangle = 0 \quad \text{für } k \neq l. \end{aligned}$$

Weiterhin ist

$$\|\cos(kx)\| = \|\sin(kx)\| = 1 \quad \text{für } k \geq 1,$$

also ist die Familie

$$\mathcal{B} := (1, \cos x, \cos(2x), \dots, \sin x, \sin(2x), \dots)$$

sogar orthonormal. Das ist die algebraische Grundlage der Theorie der FOURIER-Reihen.

Zunächst zwei wichtige elementare Eigenschaften von Orthogonalität und Orthonormalität.

Bemerkung 1 Ein orthogonales m -Tupel (v_1, \dots, v_m) mit $v_i \neq \mathbf{o}$ für alle i ist linear unabhängig.

Beweis Angenommen

$$\lambda_1 v_1 + \dots + \lambda_m v_m = \mathbf{o}. \quad (*)$$

Für jedes i kann man das Skalarprodukt von $(*)$ mit v_i bilden. Das ergibt

$$0 = \left\langle \sum_{j=1}^m \lambda_j v_j, v_i \right\rangle = \langle \lambda_i v_i, v_i \rangle = \lambda_i \cdot \langle v_i, v_i \rangle.$$

Da $\langle v_i, v_i \rangle > 0$ muss $\lambda_i = 0$ sein. ■

Daraus folgt insbesondere, dass die oben angegebene Familie \mathcal{B} der trigonometrischen Funktionen linear unabhängig ist. In Beispiel 9 aus 2.1.4 hatten wir das in einem sehr einfachen Spezialfall schon gesehen.

Bemerkung 2 Ist $\mathcal{B} = (v_1, \dots, v_n)$ eine Orthonormalbasis von V , so kann man die Darstellung eines jeden Vektors $v \in V$ berechnen als

$$v = \sum_{i=1}^n \langle v, v_i \rangle \cdot v_i.$$

Beweis Es gibt eine eindeutige Darstellung

$$v = \sum_{j=1}^n \lambda_j v_j \quad \text{mit} \quad \lambda_j \in \mathbb{K}.$$

Das Skalarprodukt mit v_i ergibt

$$\langle v, v_i \rangle = \left\langle \sum_{j=1}^n \lambda_j v_j, v_i \right\rangle = \lambda_i \cdot \langle v_i, v_i \rangle = \lambda_i. \quad \blacksquare$$

Mit Hilfe eines Skalarprodukts kann man Orthogonalität, d.h. die Eigenschaft „senkrecht zu stehen“ erklären. Ist V euklidisch bzw. unitär, so stehen zwei Vektoren $v, w \in V$ *senkrecht*, in Zeichen

$$v \perp w \quad :\Leftrightarrow \quad \langle v, w \rangle = 0.$$

In diesem Sinne steht der Nullvektor auf jedem anderen Vektor senkrecht. Ist $W \subset V$ ein Untervektorraum und $v \in V$, so ist v senkrecht zu W , in Zeichen

$$v \perp W \quad :\Leftrightarrow \quad v \perp w \quad \text{für alle } w \in W.$$

Sind schließlich $W, W' \subset V$ Untervektorräume, so nennt man sie *senkrecht*, in Zeichen

$$W \perp W' \quad :\Leftrightarrow \quad w \perp w' \quad \text{für alle } w \in W \text{ und } w' \in W'.$$

Sind (w_1, \dots, w_k) und (w'_1, \dots, w'_l) beliebige Basen von W und W' , so gilt

$$W \perp W' \quad \Leftrightarrow \quad w_i \perp w'_j \quad \text{für alle } i = 1, \dots, k \text{ und } j = 1, \dots, l. \quad (\perp)$$

Die Richtung „ \Rightarrow “ folgt aus der Definition; für „ \Leftarrow “ sei

$$w = \sum_{i=1}^k \lambda_i w_i \in W \quad \text{und} \quad w' = \sum_{j=1}^l \mu_j w'_j \in W'.$$

Dann ist $\langle w, w' \rangle = \sum_{i,j} \lambda_i \bar{\mu}_j \cdot \langle w_i, w'_j \rangle = 0$. ■

Diesen „Orthogonalitäts-Test“ (\perp) kann man in der Praxis anwenden, um etwa eine Kerze senkrecht im Ständer auf den Tisch zu bekommen. Zwei Personen betrachten sie aus linear unabhängigen Richtungen. Die erste Person dreht sie so lange, bis sie aus ihrer Richtung senkrecht erscheint. Dann biegt sie die zweite Person in der Richtung der ersten Person in eine senkrechte Position. Nach der oben bewiesenen Aussage (\perp) steht die Kerze dann aus allen Richtungen senkrecht. Am genauesten wird das Ergebnis, wenn die beiden Personen die Kerze aus senkrechten Richtungen betrachten.

Nun zur Frage der Existenz von Orthonormalbasen. Im \mathbb{K}^n gibt es die kanonische Orthonormalbasis, aber oft will man eine andere Basis wählen, die einem gegebenen Problem besser angepasst ist. Eine Antwort gibt der

Orthonormalisierungssatz von GRAM und SCHMIDT *Gegeben sei ein euklidischer bzw. unitärer Vektorraum V mit $\dim V < \infty$, und ein Untervektorraum $W \subset V$ mit einer Orthonormalbasis (w_1, \dots, w_m) . Dann gibt es eine Ergänzung zu einer Orthonormalbasis*

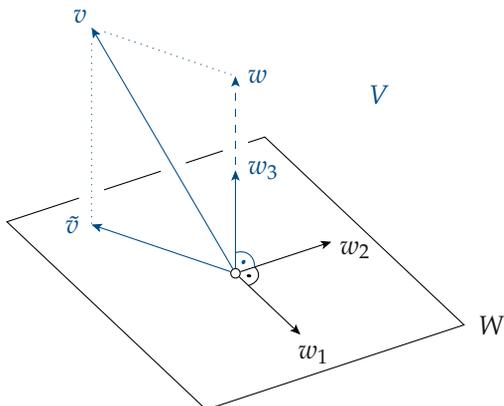
$$(w_1, \dots, w_m, w_{m+1}, \dots, w_n) \quad \text{von } V.$$

Da man auch mit $W = \{\mathbf{o}\}$ starten kann, erhält man als

Korollar *Jeder endlich-dimensionale euklidische bzw. unitäre Vektorraum besitzt eine Orthonormalbasis.* ■

Beweis des Orthonormalisierungssatzes Ist $W = V$, so ist nichts mehr zu ergänzen. Andernfalls führen wird die Ergänzung schrittweise durch. Ist $\mathbf{o} \neq v \in V \setminus W$, so betrachten wir die senkrechte Projektion von v auf W :

$$\tilde{v} := \langle v, w_1 \rangle \cdot w_1 + \dots + \langle v, w_m \rangle \cdot w_m \in W.$$



Dann steht $w := v - \tilde{v}$ senkrecht auf W :

$$\langle w, w_i \rangle = \langle v - \tilde{v}, w_i \rangle = \langle v, w_i \rangle - \langle \tilde{v}, w_i \rangle = \langle v, w_i \rangle - \langle v, w_i \rangle = 0.$$

Um den nächsten Vektor w_{m+1} für die Orthonormalbasis zu erhalten, setzt man

$$w_{m+1} := \frac{1}{\|w\|} \cdot w.$$

Durch Fortsetzung dieses Verfahrens erhält man eine Orthonormalbasis (w_1, \dots, w_n) . ■

Der Beweis ist ganz konstruktiv, wir geben ein

Beispiel 1 Sei $V := \text{Span}({}^t(0,3,4), {}^t(2,1,3)) \subset \mathbb{R}^3$ und $W := \{\mathbf{o}\}$.

Wir starten mit $v_1 := {}^t(0,3,4)$, $\|v_1\| = 5$ und erhalten $w_1 = \frac{1}{5} \cdot v_1 = \frac{1}{5} \cdot {}^t(0,3,4)$.

Im nächsten Schritt sei $v_2 = {}^t(2,1,3)$. Dann ist

$$\langle v_2, w_1 \rangle = 3, \quad \tilde{v}_2 = \langle v_2, w_1 \rangle \cdot w_1 = \frac{3}{5} \cdot {}^t(0,3,4) \quad \text{und} \quad w = v_2 - \tilde{v}_2 = \frac{1}{5} \cdot {}^t(10, -4, 3).$$

Da $\|w\|^2 = 5$, erhält man schließlich $w_2 := \frac{\sqrt{5}}{25} \cdot {}^t(10, -4, 3)$.

Will man allgemeiner für einen durch eine Basis (v_1, \dots, v_n) gegebenen Untervektorraum $V \subset \mathbb{R}^N$ mit $N \geq n$ eine bezüglich des kanonischen Skalarprodukts im \mathbb{R}^N orthonormale Basis (w_1, \dots, w_n) finden, so wird die Rechnung einfacher, wenn man in zwei Etappen vorgeht: Man bestimmt zunächst eine orthogonale Basis (u_1, \dots, u_n) von V und normiert sie anschließend zu

$$w_i := \frac{1}{\|u_i\|} \cdot u_i.$$

Der Vorteil besteht darin, dass die lästigen Quadratwurzeln erst am Ende der Rechnung auftreten.

Im ersten Schritt setzt man $u_1 = v_1$. Im zweiten Schritt sei

$$\tilde{v}_2 := \frac{\langle v_2, u_1 \rangle}{\langle u_1, u_1 \rangle} \cdot u_1 \quad \text{und} \quad u_2 := v_2 - \tilde{v}_2.$$

Dann ist $\langle u_2, u_1 \rangle = \langle v_2, v_1 \rangle - \langle \tilde{v}_2, u_1 \rangle = 0$ und $\text{Span}(u_1, u_2) = \text{Span}(v_1, v_2)$. Hat man für $m < n$ schon orthogonale (u_1, \dots, u_m) mit $\text{Span}(u_1, \dots, u_m) = \text{Span}(v_1, \dots, v_m)$ gefunden, so setzt man

$$\tilde{v}_{m+1} := \sum_{i=1}^m \frac{\langle v_{m+1}, u_i \rangle}{\langle u_i, u_i \rangle} \cdot u_i \quad \text{und} \quad u_{m+1} := v_{m+1} - \tilde{v}_{m+1}.$$

Dann ist $\langle u_{m+1}, u_i \rangle = \langle v_{m+1}, u_i \rangle - \langle \tilde{v}_{m+1}, u_i \rangle = 0$ für $i = 1, \dots, m$.

Damit ist die erste Etappe beendet, nun genügt es, die u_i zu normieren.

Beispiel 2 Sei $V = \text{Span}(v_1, v_2, v_3) \subset \mathbb{R}^4$ mit

$$v_1 = (1, 1, 0, 0), \quad v_2 = (1, 1, 0, 1) \quad \text{und} \quad v_3 = (1, 0, 1, 1).$$

Dann ist $u_1 = v_1$, $u_2 = (0, 0, 0, 1)$ und $u_3 = \frac{1}{2}(1, -1, 2, 0)$, sowie

$$w_1 = \frac{1}{2}\sqrt{2} \cdot u_1, \quad w_2 = u_2 \quad \text{und} \quad w_3 = \frac{1}{6}\sqrt{6} \cdot u_3.$$

Also ist (w_1, w_2, w_3) eine Orthonormalbasis von V .

Hat man im \mathbb{R}^3 linear unabhängige Vektoren v_1, v_2 , und ist $W = \text{Span}(v_1, v_2)$, so steht das Vektorprodukt $w := v_1 \times v_2$ senkrecht auf W , und (v_1, v_2, w) ist eine Basis von \mathbb{R}^3 (vgl. 0.3.7). Diese Konstruktion kann man allgemeiner ausführen.

Ist V ein euklidischer oder unitärer Vektorraum, und $W \subset V$ ein Untervektorraum, so ist das **orthogonale Komplement** von W erklärt als

$$W^\perp := \{v \in V : v \perp W\} \subset V.$$

Offensichtlich ist $W^\perp \subset V$ ein Untervektorraum.

Ist $W' \subset V$ ein weiterer Untervektorraum, so heißt V **orthogonale Summe** von W und W' , in Zeichen

$$V = W \oplus W',$$

wenn $V = W \oplus W'$ und $W \perp W'$. Die Existenz eines orthogonalen Summanden folgt aus dem Orthonormalisierungs-Satz:

Korollar 2 Ist $W \subset V$ Untervektorraum eines endlich-dimensionalen euklidischen oder unitären Vektorraums, so ist

$$V = W \oplus W^\perp \quad \text{und} \quad \dim V = \dim W + \dim W^\perp.$$

Beweis Wir wählen eine Orthonormalbasis (w_1, \dots, w_n) von V derart, dass (w_1, \dots, w_m) Basis von W ist. Ist

$$W' = \text{Span}(w_{m+1}, \dots, w_n),$$

so bleibt nach der Charakterisierung einer direkten Summe in 2.2.5 noch $W' = W^\perp$ zu zeigen. $W' \subset W^\perp$ ist klar.

Jedes $v \in V$ hat nach Bemerkung 1 eine eindeutige Darstellung

$$v = \sum_{i=1}^n \langle v, w_i \rangle \cdot w_i.$$

Ist $v \in W^\perp$, so ist $\langle v, w_i \rangle = 0$ für $i = 1, \dots, m$, also folgt $v \in W'$ und $W^\perp \subset W'$. ■

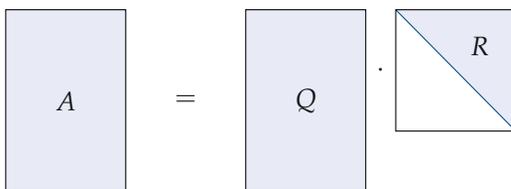
5.3.4 QR-Zerlegung und Methode der kleinsten Quadrate*

Etwa zur Lösung linearer Gleichungssysteme kann die in 2.4.8 beschriebene LR-Zerlegung invertierbarer Matrizen helfen. Es gibt eine andere Zerlegung, die nicht nur für quadratische Matrizen ausführbar ist. Wir wie anschließend sehen werden, kann sie recht nützlich sein.

Satz über die QR-Zerlegung Sei $A \in M(m \times n; \mathbb{R})$ mit $\text{rang } A = n$, also $m \geq n$, gegeben. Dann gibt es eine Matrix $Q \in M(m \times n; \mathbb{R})$ mit orthogonalen Spalten, d.h. ${}^t Q \cdot Q = E_n$, und eine obere Dreiecksmatrix $R \in GL(n; \mathbb{R})$ derart, dass

$$A = Q \cdot R.$$

Schematisch kann man das so aufzeichnen:



Beweis Seien $v_1, \dots, v_n \in \mathbb{R}^m$ die Spalten von A . Wie sich zeigen wird genügt es, aus v_1, \dots, v_n nach dem GRAM-SCHMIDT-Verfahren eine Orthonormalbasis w_1, \dots, w_n von $\text{Span}(v_1, \dots, v_n)$ zu berechnen, und sie als Spalten von Q zu verwenden.

Die einzelnen Schritte verlaufen so:

$$\begin{aligned} w_1 &:= \frac{1}{\|v_1\|} \cdot v_1, & \text{also } v_1 &= \|v_1\| \cdot w_1. \\ \tilde{w}_2 &:= v_2 - \langle w_1, v_2 \rangle \cdot w_1, & w_2 &:= \frac{1}{\|\tilde{w}_2\|} \cdot \tilde{w}_2, & \text{also } v_2 &= \langle w_1, v_2 \rangle \cdot w_1 + \|\tilde{w}_2\| \cdot w_2 \\ &\vdots & & & & \\ v_n &= \langle w_1, v_n \rangle \cdot w_1 + \dots + \langle w_{n-1}, v_n \rangle \cdot w_{n-1} + \|\tilde{w}_n\| \cdot w_n \end{aligned}$$

Diese Darstellung von (v_1, \dots, v_n) durch (w_1, \dots, w_n) ergibt die Matrix

$$R := \begin{pmatrix} \|v_1\| & \langle w_1, v_2 \rangle & \dots & \langle w_1, v_n \rangle \\ & \|\tilde{w}_2\| & \dots & \langle w_2, v_n \rangle \\ & & \ddots & \vdots \\ & 0 & & \|\tilde{w}_n\| \end{pmatrix}.$$

Sind (w_1, \dots, w_n) die Spalten von Q , so ist offensichtlich $A = Q \cdot R$. ■

Beispiel 1 Im Fall $n = 2$ wollen wir die Einträge von Q und R aus den Einträgen von A explizit ausrechnen. Es ist

$$w_1 = \frac{1}{\|v_1\|} \cdot v_1 \quad \text{und} \quad \tilde{w}_2 = v_2 - \frac{\langle v_1, v_2 \rangle}{\|v_1\|^2} \cdot v_1, \quad \text{also}$$

$$\langle w_1, v_2 \rangle = \frac{\langle v_1, v_2 \rangle}{\|v_1\|} \quad \text{und} \quad \|\tilde{w}_2\| = \sqrt{\|v_2\|^2 - \frac{\langle v_1, v_2 \rangle^2}{\|v_1\|^2}}.$$

Wie man sieht, werden diese neuen Einträge ziemlich „verwurzelt“.

In engem Zusammenhang mit der QR-Zerlegung steht das folgende

Problem Gegeben sei eine Matrix $A \in M(m \times n; \mathbb{R})$ und ein $b \in \mathbb{R}^m$ derart, dass das lineare Gleichungssystem $A \cdot x = b$ keine Lösung $x \in \mathbb{R}^n$ besitzt. Gesucht ist ein $x^* \in \mathbb{R}^n$, das eine möglichst gute Approximation für die fehlende Lösung ist.

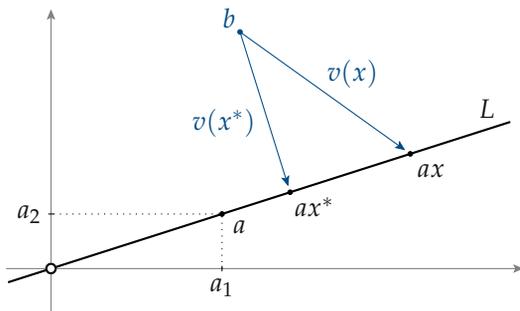
Nach den Ergebnissen von 0.5.3 tritt dieses Problem auf, wenn $\text{rang}(A, b) > \text{rang } A$. In diesem Fall ist das Gleichungssystem *überbestimmt*. Wir beginnen mit dem einfachsten Fall $n = 1$ und $m > 1$ beliebig. Das Gleichungssystem lautet dann

$$\begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} \cdot x = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}, \quad \text{kurz} \quad ax = b \quad \text{mit} \quad a \neq 0. \quad (-)$$

Um ein optimales x^* zu finden, erklären wir für jedes beliebige $x \in \mathbb{R}$ einen *Fehlervektor*

$$v(x) := a \cdot x - b \in \mathbb{R}^m.$$

Die naheliegende Bedingung für x^* ist nun, dass der Wert von $\|v(x^*)\| \in \mathbb{R}_+$ minimal ist. Für $m = 2$ hat man folgendes Bild:



Liegt b auf der Geraden $L = \mathbb{R} \cdot a$, so gibt es eine eindeutige Lösung x von $(-)$ und man kann $x^* := x$ wählen. Andernfalls fällt man wie in 0.3.4 das Lot von b auf die Gerade L , das ergibt einen Fußpunkt $a \cdot x^*$ mit $a \perp v(x^*)$. Nach dem Satz von PYTHAGORAS ist $\|v(x^*)\| \leq \|v(x)\|$ für alle $x \in \mathbb{R}$. Die Bedingung für das Minimum lautet also

$$\langle a, v(x^*) \rangle = 0, \quad \text{d.h.} \quad \langle a, a \rangle \cdot x^* - \langle a, b \rangle = 0 \quad \text{oder}$$

$$(a_1, \dots, a_m) \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} x^* = (a_1, \dots, a_m) \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}, \quad \text{kurz} \quad {}^t a a x^* = {}^t a b. \quad (*)$$

Aus dem im allgemeinen unlösbaren System $(-)$ hat man also das System $(*)$ gemacht, mit der eindeutigen Lösung

$$x^* = \frac{{}^t a b}{{}^t a a} = \frac{\langle a, b \rangle}{\|a\|^2}.$$

Nach diesem Spezialfall ist ziemlich klar, wie der allgemeine Fall

$$A \cdot x = b \quad \text{mit} \quad A \in M(m \times n; \mathbb{R}), \quad b \in \mathbb{R}^m \quad \text{und} \quad \text{rang } A = n. \quad (-)$$

zu behandeln ist. Bezeichnen $a^{(1)}, \dots, a^{(n)} \in \mathbb{R}^m$ die Spalten von A , so betrachten wir den Untervektorraum

$$W := \text{Span}(a^{(1)}, \dots, a^{(n)}) \subset \mathbb{R}^m \quad \text{mit} \quad \dim W = n.$$

Das System $(-)$ ist genau dann lösbar, wenn $b \in W$. Für beliebiges $x \in \mathbb{R}^n$ erklären wir wieder einen Fehlervektor

$$v(x) := A \cdot x - b \in \mathbb{R}^m.$$

Die Bedingung für ein Minimum von $\|v(x)\|$ lautet wieder nach PYTHAGORAS

$$v(x^*) \perp W, \quad \text{das ist gleichwertig mit} \quad v(x^*) \perp a^{(j)} \quad \text{für} \quad j = 1, \dots, n,$$

und in Matrizen geschrieben bedeutet das

$${}^tAAx^* = {}^tAb. \quad (*)$$

Da $\text{rang } A = n$, ist ${}^tAA \in GL(n; \mathbb{R})$ und das System $(*)$ ist eindeutig lösbar durch

$$x^* = ({}^tAA)^{-1} \cdot {}^tAb.$$

Für die Norm des minimalen Fehlers ergibt sich unter Benutzung von $(*)$

$$\|v(x^*)\|^2 = {}^t(Ax^* - b)(Ax^* - b) = {}^tbb - {}^tbAx^*.$$

Damit ist das oben formulierte Problem für die Theorie gelöst: Man multipliziert die im allgemeinen unlösbare Bedingung $Ax = b$ von links mit tA und erhält eine eindeutige beste Approximation.

Nun aber einige Anmerkungen zur Geschichte und zur effizienten Berechnung von x^* . Überbestimmte Gleichungssysteme können auftreten, wenn man zur Bestimmung von n Ergebnissen eine große Zahl m von Messungen durchführt, bei denen aber schwer vermeidliche Messfehler auftreten. Dieses Problem hat GAUSS bei der Bestimmung der Bahnen von Planetoiden in [GA₂] systematisch in Angriff genommen, es wurde anschließend auch in der Landvermessung mit Erfolg angewandt. Das oben beschriebene Verfahren wird *Methode der kleinsten Quadrate* genannt. Schreibt man wie oben im Fall $n = 1$

$$v(x) = ax - b, \quad \text{so ist} \quad \|v(x)\|^2 = \sum_{i=1}^m (a_i x - b_i)^2,$$

und diese Summe von Quadraten soll minimal werden. Die Bedingung $(*)$ hat schon GAUSS [GA₂, p.20] angegeben. GAUSS verwendet stattdessen eine sehr geschickte eigene Notation. Zur Begründung der Bedingung $(*)$ schreibt er nur lakonisch „*Facile quidem perspicitur...*“.

Als Hilfsmittel zur Lösung der Gleichung $(*)$ beschreibt GAUSS dann das im Prinzip schon lange vorher verwendete Verfahren von Eliminationen ganz systematisch für quadratische Matrizen. Der Name *GAUSS-Elimination* wurde erst viel später von dem Landvermesser W. JORDAN [JO], einem glühenden Verehrer von GAUSS, eingeführt.

Eine etwas andere Beschreibung der Lösung von $(*)$ als mit Hilfe von Elimination liefert die QR-Zerlegung. Ist

$$A = QR \quad \text{mit} \quad Q \in M(m \times n; \mathbb{R}) \quad \text{und} \quad R \in GL(n; \mathbb{R})$$

wie oben beschrieben, so kann man $(*)$ in der Form

$${}^t(QR)(QR)x^* = {}^t(QR)b, \quad \text{d.h.} \quad {}^tR^t(QQ)Rx^* = {}^tR^tQb$$

schreiben. Da ${}^tQQ = E_n$ und ${}^tR \in GL(n; \mathbb{R})$ wird daraus die zu $(*)$ äquivalente Bedingung

$$Rx^* = {}^tQb. \quad (**)$$

Sind Q und R aus A berechnet, kann man $(**)$ von unten nach oben lösen.

Zum Vergleich der Elimination von GAUSS und der QR-Methode geben wir ein ganz einfaches

Beispiel 2 Sei

$$(A, b) = \left(\begin{array}{cc|c} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 2 & 0 & 1 \end{array} \right).$$

Auf Zeilenstufenform gebracht erhält man

$$(\tilde{A}, \tilde{b}) = \left(\begin{array}{cc|c} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{array} \right),$$

also ist $\text{Lös}(A, b) = \emptyset$. Nun berechnet man

$$({}^tAA, {}^tAb) = \left(\begin{array}{cc|c} 5 & 1 & 4 \\ 1 & 2 & 3 \end{array} \right) =: (A^*, b^*).$$

Das Ergebnis der Elimination ist

$$(\tilde{A}^*, \tilde{b}^*) = \left(\begin{array}{cc|c} 5 & 1 & 4 \\ 0 & 9 & 11 \end{array} \right),$$

das ergibt die Lösung $x^* = {}^t(\frac{47}{45}, -\frac{11}{9})$.

Für die QR-Zerlegung von A erhält man mit etwas Rechnung und mit Hilfe von obigen Beispiel 1

$$Q = \frac{1}{15} \sqrt{5} \begin{pmatrix} 3 & 4 \\ 0 & 5 \\ 6 & -2 \end{pmatrix} \quad \text{und} \quad R = \frac{1}{15} \sqrt{5} \begin{pmatrix} 15 & 3 \\ 0 & 9 \end{pmatrix}.$$

Dann ist ${}^tQb = \frac{1}{15} \sqrt{5} \cdot {}^t(12, 11)$ und das System $Rx^* = {}^tQb$ ist äquivalent zu

$$\begin{pmatrix} 15 & 3 \\ 0 & 9 \end{pmatrix} \begin{pmatrix} x_1^* \\ x_2^* \end{pmatrix} = \begin{pmatrix} 12 \\ 11 \end{pmatrix},$$

die eindeutige Lösung ist wieder $x^* = {}^t(\frac{47}{45}, -\frac{11}{9})$.

Die beiden Methoden sind also im Prinzip gleichwertig, aber bei der direkten Elimination werden keine Quadratwurzeln benötigt. Die QR-Methode hat dagegen numerische Vorteile und ist bei anderen Problemen höchst nützlich, etwa bei einem Iterationsverfahren zur Berechnung der Eigenwerte (vgl. etwa [STR]).

5.3.5 Orthogonale und unitäre Endomorphismen

In Kapitel 4 hatten wir gesehen, dass es für die Diagonalisierung eines Endomorphismus mehrere Hindernisse gibt. In den folgenden Abschnitten werden wir sehen, wie viel besser das alles geht, wenn man geeignete Voraussetzungen über das Verhältnis des Endomorphismus zu Skalarprodukten macht. Bei den Beweisen wird sich zeigen, wie vorteilhaft es für den reellen Fall ist, den komplexen Fall daneben mitlaufen zu lassen. Zur Abkürzung schreiben wir \mathbb{K} für \mathbb{R} oder \mathbb{C} .

Sei also V ein euklidischer bzw. unitärer Vektorraum mit Skalarprodukt $\langle \cdot, \cdot \rangle$. Wie meistens zuvor setzen wir generell $\dim V < \infty$ voraus.

Ein Endomorphismus $F : V \rightarrow V$ heißt **orthogonal** (im Fall $\mathbb{K} = \mathbb{R}$) bzw. **unitär** (im Fall $\mathbb{K} = \mathbb{C}$), wenn

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

Kurz ausgedrückt: F respektiert das Skalarprodukt.

Im einfachsten Fall des Standardraums \mathbb{K}^n wird F beschrieben durch eine Matrix $A \in M(n \times n; \mathbb{K})$. Dann ist F genau dann orthogonal bzw. unitär, wenn

$$\langle A \cdot x, A \cdot y \rangle = \langle x, y \rangle \quad \text{für alle } x, y \in \mathbb{K}^n. \quad (*)$$

Da $\langle A \cdot x, A \cdot y \rangle = {}^t(A \cdot x) \cdot \overline{(A \cdot y)} = {}^t x \cdot ({}^t A \cdot \overline{A}) \cdot \overline{y}$ und $\langle x, y \rangle = {}^t x \cdot \overline{y}$, folgt durch Einsetzen von $x = e_i$ und $y = e_j$, dass Bedingung (*) äquivalent ist zu

$${}^t A \cdot \overline{A} = E_n, \quad \text{d.h.} \quad A^{-1} = {}^t \overline{A}.$$

Dem entsprechend heißt eine Matrix

$$\begin{aligned} A \in M(n \times n; \mathbb{R}) \text{ \textit{orthogonal}} & \quad :\Leftrightarrow \quad A^{-1} = {}^t A \quad \text{und} \\ A \in M(n \times n; \mathbb{C}) \text{ \textit{unitär}} & \quad :\Leftrightarrow \quad A^{-1} = {}^t \overline{A}. \end{aligned}$$

Nach den Regeln für die Matrizenmultiplikation bedeutet das in beiden Fällen, dass sowohl die Zeilenvektoren als auch die Spaltenvektoren von A eine Orthonormalbasis des \mathbb{K}^n bilden.

Wichtige Beispiele sind im reellen Fall die schon in 4.1.2 untersuchten Matrizen

$$A_\alpha = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \quad \text{und} \quad B_\alpha = \begin{pmatrix} \cos \alpha & \sin \alpha \\ \sin \alpha & -\cos \alpha \end{pmatrix}.$$

A_α beschreibt eine Drehung des \mathbb{R}^2 um den Winkel α , B_α ist eine Spiegelung. Eine einfache Rechnung zeigt

$${}^t A_\alpha \cdot A_\alpha = {}^t B_\alpha \cdot B_\alpha = E_2 \quad \text{für alle } \alpha \in \mathbb{R}.$$

Also sind A_α und B_α für alle $\alpha \in \mathbb{R}$ orthogonal. Ein wesentlicher geometrischer Unterschied wird durch die Determinante erkannt:

$$\det A_\alpha = +1 \quad \text{und} \quad \det B_\alpha = -1 \quad \text{für alle } \alpha \in \mathbb{R}.$$

Die Orientierung wird bei A_α erhalten, bei B_α umgekehrt.

Zunächst einige einfache Folgerungen aus der Definition:

Bemerkung Ist $F : V \rightarrow V$ orthogonal bzw. unitär, so folgt:

- a) $\|F(v)\| = \|v\|$ für alle $v \in V$.
- b) Aus $v \perp w$ folgt $F(v) \perp F(w)$.
- c) F ist Isomorphismus, und F^{-1} ist orthogonal bzw. unitär.
- d) Ist auch $G : V \rightarrow V$ orthogonal bzw. unitär, so ist $F \circ G$ orthogonal bzw. unitär.

Vorsicht! Die Bezeichnung „orthogonal“ für einen Endomorphismus ist üblich, aber nicht ungefährlich. Eigenschaft b) folgt daraus, aber nicht umgekehrt. Setzt man etwa $F(v) = \varrho \cdot v$ mit $\varrho \neq 0$, so ist Eigenschaft b) erfüllt, aber für $|\varrho| \neq 1$ ist F nicht orthogonal. Dagegen kann man mit Hilfe der Polarisierung aus 5.2.1 zeigen, dass Eigenschaft a) äquivalent zur Orthogonalität ist.

Für Matrizen ergibt die obige Bemerkung, dass die Teilmengen

$$\begin{aligned} O(n) &:= \{A \in GL(n; \mathbb{R}) : A^{-1} = {}^t A\} \subset GL(n; \mathbb{R}) \quad \text{und} \\ U(n) &:= \{A \in GL(n; \mathbb{C}) : A^{-1} = \overline{{}^t A}\} \subset GL(n; \mathbb{C}) \end{aligned}$$

Untergruppen sind. $O(n)$ heißt *orthogonale Gruppe*, $U(n)$ heißt *unitäre Gruppe*. Für $A \in O(n)$ oder $A \in U(n)$ ist

$$|\det A|^2 = (\det A) \cdot (\overline{\det A}) = (\det A) \cdot (\det {}^t \overline{A}) = \det(A \cdot {}^t \overline{A}) = \det E_n = 1,$$

also folgt $|\det A| = 1$. Die Untergruppe

$$SO(n) := \{A \in O(n) : \det A = +1\} \subset O(n)$$

heißt *spezielle orthogonale Gruppe*. Zu ihr gehören die Endomorphismen des \mathbb{R}^n , die orientierungstreu sind.

Nun kommen wir zum entscheidenden Punkt, den Eigenwerten:

Lemma 1 Sei $F : V \rightarrow V$ orthogonal bzw. unitär.

- a) Ist $\lambda \in \mathbb{K}$ Eigenwert von F , so gilt $|\lambda| = 1$.
- b) Eigenvektoren zu verschiedenen Eigenwerten sind orthogonal.

Beweis a) Ist $v \in V$ Eigenvektor zu λ , so gilt

$$\|v\| = \|F(v)\| = \|\lambda \cdot v\| = |\lambda| \cdot \|v\|, \quad \text{also } |\lambda| = 1.$$

b) Sind $v, w \in V$ Eigenvektoren zu λ, μ , so gilt

$$\langle v, w \rangle = \langle F(v), F(w) \rangle = \langle \lambda \cdot v, \mu \cdot w \rangle = \lambda \bar{\mu} \cdot \langle v, w \rangle.$$

Ist $\langle v, w \rangle \neq 0$, so folgt $\lambda \bar{\mu} = 1$. Wegen $|\mu| = 1$ ist $\bar{\mu} = \mu^{-1}$, also muss $\lambda = \mu$ sein. ■

Bei der Frage der Diagonalisierbarkeit muss man nun den reellen und den komplexen Fall unterscheiden, der komplexe ist einfacher.

Theorem Ist V ein unitärer Vektorraum und $F: V \rightarrow V$ ein unitärer Endomorphismus, so gibt es eine Orthonormalbasis \mathcal{B} von V , bestehend aus Eigenvektoren von F . Insbesondere ist

$$M_{\mathcal{B}}(F) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \quad \text{mit } \lambda_i \in \mathbb{C} \quad \text{und } |\lambda_i| = 1.$$

Übertragen auf Matrizen erhält man als

Korollar 1 Ist $A \in U(n)$ eine unitäre Matrix, so gibt es dazu ein $S \in U(n)$ derart, dass

$${}^t \bar{S} \cdot A \cdot S = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \quad \text{mit } \lambda_1, \dots, \lambda_n \in \mathbb{C}$$

und $|\lambda_i| = 1$ für $i = 1, \dots, n$.

Man beachte dabei, dass ${}^t \bar{S} = S^{-1}$.

Beweis des Theorems Entscheidend ist zunächst, dass im komplexen Fall das charakteristische Polynom P_F in Linearfaktoren zerfällt, also

$$P_F = \pm (X - \lambda_1) \cdot \dots \cdot (X - \lambda_n) \quad \text{mit } \lambda_i \in \mathbb{C} \quad \text{und } |\lambda_i| = 1.$$

Für den Beweis spielt die Vielfachheit der Eigenwerte keine Rolle, denn wir können Induktion über $n = \dim V$ führen. Der Fall $n = 1$ ist klar, sei also $n > 1$.

Zu λ_1 wählen wir einen Eigenvektor v_1 mit $\|v_1\| = 1$. Dazu betrachten wir das orthogonale Komplement

$$W := \{w \in V : \langle w, v_1 \rangle = 0\} \subset V.$$

Entscheidend für die Induktion ist nun, dass W F -invariant ist, d.h. $F(W) \subset W$. Für $w \in W$ ist

$$0 = \langle w, v_1 \rangle = \langle F(w), F(v_1) \rangle = \langle F(w), \lambda_1 v_1 \rangle = \overline{\lambda_1} \cdot \langle F(w), v_1 \rangle.$$

Da $\lambda_1 \neq 0$ folgt $\langle F(w), v_1 \rangle = 0$, also $F(w) \in W$. Nun betrachten wir die Beschränkung

$$G := F|_W : W \rightarrow W.$$

G ist wieder unitär, und wegen $\dim W = n - 1$ können wir die Induktionsannahme auf G anwenden: Es gibt eine Orthonormalbasis (v_2, \dots, v_n) von W bestehend aus Eigenvektoren von G . Da $V = \mathbb{C} \cdot v_1 \oplus W$, folgt

$$P_G = \pm (X - \lambda_2) \cdot \dots \cdot (X - \lambda_n),$$

also sind v_2, \dots, v_n auch Eigenvektoren von F zu den Eigenwerten $\lambda_2, \dots, \lambda_n$. Insgesamt ist

$$\mathcal{B} := (v_1, v_2, \dots, v_n)$$

eine Orthonormalbasis von V bestehend aus Eigenvektoren von F . ■

Das ging erfreulich glatt. Aber nun ist die Frage zu klären, was im reellen Fall gilt; genauer gesagt, was aus dem komplexen Fall gefolgert werden kann. Die Situation ist ganz analog zum Fundamentalsatz der Algebra: Wie in 1.4.6 erhält man aus den komplexen Nullstellen eines reellen Polynoms reelle Teiler vom Grad 2. Zunächst betrachten wir den entscheidenden Fall $n = 2$.

Lemma 2 Sei $A \in \mathbb{O}(2)$. Dann gibt es ein $\alpha \in [0, 2\pi[$ derart, dass

$$A = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \quad \text{oder} \quad A = \begin{pmatrix} \cos \alpha & \sin \alpha \\ \sin \alpha & -\cos \alpha \end{pmatrix}.$$

Der erste Fall tritt ein, wenn $A \in \text{SO}(2)$, d.h. $\det A = +1$, der zweite, wenn $A \notin \text{SO}(2)$, d.h. $\det A = -1$.

Beweis Ist

$$A := \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathbb{O}(2),$$

so seien $v := {}^t(a, b)$ und $w := {}^t(c, d)$ die Spaltenvektoren von A . Da A orthogonal ist, folgt

$$\|v\| = \|w\| = 1 \quad \text{und} \quad v \perp w.$$

Aus $\|v\|^2 = a^2 + b^2 = 1$ folgt, dass es genau einen Winkel $\alpha \in [0, 2\pi[$ gibt derart, dass

$$a = \cos \alpha \quad \text{und} \quad b = \sin \alpha.$$

Aus $v \perp w$ folgt nach der Bemerkung aus 0.3.3, dass $w = \lambda \cdot {}^t(-b, a)$, und aus $\|w\| = 1$ folgt $\lambda = \pm 1$. Also ist

$$A = A_\alpha = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \quad \text{oder} \quad A = B_\alpha = \begin{pmatrix} \cos \alpha & \sin \alpha \\ \sin \alpha & -\cos \alpha \end{pmatrix}.$$

Das sind die beiden schon in 4.1.2 untersuchten Matrizen: Die Drehung A_α hat nur für $\alpha = 0$ oder $\alpha = \pi$ reelle Eigenwerte, B_α ist eine für jeden Winkel α diagonalisierbare Spiegelung mit den Eigenwerten $+1$ und -1 . ■

Man kann nun zeigen, dass die Matrizen $A_\alpha \in O(2)$ innerhalb von $O(n)$ den „worst case“ darstellen:

Lemma 3 Sei V ein euklidischer Vektorraum, $F : V \rightarrow V$ orthogonal und P_F das charakteristische Polynom. Ist $\lambda \in \mathbb{C}$ eine nicht-reelle Nullstelle von P_F , so gibt es dazu einen 2-dimensionalen F -invarianten Unterraum $W \subset V$ derart, dass

$$P_{F|_W} = (X - \lambda) \cdot (X - \bar{\lambda}) \in \mathbb{R}[X].$$

Beweis Wir wählen irgend eine Orthonormalbasis $\mathcal{B} = (v_1, \dots, v_n)$ von V . Dann ist

$$A := M_{\mathcal{B}}(F) \in O(n) \subset U(n),$$

und wir erhalten ein kommutatives Diagramm von orthogonalen Endomorphismen

$$\begin{array}{ccc} \mathbb{R}^n & \xrightarrow{A} & \mathbb{R}^n \\ \Phi_{\mathcal{B}} \downarrow & & \downarrow \Phi_{\mathcal{B}} \\ V & \xrightarrow{F} & V, \end{array}$$

wobei $\Phi_{\mathcal{B}}(e_i) = v_i$. Nun können wir den oberen Teil des Diagramms ganz einfach „komplexifizieren“: Die orthogonale und damit auch unitäre Matrix A definiert eine unitäre Abbildung

$$A : \mathbb{C}^n \rightarrow \mathbb{C}^n, z = {}^t(z_1, \dots, z_n) \mapsto A \cdot z.$$

Zu $\lambda \in \mathbb{C}$ gibt es einen nicht-reellen Eigenvektor $z \in \mathbb{C}^n$, also ist $A \cdot z = \lambda \cdot z$. Da $P_F \in \mathbb{R}[X]$, ist nach 1.4.6 auch $\bar{\lambda}$ Nullstelle von P_F , also Eigenwert, und \bar{z} ist Eigenvektor von A zu $\bar{\lambda}$, denn

$$A \cdot \bar{z} = \bar{A} \cdot \bar{z} = \overline{A \cdot z} = \overline{\lambda \cdot z} = \bar{\lambda} \cdot \bar{z}.$$

Aus z und \bar{z} erhält man die beiden reellen Vektoren

$$x := \operatorname{rez} = \frac{1}{2} \cdot (z + \bar{z}) \quad \text{und} \quad y := \operatorname{imz} = \frac{1}{2i} \cdot (z - \bar{z}).$$

Beweis Wir zerlegen das charakteristische Polynom $P_F \in \mathbb{R}[X]$ entsprechend dem Fundamentalsatz der Algebra in der reellen Form (vgl. 1.4.6):

$$P_F = \pm(X - \mu_1) \cdot \dots \cdot (X - \mu_m) \cdot (X - \lambda_1) \cdot (X - \overline{\lambda_1}) \cdot \dots \cdot (X - \lambda_k) \cdot (X - \overline{\lambda_k}),$$

wobei $\mu_1, \dots, \mu_m \in \mathbb{R}$ und $\lambda_1, \dots, \lambda_k \in \mathbb{C} \setminus \mathbb{R}$. Da F orthogonal ist, folgt $\mu_i = \pm 1$ und $|\lambda_i| = 1$. Aus der Zerlegung von P_F kann man schrittweise eine Zerlegung

$$V = V_1 \oplus \dots \oplus V_m \oplus W_1 \oplus \dots \oplus W_k$$

in eine orthogonale Summe konstruieren. Man beginnt mit einem normierten Eigenvektor v_1 zu μ_1 , setzt

$$V_1 = \mathbb{R} \cdot v_1 \quad \text{und erhält} \quad V = V_1 \oplus V_1^\perp.$$

Entscheidend ist nun, dass V_1^\perp unter F invariant ist. Ist $v \in V_1$ und $w \in V_1^\perp$, so ist zunächst auch $F^{-1}(v) \in V_1$, also folgt

$$\langle v, F(w) \rangle = \langle F^{-1}(v), w \rangle = 0,$$

denn F ist orthogonal. Setzt man dieses Verfahren fort, so erhält man nach der ersten Etappe eine Zerlegung

$$V = V_1 \oplus \dots \oplus V_m \oplus W,$$

wobei $V_i = \mathbb{R} \cdot v_i$ und v_i normierte Eigenvektoren zu $\mu_i = \pm 1$ sind. Zu λ_1 und $\overline{\lambda_1}$ gehört nach Lemma 2 ein 2-dimensionaler Untervektorraum W_1 mit $F(W_1) \subset W_1$. Daraus erhält man eine Zerlegung von V in F -invariante Untervektorräume

$$(V_1 \oplus \dots \oplus V_m \oplus W_1) \oplus W',$$

wobei $P_{F|_{W'}} = (X - \lambda_2) \cdot (X - \overline{\lambda_2}) \cdot \dots \cdot (X - \lambda_k) \cdot (X - \overline{\lambda_k})$. Indem man W' weiter zerlegt, erhält man das gewünschte Ergebnis. ■

5.3.6 Die Gruppe $SO(3)^*$

Eine Matrix $A \in SO(3)$ beschreibt eine lineare Abbildung

$$F_A : \mathbb{R}^3 \rightarrow \mathbb{R}^3, \quad x \mapsto A \cdot x,$$

die Längen, Winkel und Orientierung erhält. Wegen der vielen Anwendungsmöglichkeiten wollen wir diesen Spezialfall orthogonaler Matrizen etwas ausführlicher beschreiben. Zunächst ein Ergebnis, das nicht nur auf den ersten Blick verwunderlich erscheint.

Satz 1 Zu jeder Matrix $A \in SO(3)$ gibt es eine Matrix $S \in SO(3)$ und einen Winkel $\alpha \in [0, 2\pi[$ derart, dass

$${}^t S \cdot A \cdot S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \alpha & -\sin \alpha \\ 0 & \sin \alpha & \cos \alpha \end{pmatrix}$$

Ist $\mu_1 = -1$, so muss auch $\det A_1 = -1$ sein, und man kann v_2, v_3 nach 4.1.2 so wählen, dass

$$M_{\mathcal{B}}(F_A) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & +1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Ist dann $\mathcal{B}' := (v_2, v_1, v_3)$, so folgt

$$M_{\mathcal{B}'}(F_A) = \begin{pmatrix} +1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

also ist in diesem Fall $\alpha = \pi$. ■

Nun noch ein paar Erläuterungen zur Gruppe $SO(3)$. Zunächst ist ganz einfach zu sehen, dass $SO(3)$ nicht abelsch ist. Etwa für

$$A := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{und} \quad B := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

ist $B \cdot A \neq A \cdot B$.

Da $SO(3) \subset M(3 \times 3; \mathbb{R}) \cong \mathbb{R}^9$ ist es eine spannende Frage, die Struktur dieser Teilmenge zu untersuchen. Sie ist offensichtlich kein Untervektorraum, dafür aber eine so genannte „Untermannigfaltigkeit der Dimension 3“. Das findet man zum Beispiel bei [BRÖ, Kap. IX, §1] beschrieben. Die Zahl 3 ist dabei die Anzahl der Parameter, von denen eine Matrix $A \in SO(3)$ abhängt: Zwei für die Drehachse, die durch einen Punkt auf der Sphäre

$$Q := \{v \in \mathbb{R}^3 : \|v\| = 1\}$$

bestimmt ist, und einen für den Drehwinkel um diese Achse.

Drei andersartige Parameter für $SO(3)$ sind die „EULERSchen Winkel“. Um sie zu erklären, benutzen wir die für jedes $t \in \mathbb{R}$ erklärten speziellen Matrizen

$$A_t := \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos t & -\sin t \\ 0 & \sin t & \cos t \end{pmatrix} \quad \text{und} \quad B_t := \begin{pmatrix} \cos t & -\sin t & 0 \\ \sin t & \cos t & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

A_t bzw. B_t beschreibt eine Drehung um den Winkel t mit der Achse x_1 bzw. x_3 . Offensichtlich gilt $A_t, B_t \in SO(3)$ für alle $t \in \mathbb{R}$, also auch

$$B_\alpha \cdot A_\beta \cdot B_\gamma \in SO(3) \quad \text{für alle} \quad \alpha, \beta, \gamma \in \mathbb{R}.$$

Wir zeigen nun folgenden

Satz 1 Die Abbildung

$$\Phi : [0, 2\pi[\times [0, \pi] \times [0, 2\pi[\rightarrow \text{SO}(3), (\alpha, \beta, \gamma) \mapsto B_\alpha \cdot A_\beta \cdot B_\gamma,$$

ist surjektiv.

Anders ausgedrückt: Jeder spezielle orthogonale Automorphismus des \mathbb{R}^3 lässt sich darstellen als Hintereinanderschaltung von drei sehr einfach zu beschreibenden Drehungen. Ist

$$A = \Phi(\alpha, \beta, \gamma) \in \text{SO}(3),$$

so heißen α, β, γ EULERSche Winkel zu A .

Es gibt viele Varianten davon und zahlreiche Anwendungen, zum Beispiel in der Luftfahrt zur Beschreibung der Lage eines Flugzeuges.

Beweis Es ist hilfreich, neben den Matrizen $A = (a_{ij})$, A_t und B_t auch zugehörige Automorphismen des \mathbb{R}^3 zu betrachten. Daher wählen wir zur Bestimmung der Winkel α, β, γ ein geometrisches Verfahren. Sei also F der zu A gehörende Automorphismus des \mathbb{R}^3 . Bezeichnet $\mathcal{B} = (e_1, e_2, e_3)$ die kanonische Basis von \mathbb{R}^3 , so ist in der Notation von 2.4.2

$$A = M_{\mathcal{B}}(F).$$

Zur Bestimmung des ersten Winkels α benutzen wir den Vektor $v := {}^t(a_{13}, a_{23}, 0) \in \mathbb{R}^3$, das ist die Projektion von $F(e_3)$ auf die Ebene $\mathbb{R} \cdot e_1 + \mathbb{R} \cdot e_2$.

Im Fall $v = \mathbf{o}$ ist $F(e_3) = \pm e_3$. Ist $F(e_3) = e_3$, so gibt es ein $\alpha \in [0, 2\pi[$ derart, dass $A = B_\alpha$ und man kann $\beta = \gamma = 0$ wählen. Falls $F(e_3) = -e_3$, gibt es ein $\alpha \in [0, 2\pi[$ derart, dass

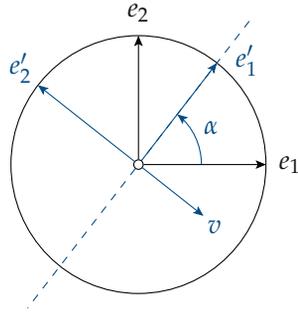
$$A = \begin{pmatrix} \cos \alpha & \sin \alpha & 0 \\ \sin \alpha & -\cos \alpha & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

also ist $A = B_\alpha \cdot A_\pi$ und $\gamma = 0$. Die geometrische Interpretation dieser Zerlegung überlassen wir dem Leser.

Im Fall $v \neq \mathbf{o}$ betrachten wir den zu v senkrechten normierten Vektor

$$e'_1 := \frac{1}{\varrho} {}^t(-a_{23}, a_{13}, 0) \quad \text{mit} \quad \varrho := \sqrt{a_{13}^2 + a_{23}^2}.$$

Die Gerade $\mathbb{R} \cdot e'_1$ ist die Schnittgerade der Ebenen $F(\mathbb{R} \cdot e_1 + \mathbb{R} \cdot e_2)$ und $\mathbb{R} \cdot e_1 + \mathbb{R} \cdot e_2$. Nun erklären wir G_α als Drehung um den Winkel α , wobei $G_\alpha(e_3) = e_3$, $G_\alpha(e_1) = e'_1$, also $\cos \alpha = \frac{-a_{23}}{\varrho}$ und $\sin \alpha = \frac{a_{13}}{\varrho}$.



Als darstellende Matrix erhalten wir

$$M_{\mathcal{B}}(G_\alpha) = B_\alpha.$$

Im zweiten Schritt wird e'_1 festgehalten und e_3 nach $F(e_3)$ gedreht. Das ergibt eine Abbildung F_β mit

$$F_\beta(e'_1) = e'_1, F_\beta(e_3) = F(e_3), \text{ also } \cos \beta = a_{33} \text{ und } \sin \beta = \varrho.$$

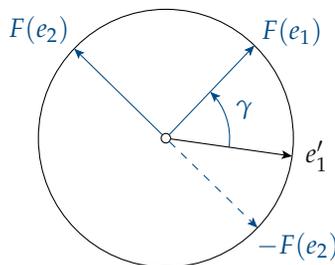
Da $\sin \beta \geq 0$, ist $\beta \in [0, \pi]$. Bezüglich der Basis $\mathcal{B}' = (e'_1, e'_2, e_3)$ mit $e'_2 = G_\alpha(e_2)$ erhalten wir die darstellende Matrix

$$M_{\mathcal{B}'}(F_\beta) = A_\beta.$$

Da F orthogonal ist, liegt $F(e_1)$ in der zu $F(e_3)$ senkrechten Ebene. Also kann man $F(e_3)$ festhalten und e'_1 nach $F(e_1)$ drehen. Das ergibt eine Abbildung G_γ mit

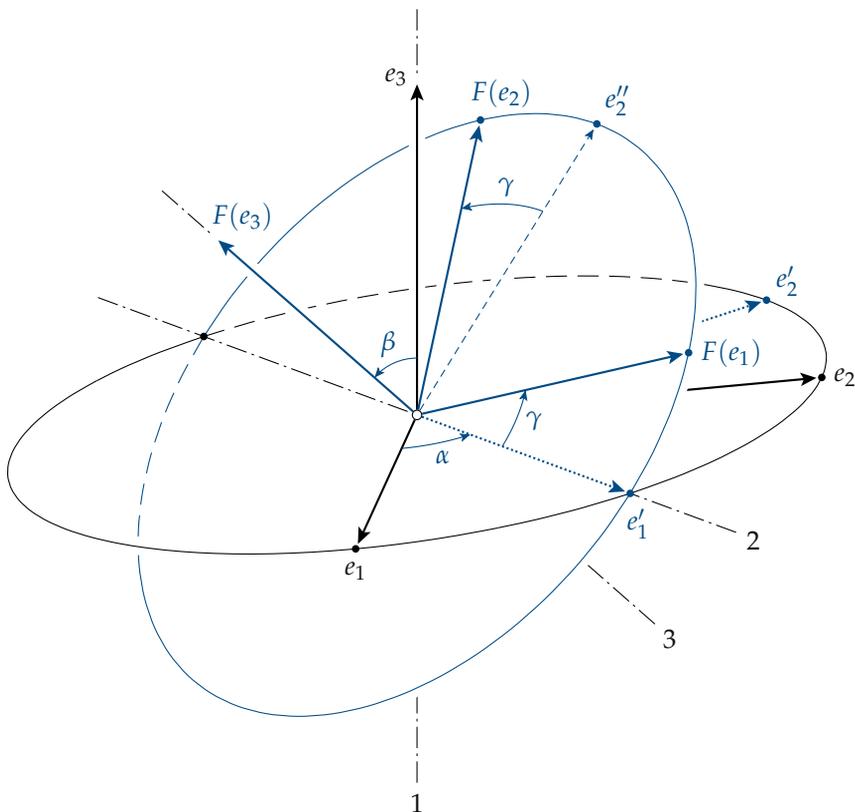
$$\begin{aligned} G_\gamma(F(e_3)) &= F(e_3), G_\gamma(e'_1) = F(e_1), \text{ also} \\ \cos \gamma &= \langle F(e_1), e'_1 \rangle = \frac{1}{\varrho} (a_{21}a_{13} - a_{11}a_{23}) = \frac{a_{32}}{\varrho} \text{ und} \\ \sin \gamma &= \langle -F(e_2), e'_1 \rangle = \frac{1}{\varrho} (a_{12}a_{23} - a_{22}a_{13}) = \frac{a_{31}}{\varrho}. \end{aligned}$$

Die verschiedenen Darstellungen von $\cos \gamma$ und $\sin \gamma$ folgen aus der speziellen Orthogonalität von A zusammen mit 3.3.1, oder mit Hilfe der Eigenschaften des Vektorprodukts (0.3.7).



Bezüglich der Basis $\mathcal{B}'' = (e'_1, e'_2, e'_3)$ mit $e'_2 := F_\beta(e'_2)$ und $e'_3 = F(e_3)$ erhalten wir die darstellende Matrix

$$M_{\mathcal{B}''}(G_\gamma) = B_\gamma.$$



Es bleiben zwei Aussagen zu beweisen:

$$G_\gamma \circ F_\beta \circ G_\alpha = F \quad \text{und} \quad B_\alpha \cdot A_\beta \cdot B_\gamma = A.$$

Die erste Aussage ist einfach

$$\begin{aligned} G_\gamma(F_\beta(G_\alpha(e_1))) &= G_\gamma(F_\beta(e'_1)) = G_\gamma(e'_1) = F(e_1) \quad \text{und} \\ G_\gamma(F_\beta(G_\alpha(e_3))) &= G_\gamma(F_\beta(e_3)) = G_\gamma(F(e_3)) = F(e_3). \end{aligned}$$

Da F eigentlich orthogonal ist, gilt das auch für e_2 , also für ganz F .

Die zweite Aussage ist tückisch: Es muss erklärt werden, wie die Umkehrung der Reihenfolge zustande kommt. Man kann die Gleichung zwar direkt durch Multiplikation

der drei links stehenden Matrizen nachrechnen, aber das liefert keine besondere Einsicht. Sie ergibt sich daraus, dass die drei darstellenden Matrizen mit Hilfe verschiedener Basen gefunden wurden. Die Umrechnungen geschehen mit Hilfe der Transformationsformel des Korollars aus 2.5.2, mit den Bezeichnungen für Basis- und Koordinatentransformationen aus 2.5.1:

$$B_\alpha = M_B(G_\alpha) = S_{B'}^B, \quad A_\beta = M_{B'}(F_\beta) = S_{B''}^{B'} \quad \text{und} \quad B_\gamma = M_{B''}(G_\gamma).$$

Daraus folgt

$$M_B(F_\beta) = T_{B'}^{B'} \cdot M_{B'}(F_\beta) \cdot T_{B'}^B = S_{B'}^B \cdot A_\beta \cdot S_B^{B'} = B_\alpha \cdot A_\beta \cdot B_{-\alpha}$$

und somit

$$M_B(F_\beta \circ G_\alpha) = M_B(F_\beta) \cdot M_B(G_\alpha) = B_\alpha \cdot A_\beta \cdot B_{-\alpha} \cdot B_\alpha = B_\alpha \cdot A_\beta.$$

Daran sieht man, wie die Umkehrung der Reihenfolge entsteht. Der nächste Schritt verläuft analog: Da

$$T_B^{B''} = T_B^{B'} \cdot T_{B'}^{B''} = S_B^{B'} \cdot S_{B''}^{B'} = B_\alpha \cdot A_\beta \quad \text{und analog} \quad T_{B''}^B = A_{-\beta} \cdot B_{-\alpha},$$

folgt

$$M_B(G_\gamma) = T_{B''}^{B''} \cdot M_{B''}(G_\gamma) \cdot T_{B''}^B = B_\alpha \cdot A_\beta \cdot B_\gamma \cdot A_{-\beta} \cdot B_{-\alpha}.$$

Daraus erhält man das endgültige Ergebnis

$$\begin{aligned} A &= M_B(G_\gamma \circ F_\beta \circ G_\alpha) = M_B(G_\gamma) \cdot M_B(F_\beta \circ G_\alpha) = B_\alpha \cdot A_\beta \cdot B_\gamma \cdot A_{-\beta} \cdot B_{-\alpha} \cdot B_\alpha \cdot A_\beta \\ &= B_\alpha \cdot A_\beta \cdot B_\gamma. \end{aligned}$$

■

Beispiel Wir betrachten die (sorgfältig präparierte) Matrix

$$A := \begin{pmatrix} \frac{1}{4}\sqrt{3} - \frac{1}{8}\sqrt{6} & -\frac{3}{4} - \frac{1}{8}\sqrt{2} & \frac{1}{4}\sqrt{2} \\ \frac{1}{4} + \frac{3}{8}\sqrt{2} & -\frac{1}{4}\sqrt{3} + \frac{1}{8}\sqrt{6} & -\frac{1}{4}\sqrt{6} \\ \frac{1}{4}\sqrt{6} & \frac{1}{4}\sqrt{2} & \frac{1}{2}\sqrt{2} \end{pmatrix} \in SO(3).$$

Hier ist $\varrho = \frac{1}{2}\sqrt{2}$, daraus folgt

$$\begin{aligned} \cos \alpha &= -\frac{a_{23}}{\varrho} = \frac{1}{2}\sqrt{3}, & \sin \alpha &= \frac{a_{13}}{\varrho} = \frac{1}{2}, & \text{also} & \alpha = \frac{\pi}{6} \\ \cos \beta &= a_{33} = \frac{1}{2}\sqrt{2}, & \sin \beta &= \varrho = \frac{1}{2}\sqrt{2}, & \text{also} & \beta = \frac{\pi}{4} \\ \cos \gamma &= \frac{a_{32}}{\varrho} = \frac{1}{2}, & \sin \gamma &= \frac{a_{31}}{\varrho} = \frac{1}{2}\sqrt{3}, & \text{also} & \gamma = \frac{\pi}{3}. \end{aligned}$$

Wie wir gesehen haben, kann die durch A bewirkte Transformation auch durch eine einzige Drehung um eine Achse beschrieben werden. Dazu berechnet man zunächst das charakteristische Polynom

$$P_A = X^3 - \frac{1}{2}\sqrt{2} \cdot X^2 + \frac{1}{2}\sqrt{2} \cdot X - 1 = (X-1)\left(X^2 + \left(1 - \frac{1}{2}\sqrt{2}\right) \cdot X + 1\right).$$

Also gibt es nur einen reellen Eigenwert 1, ein zugehöriger normierter Eigenvektor ist (auf drei Dezimalen gerundet)

$$v := {}^t(0.488, -0.131, 0.863).$$

Um den Drehwinkel φ zu bestimmen, benutzen wir einen zu v senkrechten normierten Vektor, etwa

$$w := {}^t(0.259, 0.966, 0) \quad \text{und} \quad A \cdot w = {}^t(-0.862, 0.080, 0.500);$$

Somit ist $\cos \varphi = \langle w, A \cdot w \rangle = -0.146$ und $\varphi \approx 98^\circ$.

Offensichtlich ist die Bestimmung der Eulerschen Winkel mit weit weniger Rechenaufwand verbunden.

Schon HAMILTON hatte entdeckt, wie man $SO(3)$ mit Hilfe seiner Quaternionen beschreiben kann. Das findet man zum Beispiel bei [BRÖ, Kap. IX] ausgeführt.

5.3.7 Selbstadjungierte Endomorphismen

Die Bedingung aus 5.3.4, dass ein Endomorphismus orthogonal oder unitär ist, war geometrisch sehr einsichtig gewesen. Etwas weniger plausibel ist die folgende

Definition Sei V ein euklidischer bzw. unitärer Vektorraum mit Skalarprodukt $\langle \cdot, \cdot \rangle$. Ein Endomorphismus $F : V \rightarrow V$ heißt **selbstadjungiert**, wenn

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

Ist $A \in M(n \times n; \mathbb{K})$, so ist $A : \mathbb{K}^n \rightarrow \mathbb{K}^n$ als Endomorphismus genau dann selbstadjungiert, wenn

$$\langle A \cdot x, y \rangle = \langle x, A \cdot y \rangle \quad \text{für alle } x, y \in \mathbb{K}^n.$$

Diese Bedingung kann man umformen zu

$${}^t x \cdot {}^t A \cdot \bar{y} = {}^t x \cdot \bar{A} \cdot \bar{y},$$

und indem man $x = e_i$ und $y = e_j$ einsetzt, folgt

$${}^t A = \bar{A}, \quad \text{also} \quad A = {}^t \bar{A}.$$

Das bedeutet im Fall $\mathbb{K} = \mathbb{R}$, dass A symmetrisch ist, und im Fall $\mathbb{K} = \mathbb{C}$, dass A hermitesch ist. Um den Namen „selbstadjungiert“ allgemein zu erklären, sei vermerkt, dass man zu jedem Endomorphismus F eines euklidischen bzw. unitären Vektorraums V einen **adjungierten Endomorphismus** $F^{ad} : V \rightarrow V$ erklären kann durch die Bedingung

$$\langle F(v), w \rangle = \langle v, F^{ad}(w) \rangle \quad \text{für alle } v, w \in V. \quad (*)$$

Um aus dieser Bedingung die Werte von F^{ad} zu berechnen, benutzen wir eine Orthonormalbasis $\mathcal{B} = (v_1, \dots, v_n)$ von V . Gesucht ist die Darstellung

$$F^{ad}(v_j) = \sum_{k=1}^n \alpha_{kj} v_k. \quad \text{Ist} \quad F(v_i) = \sum_{k=1}^n \beta_{ki} v_k,$$

so folgt wegen der Orthogonalität von \mathcal{B}

$$\langle F(v_j), v_j \rangle = \beta_{ji} \quad \text{und} \quad \langle v_i, F^{ad}(v_j) \rangle = \overline{\alpha_{ij}}.$$

Wegen (*) muss $\beta_{ji} = \overline{\alpha_{ij}}$, also $\alpha_{ij} = \overline{\beta_{ji}}$ sein. Für die darstellenden Matrizen bedeutet das

$$M_{\mathcal{B}}(F^{ad}) = \overline{{}^t M_{\mathcal{B}}(F)}.$$

Selbstadjungiert bedeutet also $F^{ad} = F$. Nach diesen Vorbemerkungen zum entscheiden

Lemma Ist $F : V \rightarrow V$ selbstadjungiert, so folgt:

- a) Sowohl im komplexen als auch im reellen Fall ist jeder Eigenwert von F reell.
- b) Sind v, w Eigenvektoren zu verschiedenen Eigenwerten $\lambda \neq \mu$, so folgt $v \perp w$.

Beweis a) Ist v Eigenvektor zu $\lambda \in \mathbb{C}$, so folgt

$$\lambda \cdot \langle v, v \rangle = \langle \lambda \cdot v, v \rangle = \langle F(v), v \rangle = \langle v, F(v) \rangle = \langle v, \lambda \cdot v \rangle = \overline{\lambda} \cdot \langle v, v \rangle.$$

Da $\langle v, v \rangle \neq 0$, folgt $\lambda = \overline{\lambda}$.

$$\text{b) } \lambda \cdot \langle v, w \rangle = \langle \lambda \cdot v, w \rangle = \langle F(v), w \rangle = \langle v, F(w) \rangle = \langle v, \mu \cdot w \rangle = \overline{\mu} \cdot \langle v, w \rangle.$$

Da $\overline{\mu} = \mu \neq \lambda$, folgt $\langle v, w \rangle = 0$. ■

Der sehr einfache Beweis dieses Lemmas zeigt, wie nützlich es ist, dass neben dem reellen auch der komplexe Fall nebenher betrachtet wurde. Bei der Frage der Diagonalisierbarkeit in 5.3.4 musste man diese beiden Fälle unterscheiden; im selbstadjungierten Fall geht alles glatt:

Theorem Ist V ein euklidischer oder unitärer Vektorraum, und $F : V \rightarrow V$ selbstadjungiert, so gibt es eine Orthonormalbasis \mathcal{B} von V bestehend aus Eigenvektoren von F . Insbesondere ist

$$M_{\mathcal{B}}(F) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \quad \text{mit} \quad \lambda_1, \dots, \lambda_n \in \mathbb{R}.$$

Aus den Transformationsformeln in 2.5.2 und 5.2.2 folgt für Matrizen das

Korollar 1 Ist $A \in M(n \times n; \mathbb{R})$ symmetrisch, so gibt es ein $S \in \text{SO}(n)$ derart, dass

$${}^t S \cdot A \cdot S = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \quad \text{mit } \lambda_1, \dots, \lambda_n \in \mathbb{R}.$$

Ist $A \in M(n \times n; \mathbb{C})$ hermitesch, so gibt es ein $S \in \text{U}(n)$ derart, dass

$$\bar{S} \cdot A \cdot S = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \quad \text{mit } \lambda_1, \dots, \lambda_n \in \mathbb{R}.$$

Im reellen Fall erhält man zunächst ein $S \in \text{O}(n)$. Ist $\det S = -1$, so multipliziert man eine Zeile mit -1 . Als Folgerung aus Diagonalisierungs-Kriterium in 5.3.2 und der Vorzeichenregel aus 1.4.5 erhält man das

Korollar 2 Sei $A \in M(n \times n; \mathbb{R})$ symmetrisch und

$$P_A = (-1)^n \cdot (X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0)$$

das charakteristische Polynom von A . Dann sind folgende Bedingungen äquivalent:

- i) A ist negativ definit.
- ii) Alle Nullstellen $\lambda_1, \dots, \lambda_n$ von P_A sind negativ.
- iii) Alle Koeffizienten a_0, a_1, \dots, a_{n-1} von $(-1)^n \cdot P_A$ sind positiv.

Ganz analog dazu ist A genau dann positiv definit, wenn alle Eigenwerte positiv sind, oder die Vorzeichen der Koeffizienten a_i alternieren.

Beweis des Theorems Aus dem Lemma folgt, dass sowohl im reellen als auch im komplexen Fall

$$P_F = \pm (X - \lambda_1) \cdot \dots \cdot (X - \lambda_n) \quad \text{mit } \lambda_1, \dots, \lambda_n \in \mathbb{R}.$$

Nun können wir Induktion über $n = \dim V$ führen. Der Fall $n = 1$ ist klar, sei also $n \geq 2$. Zunächst wählen wir einen normierten Eigenvektor v_1 zu λ_1 , es sei

$$V_1 := \mathbb{K} \cdot v_1 \quad \text{und} \quad W := V_1^\perp = \{w \in V : \langle v_1, w \rangle = 0\}.$$

Offensichtlich ist $F(V_1) \subset V_1$; aber entscheidend ist, dass auch $F(W) \subset W$: Ist $w \in W$, so gilt

$$\langle v_1, F(w) \rangle = \langle F(v_1), w \rangle = \langle \lambda_1 \cdot v_1, w \rangle = \lambda_1 \cdot \langle v_1, w \rangle = 0.$$

Da $V = V_1 \oplus W$, ist $\dim W = n - 1$, also können wir die Induktionsannahme auf W und $F|_W$ anwenden: Es gibt eine Orthonormalbasis (v_2, \dots, v_n) von W , bestehend aus Eigenvektoren von $F|_W$ und damit auch von F . Somit ist

$$\mathcal{B} = (v_1, \dots, v_n)$$

eine Orthonormalbasis von V bestehend aus Eigenvektoren von F . ■

Beispiel Wir wollen noch einmal die symmetrische Matrix

$$A := \begin{pmatrix} 17 & -32 & 29 \\ -32 & 63 & -58 \\ 29 & -58 & 59 \end{pmatrix}$$

aus 5.3.2 betrachten. Für das charakteristische Polynom erhält man

$$P_A = -(X^3 - 139X^2 + 562X - 250).$$

Nach der Vorzeichenregel hat es nur positive Nullstellen, also ist A positiv definit. Die Berechnung der Eigenwerte ergibt

$$\lambda_1 = 0.508\dots, \quad \lambda_2 = 3.645\dots, \quad \lambda_3 = 134.846\dots$$

An dieser Stelle scheint eine Anmerkung zum Vergleich der verschiedenen Definitheitstests angebracht. Den geringsten Rechenaufwand erfordert das Diagonalisierungskriterium aus 5.3.2, dabei werden auch Rang und Positivitäts-Index ablesbar (vgl. 5.2.5). Das Haupt-Minoren-Kriterium erfordert die Berechnung von Determinanten, die bei geeigneter Diagonalisierung auch schon an der diagonalen Matrix ablesbar sind. Es hat etwas theoretische Bedeutung, weil man damit wegen der Stetigkeit der Determinanten sofort sehen kann, dass die Definitheit bei kleinen Störungen der Einträge der Matrix erhalten bleibt.

Am meisten Aufwand bereitet die Berechnung der Eigenwerte, dafür erhält man zusätzlich wichtige quantitative Informationen. Etwa dazu, wie stark eine Funktion mehrerer Veränderlicher von einem relativen Minimum aus in den verschiedenen Richtungen ansteigt (vgl. 5.3.2). Bei der symmetrischen Diagonalisierung bleiben nur die Vorzeichen stabil, nicht die Werte.

Die Existenz reeller Eigenwerte einer symmetrischen reellen Matrix hatten wir in obigem Lemma 1 mit Hilfe komplexer Zahlen bewiesen. Man kann auch einen Beweis mit Hilfe reeller Analysis geben, bei dem Eigenwert und Eigenvektor zusammen gefunden werden, und der auch Grundlage für ein numerisches Rechenverfahren ist.

Lemma 2 Ist $A \in M(n \times n; \mathbb{R})$ symmetrisch, so gibt es mindestens einen reellen Eigenwert λ von A .

Beweis Wir betrachten die zu A gehörige quadratische Form

$$q : \mathbb{R}^n \rightarrow \mathbb{R}, x \mapsto \langle x, A \cdot x \rangle = \sum_{i,j} a_{ij} x_i x_j.$$

Das ist eine stetige Abbildung, also nimmt q auf der kompakten Menge

$$Q := \{x \in \mathbb{R}^n : \|x\| = 1\}$$

ein Maximum und ein Minimum an. Ist $v \in Q$ derart, dass q in v ein Extremum annimmt, so wird behauptet, dass es ein $\lambda \in \mathbb{R}$ gibt derart, dass

$$A \cdot v = \lambda \cdot v,$$

d.h. v ist Eigenvektor zu λ . Dazu betrachtet man das orthogonale Komplement

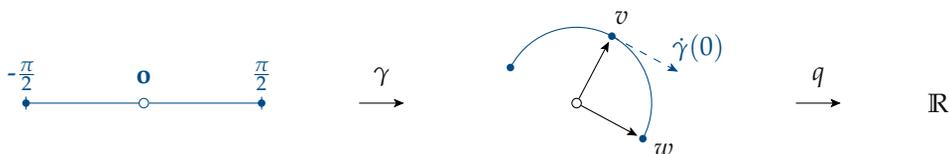
$$W := (\mathbb{R} \cdot v)^\perp.$$

Um zu zeigen, dass $A \cdot v = \lambda \cdot v$, genügt es nachzuweisen, dass für jedes $w \in W$

$$\langle A \cdot v, w \rangle = 0 \quad \text{d.h.} \quad A \cdot v \perp w.$$

Weiter kann man $\|w\| = 1$, also $w \in Q$ annehmen. Um das Problem auf das Extremum einer reellen Funktion von einer Veränderlichen zurückzuführen, benutzen wir den differenzierbaren Weg

$$\gamma : \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \rightarrow Q, \gamma(t) := (\cos t) \cdot v + (\sin t) \cdot w,$$



mit $\gamma(0) = v$ und $\dot{\gamma}(0) = w$. Da q ein Extremum in v hat, ist 0 ein relatives Extremum von $q \circ \gamma$. Also muss

$$\frac{d}{dt}(q \circ \gamma)(0) = 0$$

sein. Diese Ableitung kann man wie folgt berechnen: Zunächst ist

$$\frac{\partial q}{\partial x_i} = 2 \sum_{j=1}^n a_{ij} x_j \quad \text{für } i = 1, \dots, n.$$

Mit $\gamma(t) = (x_1(t), \dots, x_n(t))$ folgt

$$\frac{d}{dt}(q \circ \gamma) = \sum_{i=1}^n \frac{\partial q}{\partial x_i} \cdot \frac{dx_i}{dt} = 2 \sum_{i,j=1}^n a_{ij} x_j \dot{x}_i.$$

Für $t = 0$ erhält man

$$0 = 2 \sum_{i,j} a_{ij} \cdot x_j(0) \dot{x}_i(0) = 2 \langle A \cdot \gamma(0), \dot{\gamma}(0) \rangle = 2 \langle A \cdot v, w \rangle.$$

■

Für den zum Eigenvektor v gehörenden Eigenwert λ kann man daraus nur den Betrag angeben; wegen $\|v\| = 1$ ist

$$|\lambda| = \|A \cdot v\|.$$

Die weiteren Eigenwerte und Eigenvektoren von A findet man iterativ, indem man q zunächst auf $W \cap Q$ beschränkt, u.s.w.

Aus der Analysis kennt man ein Verfahren, die Extrema von q auf Q zu bestimmen [FO₂, §8]. Dabei wird

$$h(x) := \sum_{i=1}^n x_i^2 - 1 = 0$$

als „Nebenbedingung“ bezeichnet. Die LAGRANGE-Bedingung lautet dann

$$(\text{grad } q)(v) = \lambda \cdot (\text{grad } h)(v). \quad (*)$$

Wenn man die Gradienten ausrechnet, erhält man

$$(\text{grad } h)(x) = 2 \cdot x \quad \text{und} \quad (\text{grad } q)(x) = 2 \cdot A \cdot x.$$

Also ist (*) äquivalent zu $A \cdot x = \lambda \cdot x$, das ist die Eigenwert-Bedingung für A . Der **LAGRANGE-Multiplikator** λ ist also gleich dem Eigenwert.

5.3.8 Hauptachsentransformation von Quadriken*

Dieser Abschnitt ist ein kleiner Höhepunkt der elementaren analytischen Geometrie. Wie in 5.2.7 erläutert, sei eine quadratische Gleichung in den Variablen x_1, \dots, x_n vorgegeben. Mit Hilfe von symmetrischen Matrizen kann man das so beschreiben: Zu $A \in M(n \times n; \mathbb{R})$ mit ${}^t A = A$ betrachtet man die erweiterte Matrix

$$A' := \left(\begin{array}{c|ccc} a_{00} & a_{01} & \cdots & a_{0n} \\ \hline a_{01} & & & \\ \vdots & & A & \\ a_{0n} & & & \end{array} \right) \in M((n+1) \times (n+1); \mathbb{R}).$$

Ist $r := \text{rang } A \geq 1$, so hat man eine Quadrik

$$Q := \{x \in \mathbb{R}^n : {}^t x' \cdot A' \cdot x' = 0\} \subset \mathbb{R}^n,$$

und man möchte aus der Matrix A' die geometrischen Eigenschaften von Q berechnen. In 5.2.7 hatten wir gezeigt, wie man durch symmetrische Umformungen von A' eine Affinität $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$ bestimmen kann, so dass $f(Q)$ durch eine Gleichung in Normalform beschrieben wird. Dadurch ist der Typ von Q bestimmt, aber da f weder Längen noch Winkel respektieren muss, werden dadurch die metrischen Eigenschaften von Q nicht entdeckt. Um ein verbessertes Ergebnis formulieren zu können, ist noch einmal ein neuer Name hilfreich.

Definition Eine Affinität

$$f: \mathbb{R}^n \rightarrow \mathbb{R}^n, x \mapsto b + A \cdot x,$$

mit $A \in GL(n; \mathbb{R})$ heißt **Isometrie**, wenn A orthogonal ist, d.h. $A \in O(n)$.

In 0.3.1 hatten wir für Punkte $p, q \in \mathbb{R}^n$ den Abstand

$$d(p, q) := \|q - p\|$$

eingeführt. Der Name Isometrie ist gerechtfertigt durch die einfache

Bemerkung Ist f eine Isometrie des \mathbb{R}^n , so gilt für alle $p, q \in \mathbb{R}^n$

$$d(f(p), f(q)) = d(p, q).$$

Beweis Aus $f(x) = b + A \cdot x$ folgt

$$f(q) - f(p) = b + A \cdot q - b - A \cdot p = A \cdot (q - p), \quad \text{also} \quad \|f(q) - f(p)\| = \|q - p\|.$$

nach Teil a) der Bemerkung aus 5.3.4. ■

Wir erinnern noch einmal an die Bezeichnungen aus 5.2.7. Es ist $r = \text{rang } A$ und $r' = \text{rang } A'$, und nach Voraussetzung ist $1 \leq r \leq r' \leq n + 1$. Weiter ist

$$r' \leq r + 2.$$

Das abschließende Ergebnis ist der Satz über die

Hauptachsentransformation von Quadriken Zu jeder Quadrik

$$Q = \{x \in \mathbb{R}^n : {}^t x' \cdot A' \cdot x' = 0\} \subset \mathbb{R}^n$$

gibt es eine Isometrie $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$ derart, dass $f(Q) \subset \mathbb{R}^n$ durch eine der folgenden Gleichungen beschrieben wird:

$$\frac{y_1^2}{\alpha_1^2} + \dots + \frac{y_k^2}{\alpha_k^2} - \frac{y_{k+1}^2}{\alpha_{k+1}^2} - \dots - \frac{y_r^2}{\alpha_r^2} = \begin{cases} 0 & \text{falls } r' = r, \\ 1 & \text{falls } r' = r + 1, \\ 2y_{r+1} & \text{falls } r' = r + 2. \end{cases} \quad \begin{matrix} (0) \\ (1) \\ (2) \end{matrix}$$

Dabei ist $0 \leq k \leq r$ und $\alpha_i > 0$ für $i = 1, \dots, r$. Die $\alpha_1, \dots, \alpha_r$ sind die Längen der **Hauptachsen** von Q .

Beweis Wir skizzieren ein iteratives Verfahren zur Berechnung einer Matrix S' mit $S' \in \text{GL}(n+1; \mathbb{R})$, die f beschreibt.

Im ersten Schritt wird die Teilmatrix A entsprechend 5.3.5 diagonalisiert, d.h. man berechnet die Eigenwerte $\lambda_1, \dots, \lambda_n$ und dazu orthonormale Eigenvektoren v_1, \dots, v_n . Die Reihenfolge sei so gewählt, dass

$$\lambda_i > 0 \text{ für } i = 1, \dots, k, \quad \lambda_i < 0 \text{ für } i = k+1, \dots, r \quad \text{und} \quad \lambda_i = 0 \text{ für } i = r+1, \dots, n.$$

Ist T_1 die Matrix mit v_1, \dots, v_n als Spalten, so ist $T_1 \in \text{O}(n)$ und

$${}^t T_1 \cdot A \cdot T_1 = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

Durch die Eigenvektoren v_1, \dots, v_n sind schon die Richtungen der Hauptachsen bestimmt, durch $\lambda_1, \dots, \lambda_r$ die Längen, denn aus

$$|\lambda_i| = \frac{1}{\alpha_i^2} \quad \text{folgt} \quad \alpha_i = |\lambda_i|^{-\frac{1}{2}} \quad \text{für } i = 1, \dots, r.$$

Eine lineare Isometrie f_1 des \mathbb{R}^n ist erklärt durch

$$T'_1 := \left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & T_1 & \\ 0 & & & \end{array} \right) \in \text{O}(n+1),$$

eine Gleichung von $f_1(Q)$ ist gegeben durch die symmetrische Matrix

$$A'_1 := {}^t T'_1 \cdot A' \cdot T'_1 := \left(\begin{array}{c|ccc} b_{00} & b_{01} & \cdots & b_{0n} \\ \hline b_{01} & \lambda_1 & & 0 \\ \vdots & & \ddots & \\ b_{0n} & 0 & & \lambda_n \end{array} \right).$$

Im zweiten Schritt werden die Terme b_{00}, \dots, b_{0n} vereinfacht, geometrisch wird die gesuchte affine Isometrie durch eine zusätzliche Translation aus f_1 erhalten. Das kann man rechnerisch durch wiederholte symmetrische Umformungen von A'_1 und parallel entsprechende Spaltenumformungen an T'_1 und den daraus entstandenen Matrizen ausführen. Dabei sind nur solche Umformungen erlaubt, die an der ersten Zeile $(1, 0, \dots, 0)$

der rechts stehenden Transformationsmatrix nichts ändern, und bei denen die Teilmatrix orthogonal bleibt. Schematisch sieht das so aus:

$$\begin{array}{|c|c|} \hline B'_1 & T'_1 \\ \hline \vdots & \vdots \\ \hline B' & T' \\ \hline \end{array},$$

wobei man für B' je nach den Einträgen b_{00}, \dots, b_{0n} eine der folgenden Matrizen erhalten kann:

$$\begin{array}{c} \left(\begin{array}{c|cccc} 0 & 0 & \cdots & 0 \\ 0 & \lambda_1 & & 0 \\ & & \ddots & \\ \vdots & & & \lambda_r \\ & & & 0 \\ & & & \ddots \\ 0 & 0 & & 0 \end{array} \right)_{r'=r}, & \left(\begin{array}{c|cccc} -1 & 0 & \cdots & 0 \\ 0 & \lambda_1 & & 0 \\ & & \ddots & \\ \vdots & & & \lambda_r \\ & & & 0 \\ & & & \ddots \\ 0 & 0 & & 0 \end{array} \right)_{r'=r+1}, \\ \\ \left(\begin{array}{c|cccc} 0 & 0 & \cdots & 0 & -1 \\ 0 & \lambda_1 & & & 0 \\ \vdots & & \ddots & & \\ & & & \lambda_r & \\ -1 & 0 & & & 0 \end{array} \right)_{r'=r+2}. \end{array}$$

Dabei haben wir bei $r' = r + 2$ nur den Fall $r = n - 1$ betrachtet. Ist dann f die durch $S' = (T')^{-1}$ beschriebene Isometrie des \mathbb{R}^n , so wird $f(Q) \subset \mathbb{R}^n$ nach der Transformationsformel aus 5.2.7 beschrieben durch

$$B' = {}^t T' \cdot A' \cdot T'.$$

Man beachte dabei, dass die erweiterten Matrizen S' und T' nicht mehr orthogonal sein müssen. ■

Wir behandeln nun nach diesem Verfahren noch einmal die schon in 5.2.7 auf affine Normalform gebrachten Beispiele einer Parabel und einer Ellipse.

Beispiel 1 Hier war

$$Q := \{(x_1, x_2) \in \mathbb{R}^2 : x_1^2 + 2x_1x_2 + x_2^2 + 2x_2 + 2 = 0\}, \quad \text{also } A' = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Zunächst wird die Matrix $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ auf Hauptachsen transformiert.

$$P_A = X^2 - 2X \quad \text{hat die Nullstellen } \lambda_1 = 2 \quad \text{und} \quad \lambda_2 = 0.$$

Zur Abkürzung setzen wir $\alpha = \frac{1}{2}\sqrt{2}$ mit $\alpha^2 = \frac{1}{2}$. Dann sind zu λ_1 und λ_2 gehörige normierte Eigenvektoren gleich

$$v_1 = {}^t(\alpha, \alpha) \quad \text{und} \quad v_2 = {}^t(\alpha, -\alpha).$$

Daraus erhält man die Transformationsmatrizen

$$T_1 := \begin{pmatrix} \alpha & \alpha \\ \alpha & -\alpha \end{pmatrix} \quad \text{und} \quad T'_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & \alpha \\ 0 & \alpha & -\alpha \end{pmatrix}$$

mit $\det T_1 = \det T'_1 = -1$. Durch v_1 und v_2 sind schon die Richtungen der Hauptachsen der Parabel Q bestimmt. Um den Scheitel p von Q zu finden, muss noch eine passende Translation des \mathbb{R}^2 gefunden werden. Das geschieht wieder durch symmetrische Umformungen der Matrix

$$B'_1 := {}^tT_1 \cdot A' \cdot T'_1$$

mit parallelen Spaltenumformungen an T'_1 . Dabei ist zu beachten, dass die erste Zeile der Transformationsmatrix rechts immer gleich $(1, 0, 0)$ bleiben muss:

B'_1	T'_1	
2 α $-\alpha$	1 0 0	
α 2 0	0 α α	
$-\alpha$ 0 0	0 α $-\alpha$	(1) $-\frac{\alpha}{2} \cdot$ (2)
$\frac{7}{4}$ 0 $-\alpha$	1 0 0	
0 2 0	$-\frac{1}{4}$ α α	
$-\alpha$ 0 0	$-\frac{1}{4}$ α $-\alpha$	(1) $+\frac{7}{4}\alpha \cdot$ (3)
0 0 $-\alpha$	1 0 0	
0 2 0	$\frac{5}{8}$ α α	
$-\alpha$ 0 0	$-\frac{9}{8}$ α $-\alpha$	
B'	T'	

Zur Kontrolle kann man noch einmal nachrechnen, dass $B' = {}^tT' \cdot A' \cdot T'$. Um die gesuchte Isometrie $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ zu erhalten, berechnet man

$$S' := (T')^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{2}\alpha & \alpha & \alpha \\ -\frac{7}{4}\alpha & \alpha & -\alpha \end{pmatrix}.$$

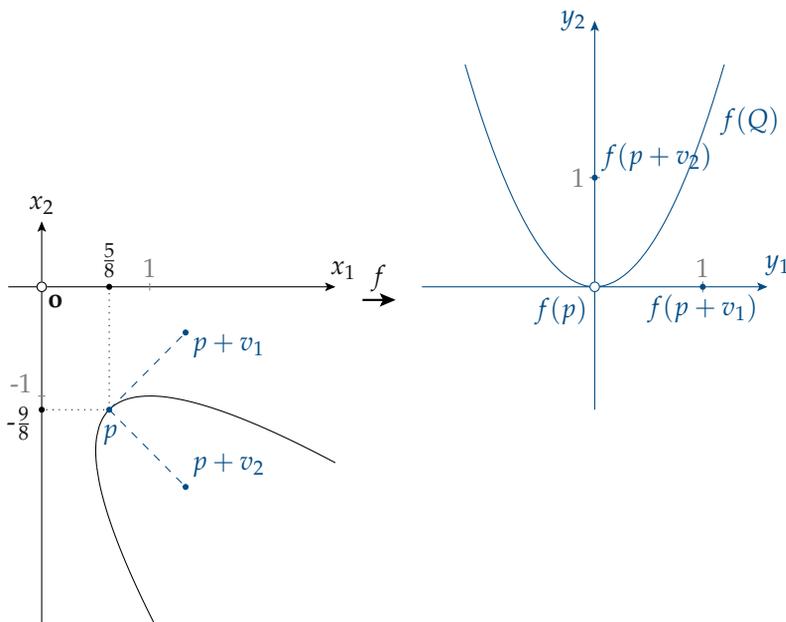
Dann ist ganz explizit

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = f \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \frac{1}{2}\alpha \\ -\frac{7}{4}\alpha \end{pmatrix} + \begin{pmatrix} \alpha(x_1 + x_2) \\ \alpha(x_1 - x_2) \end{pmatrix} \quad \text{und} \\ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = f^{-1} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} \frac{5}{8} \\ -\frac{9}{8} \end{pmatrix} + \begin{pmatrix} \alpha(y_1 + y_2) \\ \alpha(y_1 - y_2) \end{pmatrix}.$$

Die Gleichung von $f(Q)$ ist $2 \cdot y_1^2 = 2\alpha \cdot y_2$; man kann sie durch $\alpha \neq 0$ dividieren, dann ist

$$f(Q) = \{(y_1, y_2) \in \mathbb{R}^2 : \sqrt{2} \cdot y_1^2 = 2 \cdot y_2\}.$$

Den Scheitel p von Q kann man an der ersten Spalte von T' ablesen, es ist $p = (\frac{5}{8}, -\frac{9}{8})$.



Beispiel 2 Bei $Q = \{(x_1, x_2) \in \mathbb{R}^2 : 5x_1^2 - 2x_1x_2 + 2x_2^2 + 8x_1 + 2x_2 + 4 = 0\}$ ist

$$A' = \begin{pmatrix} 4 & 4 & 1 \\ 4 & 5 & -1 \\ 1 & -1 & 2 \end{pmatrix}.$$

Im ersten Schritt bestimmt man Eigenwerte und Eigenvektoren. Wir rechnen dabei mit Dezimalbrüchen, die Ergebnisse sind gerundet auf drei Stellen. Das charakteristische Polynom von A ist $P_A = X^2 - 7X + 9$ mit Nullstellen

$$\lambda_1 = \frac{1}{2}(7 - \sqrt{13}) = 1.697 \quad \text{und} \quad \lambda_2 = \frac{1}{2}(7 + \sqrt{13}) = 5.303$$

wobei $0 < \lambda_1 < \lambda_2$. Eigenvektoren dazu sind

$$v_1 = \begin{pmatrix} -\frac{1}{2}(3 - \sqrt{13}) \\ 1 \end{pmatrix} = \begin{pmatrix} 0.303 \\ 1 \end{pmatrix} \quad \text{und} \quad v_2 = \begin{pmatrix} -\frac{1}{2}(3 + \sqrt{13}) \\ 1 \end{pmatrix} = \begin{pmatrix} -3.303 \\ 1 \end{pmatrix}.$$

Da $v_1 \perp v_2$ und $\|v_1\| = 1.045$, $\|v_2\| = 3.451$, wird daraus die Orthonormalbasis

$$w_1 = \begin{pmatrix} 0.290 \\ 0.957 \end{pmatrix}, \quad w_2 = \begin{pmatrix} -0.957 \\ 0.290 \end{pmatrix}.$$

Als Spalten in T_1 eingetragen erhält man

$$T_1 = \begin{pmatrix} 0.290 & -0.957 \\ 0.957 & 0.290 \end{pmatrix} \quad \text{und} \quad {}^tT_1 \cdot A \cdot T_1 = \begin{pmatrix} 1.697 & 0 \\ 0 & 5.303 \end{pmatrix}.$$

Nun erweitert man die Transformationsmatrix T_1 zu

$$T'_1 = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & & T_1 \\ 0 & & \end{array} \right) \quad \text{und berechnet} \quad B'_1 = {}^tT_1 \cdot A' \cdot T'_1.$$

Damit beginnt die zweite Etappe mit symmetrischen Umformungen von B'_1 , daneben die entsprechenden Spaltenumformungen von T'_1 :

B'_1			T'_1			
4	2.116	-3.539	1	0	0	
2.116	1.697	0	0	0.290	-0.957	
-3.539	0	5.303	0	0.957	0.290	
						(1) + 0.667 · (3)
1.639	2.116	0	1	0	0	
2.116	1.697	0	-0.639	0.290	-0.957	
0	0	5.303	0.193	0.957	0.290	
						(1) - 1.247 · (2)
-1	0	0	1	0	0	
0	1.697	0	-1	0.290	-0.957	
0	0	5.303	-1	0.957	0.290	
B'			T'			

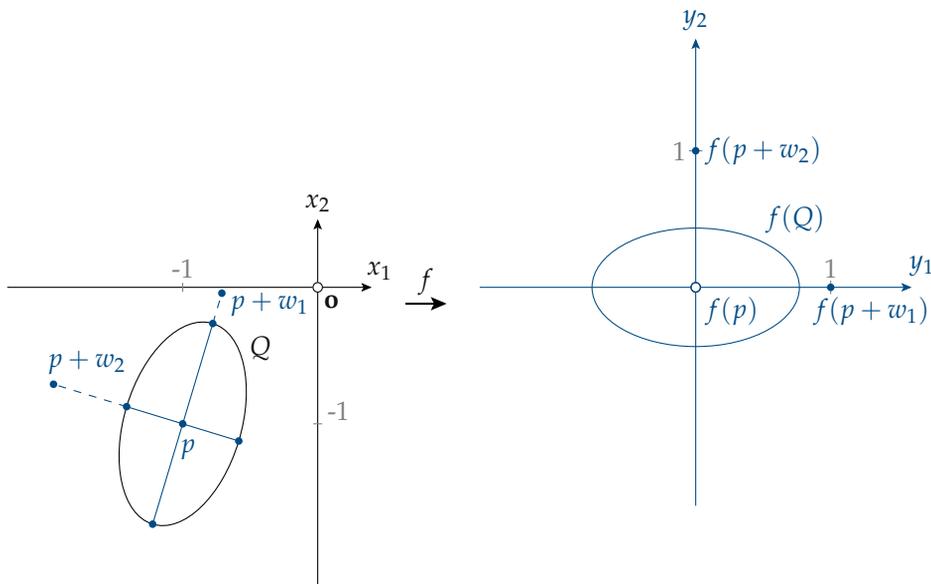
Schließlich kann man T' noch invertieren:

$$S' = (T')^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 1.247 & 0.290 & 0.957 \\ -0.667 & -0.957 & 0.290 \end{pmatrix}.$$

Ist dann die Isometrie $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ beschrieben durch S' , so ist $f(Q)$ beschrieben durch B' , d.h.

$$f(Q) = \{(y_1, y_2) \in \mathbb{R}^2 : \lambda_1 y_1^2 + \lambda_2 y_2^2 - 1 = 0\}.$$

Die Hauptachsen von $f(Q)$ und von Q sind also $a = \lambda_1^{-\frac{1}{2}} = 0.768$ und $b = \lambda_2^{-\frac{1}{2}} = 0.434$. Der Mittelpunkt von $f(Q)$ ist der Ursprung \mathbf{o} , sein Urbild $p = f^{-1}(\mathbf{o})$, das man an der ersten Spalte von T' ablesen kann, ist $(-1, -1)$. Die Richtungen der Hauptachsen von Q sind w_1 und w_2 , man findet sie in den Spalten 2 und 3 von T' .

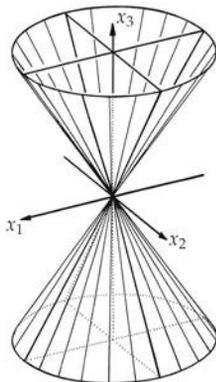


Nachdem wir bisher als Beispiele für Quadriken nur Kegelschnitte im \mathbb{R}^2 betrachtet hatten, sollen zum Schluß noch die typischen Beispiele von Quadriken im \mathbb{R}^3 vorgeführt werden, das sind Flächen. Wir beschränken uns dabei auf den Fall $\text{rang } A' \geq 3$. Die in klassischer Weise von Hand gezeichneten Illustrationen sind aus [F-B] entnommen.

Typ (0) Der einzig interessante Fall ist $k = 2$ und $r = r' = 3$, also lautet die Gleichung

$$\frac{x_1^2}{a_1^2} + \frac{x_2^2}{a_2^2} - \frac{x_3^2}{a_3^2} = 0.$$

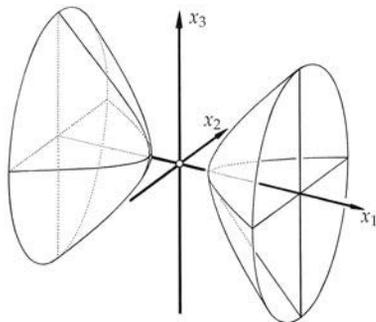
Das ist ein *elliptischer Kegel*, der Schnitt mit jeder Ebene $x_3 = c \neq 0$ ist eine Ellipse.



Typ (1) Für $k = 1$, $r = 3$ und $r' = 4$ lautet die Gleichung

$$\frac{x_1^2}{a_1^2} - \frac{x_2^2}{a_2^2} - \frac{x_3^2}{a_3^2} = 1,$$

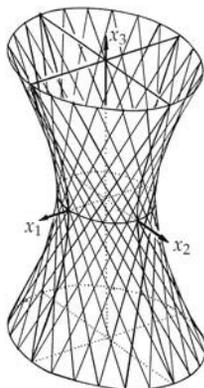
das ist ein *zweischaliges Hyperboloid*.



Für $k = 2$, $r = 3$ und $r' = 4$ lautet die Gleichung

$$\frac{x_1^2}{a_1^2} + \frac{x_2^2}{a_2^2} - \frac{x_3^2}{a_3^2} = 1,$$

das ist ein *einschaliges Hyperboloid*.



Bemerkenswert ist, dass es auf einem einschaligen Hyperboloid Q zwei Scharen von Geraden gibt. Ist etwa $\alpha_1 = \alpha_2 = \alpha_3 = 1$, so sind die beiden Geraden durch $(1,0,0)$ gegeben durch die Parametrisierungen

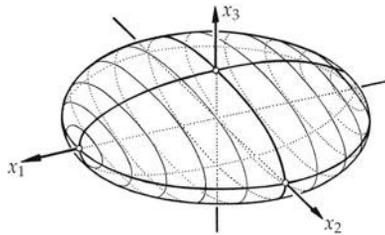
$$\varphi_1 : \mathbb{R} \rightarrow Q, t \mapsto (1, t, t) \quad \text{und} \quad \varphi_2 : \mathbb{R} \rightarrow Q, t \mapsto (1, t, -t).$$

Alle anderen Geraden kann man analog beschreiben.

Für $k = r = 3$ und $r' = 4$ lautet die Gleichung

$$\frac{x_1^2}{a_1^2} + \frac{x_2^2}{a_2^2} + \frac{x_3^2}{a_3^2} = 1,$$

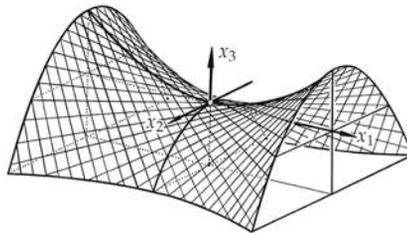
das ist ein **Ellipsoid** mit den Hauptachsen $\alpha_1, \alpha_2, \alpha_3$.



Typ (2) Für $k = 1, r = 2$ und $r' = 4$ lautet die Gleichung

$$\frac{x_1^2}{a_1^2} - \frac{x_2^2}{a_2^2} = 2x_3,$$

diese Quadrik Q ist ein **hyperbolisches Paraboloid** von der Form einer **Sattelfläche**.



Auch hier gibt es zwei Scharen von Geraden. Das kann man ganz einfach nachrechnen, indem man Q durch die affin äquivalente Quadrik

$$Q' := \{(y_1, y_2, y_3) \in \mathbb{R}^3 : y_1 y_2 = y_3\}$$

ersetzt. Dann hat man eine bijektive Abbildung

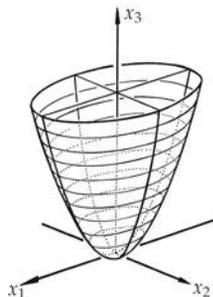
$$\varphi : \mathbb{R}^2 \rightarrow Q', (s, t) \mapsto (s, t, s \cdot t),$$

bei der alle Geraden $s = \text{const.}$ und $t = \text{const.}$ aus \mathbb{R}^2 auf Geraden in Q' abgebildet werden.

Für $k = r = 2$ und $r' = 4$ lautet die Gleichung

$$\frac{x_1^2}{a_1^2} + \frac{x_2^2}{a_2^2} = 2x_3,$$

das ist ein *elliptisches Paraboloid*.



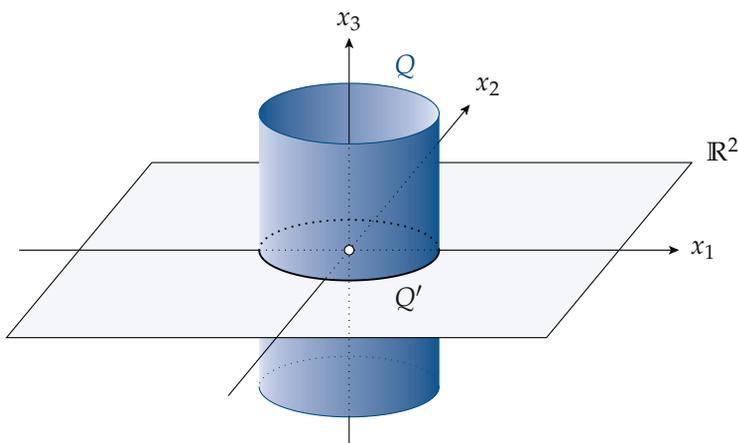
Schließlich noch eine Bemerkung zum Fall eines kleinen Ranges von A' . Dazu betrachten wir als Beispiel

$$Q := \{(x_1, x_2, x_3) \in \mathbb{R}^3 : x_1^2 + x_2^2 = 1\} \subset \mathbb{R}^3.$$

Hier ist $\text{rang } A = 2 < \text{rang } A' = 3 < 4 = n + 1$. Da x_3 in der Gleichung nicht vorkommt, ist Q ein *Zylinder* mit dem Kreis

$$Q' := \{(x_1, x_2) \in \mathbb{R}^2 : x_1^2 + x_2^2 = 1\} \subset \mathbb{R}^2.$$

als Basis.



Ganz analog erhält man im allgemeinen Fall Zylinder über einer Quadrik Q' aus einem Unterraum.

5.3.9 Der Trägheitstensor*

Von den zahlreichen Anwendungen der linearen Algebra wollen wir hier eine aus der Physik beschreiben: Die elementare Dynamik rotierender Körper. Zunächst einmal zur Erinnerung an einen Körper der Masse m , der sich im Raum geradlinig mit der Geschwindigkeit v bewegt. Dabei ist $m \in \mathbb{R}_+$ ein Skalar und $v \in \mathbb{R}^3$ ein Vektor. Dann ist

$$p = m \cdot v \quad \text{der Impuls} \quad \text{und} \quad E = \frac{1}{2} m \cdot \|v\|^2 \quad \text{die Energie}.$$

Wenn sich ein „starrer ausgedehnter Körper“ um eine Achse dreht, ist die Beschreibung schwieriger. Zunächst ist die *Winkelgeschwindigkeit* $\omega \in \mathbb{R}^3$ ein Vektor, der in Richtung der Drehachse zeigt. Gesucht ist nun der

$$\text{Drehimpuls } L \quad \text{und die Rotationsenergie } E$$

des Körpers als Funktion von ω .

Zur Vereinfachung der Beschreibung nehmen wir an, dass der Körper aus endlich vielen Massenelementen zusammengesetzt ist, die beschrieben sind durch Skalare $m_1, \dots, m_n \in \mathbb{R}_+$ und Vektoren $r^{(1)}, \dots, r^{(n)} \in \mathbb{R}^3$, die die Positionen der Massenelemente zu einer festen Zeit angeben. Die Rotation soll so verlaufen, dass der Schwerpunkt zu jeder Zeit im Ursprung liegt, d.h.

$$\sum_{v=1}^n m_v \cdot r^{(v)} = \mathbf{o}.$$

Physikalisch bedeutet das, dass der Ursprung auf der Drehachse liegt.

Die Bedingung der „Starrheit“ des Körpers soll bedeuten, dass sich die Abstände der Massenelemente zueinander und zur Drehachse während der Rotation nicht ändern. In Koordinaten geschrieben ist

$$\omega = \begin{pmatrix} \omega_1 \\ \omega_2 \\ \omega_3 \end{pmatrix} \quad \text{und} \quad r^{(v)} \equiv \begin{pmatrix} r_1^{(v)} \\ r_2^{(v)} \\ r_3^{(v)} \end{pmatrix}.$$

Dabei sollen die ω_i von der Zeit unabhängig sein, während die $r_i^{(v)}$ von ω und der Zeit abhängen.

Wir betrachten zunächst ein einzelnes Massenelement m_v und seine Position $r^{(v)}$ während der durch ω beschriebenen Rotation zu einer festen Zeit. Wenn wir zur Vereinfachung der Schreibweise den Index v vorübergehend unterdrücken, so gilt für Geschwindigkeit und Impuls zu dieser Zeit

$$v = \omega \times r \quad \text{und} \quad p = m \cdot v = m \cdot (\omega \times r).$$

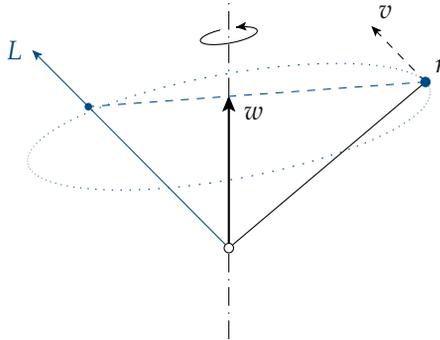
Der *Drehimpuls* des Massenelements m ist nun erklärt durch

$$L := m \cdot (r \times v) \in \mathbb{R}^3.$$

Er hängt also im Gegensatz zum linearen Impuls nicht nur von der Masse m und der augenblicklichen linearen Geschwindigkeit v , sondern auch vom Radius r ab. Indem man die GRASSMANN-Identität aus 0.3.7 benutzt und nach den Komponenten von r und ω sortiert, erhält man

$$\begin{aligned} L &= m \cdot (r \times v) = m \cdot r \times (\omega \times r) \\ &= m \cdot (\langle r, r \rangle \cdot \omega - \langle r, \omega \rangle \cdot r) \\ &= m \cdot \begin{pmatrix} \|r\|^2 - r_1^2 & -r_1 r_2 & -r_1 r_3 \\ -r_2 r_1 & \|r\|^2 - r_2^2 & -r_2 r_3 \\ -r_3 r_1 & -r_3 r_2 & \|r\|^2 - r_3^2 \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \\ \omega_3 \end{pmatrix}. \end{aligned}$$

Man beachte, dass L in dem von ω und r aufgespannten Untervektorraum des \mathbb{R}^3 liegt.



Bezeichnet man die obige von $r = r^{(v)}$ abhängige symmetrische Matrix mit R_v , so kann man für den Drehimpuls des Massenelements m_v auch

$$L^{(v)} = m_v \cdot R_v \cdot \omega$$

schreiben. Der gesamte *Drehimpuls* des Körpers ist dann erklärt durch

$$L := \sum_{v=1}^n L^{(v)}.$$

Da die Matrizen R_v symmetrisch sind, ist auch

$$\Theta := \sum_{v=1}^n m_v \cdot R_v$$

symmetrisch, und man erhält schließlich

$$L = \Theta \cdot \omega.$$

Die symmetrische Matrix $\Theta \in M(3 \times 3; \mathbb{R})$ wird **Trägheitstensor** des gegebenen starren Körpers genannt. Bei einem Körper mit kontinuierlich verteilter Dichte kann man die obigen n Summanden durch passende Integrale ersetzen.

Man beachte, dass die Radien $r^{(v)}$ von der Zeit t abhängen und dass der Verlauf durch ein fest gewähltes ω gesteuert wird. Demnach hängen auch die Matrizen R_v und schließlich Θ von ω und t ab.

Die Matrix Θ hat verschiedene Wirkungen. Zunächst ist

$$\Theta : \mathbb{R}^3 \rightarrow \mathbb{R}^3, \quad \omega \mapsto \Theta \cdot \omega = L$$

eine lineare Abbildung. Wegen der Symmetrie beschreibt Θ auch eine symmetrische Bilinearform

$$s : \mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}, \quad (x, x') \mapsto {}^t x \cdot \Theta \cdot x',$$

und dazu gehört eine Quadrik

$$Q := \{x \in \mathbb{R}^3 : {}^t x \cdot \Theta \cdot x = 1\} \subset \mathbb{R}^3.$$

Unter der Voraussetzung, dass die Massenelemente nicht alle auf einer Geraden durch o liegen, kann man zeigen, dass Θ positiv definit ist. Dann ist Q ein Ellipsoid, man nennt es **Trägheitsellipsoid**. Bevor wir seine physikalische Bedeutung beschreiben, berechnen wir Θ in Spezialfällen.

Beispiel 1 Besteht der Körper aus zwei Elementen gleicher Masse m_1 in den Punkten

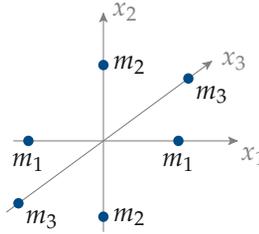
$$\begin{pmatrix} r_1 \\ 0 \\ 0 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} -r_1 \\ 0 \\ 0 \end{pmatrix} \quad \text{mit } r_1 > 0$$

zur Zeit $t = 0$, so gehört dazu der Trägheitstensor

$$\Theta_1 = 2 \cdot \begin{pmatrix} 0 & 0 & 0 \\ 0 & m_1 r_1^2 & 0 \\ 0 & 0 & m_1 r_1^2 \end{pmatrix}.$$

Befestigt man analog je zwei Massen m_2 und m_3 in Richtung x_2 und x_3 in Abständen $\pm r_2$ und $\pm r_3$, so erhält man entsprechende Matrizen Θ_2 und Θ_3 . Für den Trägheitstensor des ganzen als starr angenommenen Körpers gilt dann

$$\Theta = \Theta_1 + \Theta_2 + \Theta_3 = 2 \cdot \begin{pmatrix} m_2 r_2^2 + m_3 r_3^2 & 0 & 0 \\ 0 & m_1 r_1^2 + m_3 r_3^2 & 0 \\ 0 & 0 & m_1 r_1^2 + m_2 r_2^2 \end{pmatrix}.$$



Das ist eine Diagonalmatrix, die diagonalen Einträge

$$\vartheta_i = 2(m_j r_j^2 + m_k r_k^2)$$

mit paarweise verschiedenen $i, j, k \in \{1, 2, 3\}$ heißen **Hauptträgheitsmomente** des speziellen Körpers. In diesem einfachen Spezialfall ist also

$$L = \begin{pmatrix} L_1 \\ L_2 \\ L_3 \end{pmatrix} = \begin{pmatrix} \vartheta_1 \omega_1 \\ \vartheta_2 \omega_2 \\ \vartheta_3 \omega_3 \end{pmatrix}.$$

Bis hierher waren die Rechnungen ganz elementar, jetzt benutzen wir die Ergebnisse aus 5.3.5. Da die Matrix Θ , die im allgemeinen Fall den Trägheitstensor eines starren Körpers beschreibt, symmetrisch ist, hat sie reelle Eigenwerte $\vartheta_1, \vartheta_2, \vartheta_3$ und es gibt eine Matrix $S \in \text{SO}(3)$ derart, dass

$${}^t S \cdot \Theta \cdot S = \begin{pmatrix} \vartheta_1 & 0 & 0 \\ 0 & \vartheta_2 & 0 \\ 0 & 0 & \vartheta_3 \end{pmatrix} =: D$$

diagonal ist.

Die Spalten von S sind Eigenvektoren v_1, v_2, v_3 von Θ zu den Eigenwerten $\vartheta_1, \vartheta_2, \vartheta_3$. Man nennt die Geraden $\mathbb{R} \cdot v_i$ die **Hauptträgheitsachsen** des gegebenen starren Körpers. Wie im obigen Spezialfall heißen die Eigenwerte ϑ_i die **Hauptträgheitsmomente**. Man kann nachrechnen, dass Θ immer positiv semidefinit ist, also gilt auch $\vartheta_i \geq 0$.

Die physikalische Konsequenz dieses Ergebnisses ist, dass ein allgemeiner starrer Körper in den neuen orthonormalen Koordinaten

$$y = S^{-1} \cdot x = {}^t S \cdot x$$

das gleiche Trägheitsverhalten bei Rotationen hat, wie der ganz spezielle Körper mit nur sechs Elementarmassen $\frac{1}{2}$ in den Punkten auf den Koordinatenachsen mit den Abständen $\sqrt{\vartheta_i}$ von \mathbf{o} . Man beachte, dass die Hauptträgheitsachsen während der Rotation nur relativ zu dem starren Körper unverändert bleiben. Relativ zu dem Koordinatensystem des umgebenden Raumes bewegen sie sich mit dem rotierenden Körper. Die Eigenwerte von $\Theta(t)$ sind dagegen bis auf die Reihenfolge von der Zeit unabhängig.

Das *Trägheitsellipsoid* Q wird in den neuen y -Koordinaten wegen

$${}^t x \Theta x = {}^t (Sy) \Theta (Sy) = {}^t y ({}^t S \Theta S) y = {}^t y D y$$

beschrieben durch

$$Q = \{y \in \mathbb{R}^3 : \vartheta_1 y_1^2 + \vartheta_2 y_2^2 + \vartheta_3 y_3^2 = 1\}.$$

Ist Θ positiv definit, also $\vartheta_i > 0$ für $i = 1, 2, 3$, so ist das ein Ellipsoid mit den Hauptachsen

$$a_i = \frac{1}{\sqrt{\vartheta_i}}.$$

Eine einfache physikalische Interpretation des Trägheitsellipsoids erhält man durch die Berechnung der in der Rotation des Körpers steckenden Energie. Für ein einzelnes Massenelement $m = m_\nu$ ist die Energie gegeben durch

$$E = \frac{1}{2} m \cdot \|v\|^2 = \frac{1}{2} m \cdot \|\omega \times r\|^2.$$

Nach 0.3.7 ist

$$\|\omega \times r\|^2 = \|\omega\|^2 \cdot \|r\|^2 - \langle \omega, r \rangle^2 = \langle \omega, \|r\|^2 \cdot \omega - \langle \omega, r \rangle \cdot r \rangle,$$

und daraus folgt für das Massenelement m_ν , dass

$$E_\nu = \frac{1}{2} \langle \omega, L^{(\nu)} \rangle.$$

Wegen $E = \sum E_\nu = \frac{1}{2} \sum \langle \omega, L^{(\nu)} \rangle = \frac{1}{2} \langle \omega, L \rangle$ folgt daraus schließlich für die gesamte Rotationsenergie

$$E = \frac{1}{2} {}^t \omega \cdot \Theta \cdot \omega.$$

Das kann man so sehen: Will man in einen starren Körper die Rotationsenergie $\frac{1}{2}$ stecken, so muss man ω auf dem Trägheitsellipsoid wählen. Für eine beliebige vorgegebene Energie E hat man ein entsprechendes *Energieellipsoid*

$$Q_E := \{x \in \mathbb{R}^3 : {}^t x \cdot \Theta \cdot x = 2E\}.$$

Nun wollen wir die Abhängigkeit des Drehimpulses L von der Winkelgeschwindigkeit ω und von der Zeit t an einfachen Beispielen explizit berechnen.

Beispiel 2 Wir betrachten wieder einen als starr angenommenen Körper bestehend aus zwei Massenelementen $m_1 = m_2 = \frac{1}{2}$ in den Positionen

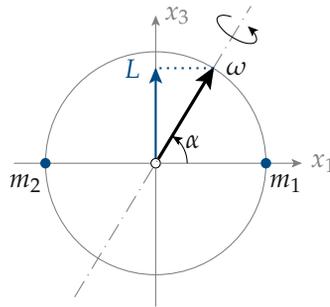
$$r^{(1)} = e_1 \quad \text{und} \quad r^{(2)} = -e_1.$$

Dann liegt der Schwerpunkt in \mathbf{o} und es ist

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

Wählen wir nun für $\alpha \in [0, 2\pi[$

$$\omega = \begin{pmatrix} \cos \alpha \\ 0 \\ \sin \alpha \end{pmatrix}, \quad \text{so ist} \quad L = \Theta \cdot \omega = \begin{pmatrix} 0 \\ 0 \\ \sin \alpha \end{pmatrix}.$$



Nur für $\omega = \pm e_3$ hat L die Richtung von ω .

Beispiel 3 Um zu sehen, wie sich der Trägheitstensor Θ und damit auch der Drehimpuls L im Lauf der Zeit verändern können, betrachten wir einen Körper, der aus zwei Massenelementen $m_1 = m_2 = \frac{1}{2}$ besteht, die sich zur Zeit $t = 0$ in den Positionen

$$r^{(1)}(0) = e_1 + e_3 \quad \text{und} \quad r^{(2)}(0) = -r^{(1)}(0)$$

befinden. Bei Rotation um die x_3 -Achse mit Einheitsgeschwindigkeit, also $\omega = e_3$, erhält man

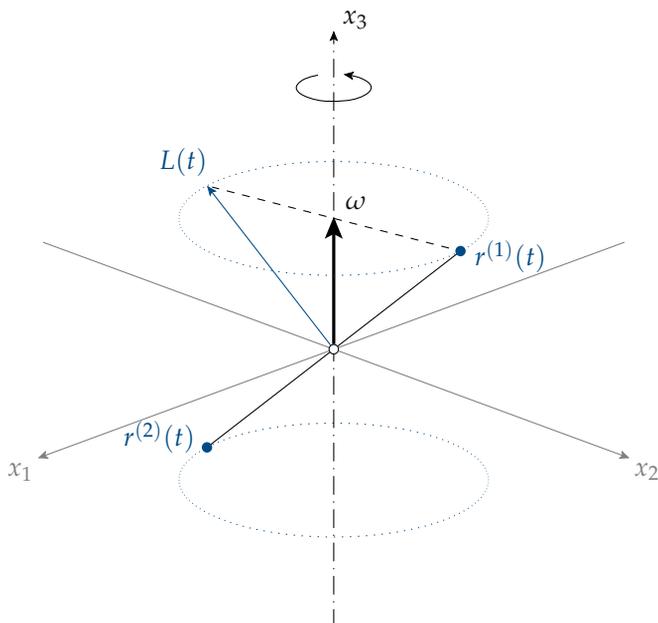
$$r^{(1)}(t) = \begin{pmatrix} \cos t \\ \sin t \\ 1 \end{pmatrix} \quad \text{und} \quad r^{(2)}(t) = -r^{(1)}(t).$$

Daraus folgt durch einfache Rechnung

$$\Theta(t) = \begin{pmatrix} 1 + \sin^2 t & -\cos t \sin t & -\cos t \\ -\cos t \sin t & 1 + \cos^2 t & -\sin t \\ -\cos t & -\sin t & 1 \end{pmatrix}$$

und somit

$$L(t) = \begin{pmatrix} -\cos t \\ -\sin t \\ 1 \end{pmatrix}.$$



Der Drehimpulsvektor $L(t)$ rotiert also mit dem Körper, die Norm $\|L(t)\| = \sqrt{2}$ und die Energie $E = \frac{1}{2} \langle \omega, L(t) \rangle = \frac{1}{2}$ bleiben dabei konstant. Der Trägheitstensor $\Theta(t)$ ist zu keiner Zeit in Hauptachsenform.

Die in Beispiel 3 beobachtete Veränderung des Drehimpulses im Laufe der Zeit hat eine physikalische Bedeutung. Um sie zu beschreiben betrachten wir zunächst wieder ein einzelnes Massenelement m , das sich in einer Position r mit der linearen Geschwindigkeit v bewegt. Dann ist

$$L = m \cdot (r \times v),$$

wobei die Vektoren r und v , also auch L von der Zeit t abhängen. Differentiation nach t mit Hilfe der Produktregel ergibt:

$$\dot{L} = m(\dot{r} \times v + r \times \dot{v}).$$

Da $\dot{r} = v$, folgt $\dot{r} \times v = \mathbf{o}$, also $\dot{L} = r \times m \dot{v}$. Der Vektor

$$F := m\dot{v}$$

ist die **Zentripetalkraft**, die das Massenelement zum Ausgleich der Zentrifugalkraft $-F$ in der Bahn hält. Das ergibt ein Drehmoment

$$M := r \times F = r \times m\dot{v} = m(r \times \dot{v}) = \dot{L}.$$

Also ist \dot{L} gleich dem Drehmoment, das nötig ist, um die Rotation des Massenelements in einer stabilen Bahn zu ermöglichen. Das gilt für jedes einzelne Massenelement m_ν , also ist

$$M = \sum_{\nu=1}^n M^{(\nu)} = \sum_{\nu=1}^n \dot{L}^{(\nu)} = \dot{L},$$

d.h. der Vektor \dot{L} beschreibt das gesamte Drehmoment, das als zeitabhängige „äußere Kraft“ auf die Drehachse wirken muss um die Rotation zu stabilisieren.

In Beispiel 3 gilt für die Massenelemente m_1 und m_2

$$\dot{v}^{(1)} = \begin{pmatrix} -\cos t \\ -\sin t \\ 0 \end{pmatrix} \quad \text{und} \quad \dot{v}^{(2)} = -\dot{v}^{(1)}, \quad \text{also}$$

$$M^{(1)} = \frac{1}{2}(r^{(1)} \times \dot{v}^{(1)}) = \frac{1}{2} \begin{pmatrix} \sin t \\ -\cos t \\ 0 \end{pmatrix} = M^{(2)}, \quad \text{also}$$

$$M = M^{(1)} + M^{(2)} = \dot{L}.$$

In der Physik beweist man durch Fortsetzung dieser Überlegungen den

Satz von der Erhaltung des Drehimpulses *Bei Abwesenheit äußerer Kräfte ist der Drehimpuls zeitlich konstant, in Zeichen*

$$\dot{L} = \mathbf{o}.$$

Man nennt den Trägheitstensor Θ einen „Tensor 2. Stufe“. Eine präzise mathematische Beschreibung dieser Objekte erfordert einigen formalen Aufwand (vgl. dazu etwa [BRÖ, Kap. VII] oder [FI₁, 6.3]). Von einem naiveren Standpunkt kann man einen Tensor 2. Stufe als Matrix ansehen. Allerdings ist es wichtig hinzuzufügen, welchen abstrakten Vorgang sie beschreibt, und wie sie sich somit bei Änderung der Koordinaten transformiert. Für den Trägheitstensor Θ und orthogonale Transformationen ist das besonders einfach. Sind im \mathbb{R}^3 , wie schon gerade beschrieben, neue Koordinaten gegeben durch

$$y = T \cdot x \quad \text{mit} \quad T \in \text{SO}(3), \quad \text{also} \quad x = S \cdot y \quad \text{mit} \quad S = -T^{-1},$$

und bezeichnen Θ_x bzw. Θ_y die Trägheitstensoren in den x - bzw. y -Koordinaten, so hat man für diese beiden Matrizen entsprechend ihren verschiedenen Wirkungen zwei Transformationsformeln (vgl. 5.2.2)

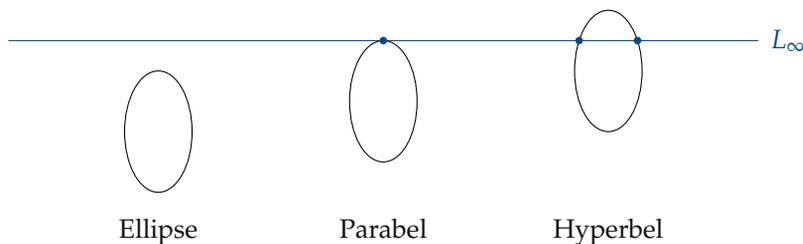
$$\begin{aligned} \Theta_y &= T \cdot \Theta_x \cdot T^{-1} = S^{-1} \cdot \Theta_x \cdot S, & \text{als Endomorphismen} & \quad \text{und} \\ \Theta_y &= {}^t S \cdot \Theta_x \cdot S & \text{als symmetrische Bilinearformen.} & \end{aligned}$$

Da $S \in \text{SO}(3)$, ist $S^{-1} = {}^t S$ und diese beiden Formeln passen zusammen.

5.3.10 Ausblick

Zum Abschluss dieses Buches erscheint ein Blick auf den großen Baum der Mathematik angebracht: er ist im Laufe der Zeit hoch gewachsen und hat sich dabei weit verzweigt; zwischen den verschiedenen Ästen bestehen zahlreiche Querverbindungen. Am Ende der vorausgegangenen Kapitel sind wir noch sehr weit entfernt von den Wipfeln, in denen der Baum, genährt aus den niedrigeren Ästen, durch die Ergebnisse der aktuellen Forschung stetig weiter wächst. Jedes gelöste Problem erzeugt neue Probleme und weitere Verzweigungen der Äste. Wir können hier nur ganz kurz andeuten, wie es nun auf einem der vielen Wege den Baum hinauf weitergeht.

In der analytischen Geometrie wird vieles übersichtlicher, wenn man zu den Standardräumen K^n „unendlich ferne“ Punkte hinzunimmt, und sie zu den projektiven Räumen $\mathbb{P}_n(K)$ abschließt. Dadurch kann man – etwa bei der Klassifikation von Quadriken – viele Fallunterscheidungen vermeiden. Im einfachsten Fall der Ebene \mathbb{R}^2 kommt eine unendlich ferne Gerade L_∞ hinzu, und in $\mathbb{P}_2(\mathbb{R})$ unterscheiden sich Ellipse, Parabel und Hyperbel nur noch durch ihre Lage zu L_∞ :



Quadriken sind beschrieben durch eine quadratische Gleichung und stehen – wie wir gesehen haben – in engem Zusammenhang zu Matrizen und damit noch zur linearen Algebra. Betrachtet man allgemeiner im K^n oder in $\mathbb{P}_n(K)$ die Menge der Nullstellen eines oder mehrerer Polynome beliebigen Grades, so erhält man als Verallgemeinerung der Lösungsmenge eines linearen Gleichungssystems eine so genannte „algebraische Varietät“; diese sind die Objekte der „algebraischen Geometrie“, die sich im 20. Jahrhundert zusammen mit den Methoden der Algebra stürmisch entwickelt hat. Durch die engen Bezüge der algebraischen Geometrie zur Zahlentheorie ist es gelungen, ein uraltes Problem zu lösen. Es geht dabei um positive ganzzahlige Lösungen der Gleichung

$$x^n + y^n = z^n. \quad (*)$$

Für $n = 2$ heißen die Lösungen (x, y, z) – etwa $(3, 4, 5)$ – *pythagoreische Tripel*. Dass es davon unendlich viele gibt, die nicht Vielfache voneinander sind, ist schon seit EUKLID bekannt: Es gibt unendlich viele ungerade Primzahlen p , also auch unendlich viele Zahlen der Form $p^2 = 2k + 1$, mit $k \in \mathbb{N}$. Daher ist jedes der unendlich vielen Tripel $(p, k, k + 1)$ pythagoreisch. FERMAT hatte 1670 die Aussage, dass es für $n \geq 3$ keine positiven ganzzahligen Lösungen der Gleichung $(*)$ geben kann, am Rand eines Buches

notiert, aber keinen Beweis dafür gegeben. Seither hatten sich zahllose Zahlentheoretiker an diesem Problem versucht, aber nur relativ kleine Teilerfolge erzielt. Schließlich ist es A. WILES mit Unterstützung anderer Zahlentheoretiker im Jahr 1994 gelungen, die Aussage von FERMAT zu beweisen. Dabei werden im 20. Jahrhundert erzielte Ergebnisse aus den höchsten Wipfeln der Algebra benötigt.

Leider ist es kaum möglich, in einem gewöhnlichen Studium der Mathematik bis zum Verständnis eines solchen Beweises vorzudringen; das gelingt nur einigen Experten. Aber wenigstens eine über die lineare Algebra hinausgehende Vorlesung über „höhere“ Algebra gehört zu den meisten Curricula: Dort werden auf jeden Fall Polynome beliebigen Grades und ihre Nullstellen, sowie grundlegende Ergebnisse über Gruppen und Ringe behandelt.

Literaturverzeichnis

- [BA] BANACH, ST.: *Théorie des opérations linéaires*. Warschau, 1932
- [BR] BRIESKORN, E.: *Lineare Algebra und analytische Geometrie I*. Vieweg, 1983
- [BRÖ] BRÖCKER, T.: *Lineare Algebra und analytische Geometrie*. Birkhäuser, 2004²
- [CA₁] CANTOR, G.: *Über die Ausdehnung eines Satzes aus der Theorie der trigonometrischen Reihen*. Math. Ann. **5**, 123-132 (1872)
- [CA₂] CANTOR, G.: *Beiträge zur Begründung der transfiniten Mengenlehre*. Math. Ann. **46**, 481-512 (1895)
- [DED₁] DEDEKIND, R.: *Stetigkeit und Irrationalzahlen*. Vieweg, 1872
- [DED₂] DEDEKIND, R.: *Was sind und was sollen die Zahlen*. Vieweg, 1888
- [DÜ] DÜRER, A.: *Underweysung der messung mit dem zirckel un̄ richtscheyt in Linien ebenen unnd gantzen corporen*. Nürnberg, 1525
- [EB] EBBINGHAUS, H.-D. ET AL: *Zahlen*. Springer, 1992³
- [EU] EUKLID: *Die Elemente*. Vieweg, 1933-1937
- [FI₁] FISCHER, G.: *Lineare Algebra*. Vieweg, 2010¹⁷
- [FI₂] FISCHER, G.: *Analytische Geometrie*. Vieweg, 2001⁷
- [FI₃] FISCHER, G.: *Lehrbuch der Algebra*. Vieweg, 2011²
- [FI₄] FISCHER, G.: *Plane Algebraic Curves*. American Mathematical Society, 2001. American Mathematical Society, 2001
- [F-B] FLADT, K., BAUR, A.: *Analytische Geometrie spezieller Flächen und Raumkurven*. Vieweg, 1975
- [FO₁] FORSTER, O.: *Analysis I*. Vieweg, 2008⁹
- [FO₂] FORSTER, O.: *Analysis II*. Vieweg, 2008⁸
- [FO₃] FORSTER, O.: *Analysis III*. Vieweg, 2011⁶
- [GA₁] GAUSS, C. F.: *Demonstratio nova theorematum omnium functionum algebraicarum racionales integram unius variabilis in factores reales primi vel secundi gradus resolvi posse*. Göttingen 1799. Werke Band 3, 1-30
- [GA₂] GAUSS, C. F.: *Disquisitio de elementis ellipticis Palladis*. Göttingen 1811. Werke Band 6, 3-24
- [GA₃] GAUSS, C. F.: *Theoria residuorum biquadraticorum, commentatio secunda*. Göttingen 1831. Werke Band 2, 93-148
- [GR] GRASSMANN, H.: *Die Ausdehnungslehre*. Enslin, 1862
- [GRC] GRCAR, J.: *How Ordinary Elimination Became Gaussian Elimination*. Historia Math. **38**, 163-218 (2011)

- [HI₁] HILBERT, D.: *Über die stetige Abbildung einer Linie auf ein Flächenstück*. Math. Ann. **38**, 459-460 (1891)
- [HI₂] HILBERT, D.: *Grundlagen der Geometrie*. Teubner, 1899
- [JO] JORDAN, W.: *Handbuch der Vermessungskunde. Band 1, Ausgleichsrechnung*. Metzler, 1888³
- [HI₃] HILBERT, D.: *Mathematische Probleme*. Göttingen, 1900, Ges. Abh. 3, 290-329
- [KA] KANT, I.: *Versuch den Begriff der negativen Größen in die Weltweisheit einzuführen*. J. Kanter, 1763. Werkausgabe 2, Suhrkamp, 1977
- [KOE] KOECHER, M.: *Lineare Algebra und analytische Geometrie*. Springer, 1983
- [KR] KRAMER, J.: *Zahlen für Einsteiger*. Vieweg, 2008
- [L-M] LIESEN, J., MEHRMANN, V.: *Lineare Algebra*. Vieweg+Teubner, 2011
- [MU] MUIR, TH.: *The Theory of Determinants*. Cambridge, 1906-1923
- [PE₁] PEANO, G.: *Calcolo geometrico secondo l'Ausdehnungslehre di H. Grassmann*. Frat. Bocca, 1888
- [PE₂] PEANO, G.: *Arithmetices principia nova exposita*. Frat. Bocca, 1889
- [PE₃] PEANO, G.: *Sur une courbe, qui remplit toute une aire plane*. Math. Ann. **36**, 157-160 (1890)
- [R-S] REISS, K., G. SCHMIEDER: *Basiswissen Zahlentheorie*. Springer, 2007²
- [R-O] RICHTER-GEBERT, J., ORENDT, T.: *Geometrikalküle*. Springer, 2009
- [S-S] SCHREIER, O., E. SPERNER: *Einführung in die analytische Geometrie und Algebra*. Teubner, 1931
- [ST] STEINITZ, E.: *Bedingt konvergente Reihen und konvexe Systeme*. J. Reine Angew. Math. **143**, 128-175 (1913)
- [STR] STRANG, G.: *Lineare Algebra*. Springer, 2003
- [WA] VAN DER WAERDEN, B.L.: *Moderne Algebra*. Springer, 1931
- [WEB] WEBER, H.: *Die allgemeinen Grundlagen der Galois'schen Gleichungstheorie*. Math. Ann. **43**, 521-549 (1893)
- [WEY] WEYL, H.: *Raum-Zeit-Materie*. Springer, 1918
- [ZI] ZIEGLER, G.M.: *Darf ich Zahlen?* Piper, 2010 Der „Exponent“ an der Jahreszahl gibt die Nummer der Auflage an.

Der „Exponent“ an der Jahreszahl gibt die Nummer der Auflage an.

Index

- Abbildung, 85
 - affine, 394
 - alternierende, 288
 - bijektive, 86
 - bilineare, 380
 - identische, 85
 - injektive, 86
 - lineare, 217
 - surjektive, 86
- Absolutbetrag, 125, 137
- Abstand, 22
 - eines Punktes von einer Ebene, 61
 - zweier Geraden, 49
 - zwischen Punkt und Gerade, 33
- Achsen, 7
- Addition
 - zweier Vektoren, 8
- Additionstheoreme, 251
- Affinität, 394
- allgemeine Lage, 372
- Annulator, 269
- Anordnung, 124, 136
 - archimedische, 124
- Antinomie
 - von RUSSEL, 83
- Apfel-Lemma, 228
- Äquivalenz, 93
- Äquivalenzklasse, 95
- Äquivalenzrelation, 94
- Argument
 - einer komplexen Zahl, 148
- Assoziativität, 4, 100
- Asymptoten
 - einer Hyperbel, 369
- Aufhängepunkt, 13
- Ausartungsraum, 384
- Austauschlemma, 193
- Automorphismus, 224
- Axiom, 81
- Basis, 188
 - affine, 394
 - kanonische, 188
 - orthogonale, 386
- Basis-Austauschsatz, 191
- Basis-Auswahlsatz, 190
- Basis-Ergänzungssatz, 193
- Basisvektor
 - kanonischer, 10
- Basiswechsel, 273
- Betrag, 125
 - einer komplexen Zahl, 145
- Bild, 85, 220
- Bilinearform, 380
 - alternierende, 380
 - indefinite, 411
 - negativ definite, 411
 - nicht entartete, 385
 - positiv definite, 411
 - symmetrische, 380
- Blockmatrizen, 294
- Brennpunkt
 - einer Ellipse, 367
 - einer Hyperbel, 369
 - einer Parabel, 369
- Büschel, 371
- CAUCHY-Folge, 132
- Charakteristik, 152
- charakteristische Funktion, 325
- Cosinussatz, 30
- CRAMERSche Regel, 282, 314

- Darstellung
 - binäre, 118
 - g -adische, 118
 - triviale, 181
- Definitheit, 411, 416, 444
- Definition
 - rekursive, 99
- Determinante, 39, 63, 287
 - eines Endomorphismus, 325
- Determinanten-Multiplikations-Satz, 295
- Dezimalbruch, 5, 126, 139
 - abbrechender, 126
 - echter, 140
 - periodischer, 126
 - rein periodischer, 126
- Dezimaldarstellung, 117, 118
- Dezimalentwicklung, 5
- Diagonalen-Satz, 25
- Diagonalisierbarkeit, 329, 334, 431, 443
- Diagonalmatrix, 291
- Diagonalverfahren, 90, 92
- Diagramm
 - kommutatives, 243
- Differenz
 - zweier Mengen, 84
- Dimension
 - eines affinen Raumes, 232, 394
 - eines Vektorraums, 192
- Dimensionsformel
 - für lineare Abbildungen, 228
 - für Untervektorräume, 203
- Diskriminante, 162
- Distributivität, 4, 100
- Division mit Rest, 116, 160
- Drehimpuls, 458, 459
- Drehung, 250, 318
- Dreiecksmatrix, 291
 - obere, 267
 - untere, 267
- Dreiecksungleichung, 30, 145
- Dualität, 268
- Durchschnitt, 84

- Ebene, 51
- Ebenen
 - parallele, 58
 - windschiefe, 55
- Eigenraum, 316
- Eigenvektor, 316
- Eigenwert, 316
- Einheit
 - imaginäre, 144
- Einheitsmatrix, 252
- Einheitswurzel, 171
- Einschränkung, 86
- Einselement, 115
- Element, 82
 - inverses, 103, 105
 - negatives, 105
 - neutrales, 100, 103, 105
- Elementarmatrix, 259
- Elimination, 64, 73
- Ellipse, 366
- Ellipsoid, 456
- Endomorphismen-Ring, 227
- Endomorphismus, 224
 - adjungierter, 442
 - diagonalisierbarer, 329, 334
 - nilpotenter, 343, 349
 - orthogonaler, 429
 - selbstadjungierter, 442
 - trigonalisierbarer, 339
 - unitärer, 429
- Energie, 458
- Energieellipsoid, 462
- Epimorphismus, 224
- Erzeugendensystem, 188
 - unverkürzbares, 196
 - unverlängerbares, 196
- Exponentialreihe, 146

- Fahne, 338
- Fakultät, 106
- Faser, 85
- Fehlervektor, 425
- Fehlstand, 299
- Fluss, 321
- Folge
 - konvergente, 132
- Formel
 - von EULER, 147
- FOURIER-Reihe, 380
- Fundamentalsatz der Algebra, 168
- Funktion
 - elementarsymmetrische, 166
- Fußpunkt, 33

- Gärtnerkonstruktion, 368

- GRASSMANN-Identität, 45
- GAUSS-Elimination, 427
- GAUSS-JORDAN-Verfahren, 262
- Gerade, 1, 13
- Geraden
 - parallele, 16, 46
 - windschiefe, 46
- Gleichungssystem, 66
 - überbestimmtes, 425
 - homogenes, 72
 - inhomogenes, 72
 - überbestimmtes, 71
- Grad
 - eines Polynoms, 157
- Graph, 85, 93
- Gruppe, 105
 - abelsche, 105
 - allgemeine lineare, 256
 - alternierende, 304
 - orthogonale, 430
 - spezielle orthogonale, 430
 - symmetrische, 106, 300
 - unitäre, 430
- Halbgruppe, 104
- Haupt-Minor, 416
- Hauptachsen
 - einer Ellipse, 365, 367
 - einer Hyperbel, 366
 - einer Quadrik, 449
- Hauptachsentransformation, 448
- Hauptraum, 344
- Haupttragheitsachsen, 461
- Haupttragheitsmomente, 461
- Haupttragsheitsmomente, 461
- hermitesche Form, 410
- HESSE-Matrix, 411
- HILBERT-Matrix, 79, 382
- Höhensatz, 31
- Höhenschnittpunkt-Satz, 32
- Homomorphismus, 113, 123, 217, 224
- Hyperbel, 364, 366
- Hyperboloid
 - einschaliges, 455
 - zweischaliges, 455
- Ideal, 134
- Identifikation, 93
- Imaginärteil, 145
- Impuls, 458
- Induktion, 98
- Intervallschachtelung, 132
- Invariante, 357
- Isometrie, 448
- Isomorphie, 224
- Isomorphismus, 113, 123, 224
- JORDAN-Matrix, 350
- JORDAN-Strang, 350
- Kegel, 408
 - elliptischer, 454
- Kegelschnitt, 397
 - irreduzibler, 375
 - reduzibler, 375
- Kern, 220
- Klasse, 83
- Klassifikation
 - von Endomorphismen, 357
- Koeffizient, 12, 66, 157
- Koeffizientenmatrix, 67
- Kommutativität, 4, 100
- Komplement
 - orthogonales, 423
- Komposition
 - von Abbildungen, 87
- Kongruenz, 94
- Konjugation
 - komplexe, 145
- Koordinaten, 242
 - kartesische, 2, 7
- Koordinatensystem, 242
- Körper, 4, 120
 - endlicher, 149
 - vollständiger, 138
- Kreiskegel, 363
- Kreuzprodukt, 41
- Kurve, 320
- Kürzungsregel, 11, 100, 103
- LAGRANGE-Multiplikator, 447
- Länge
 - einer Basis, 189
 - eines Vektors, 20
- LAPLACE-Entwicklung, 313
- Law of Moduli, 145
- LEIBNIZ-Formel, 305
- Leitgerade

- einer Parabel, 369
- Lemma von FITTING, 345
- linear abhängig, 38, 40, 182
- linear unabhängig, 38, 40, 62, 181
- Linearfaktor, 165
- Linearform, 269
- Linearkombination, 10, 180
- Linie, 1
- Linkstranslation, 107
- Lösung
 - triviale, 72
- Lösungsmenge, 66, 67
- Lösungsraum, 12, 233
- LR-Zerlegung, 267

- Mächtigkeit, 82
- Matrix, 66
 - darstellende, 243, 381
 - diagonalisierbare, 329
 - erweiterte, 396
 - hermitesche, 410
 - inverse, 255, 311
 - invertierbare, 255
 - komplementäre, 311
 - nilpotente, 343
 - orthogonale, 429
 - symmetrische, 211
 - transponierte, 211
 - unitäre, 429
- Matrizen
 - ähnliche, 357
- Matrizen-Ring, 254
- Maximums-Norm, 238
- Menge, 81
 - abzählbar unendliche, 89
 - abzählbare, 89
 - endliche, 82
- Mengen
 - gleichmächtige, 89
- Methode der kleinsten Quadrate, 427
- Mittelpunkt, 25
- Modul, 94, 198
- Monom, 184
- Monomorphismus, 224
- Multiplikation
 - mit einem Skalar, 9
 - von Matrizen, 249
 - zweier Vektoren, 11

- n -Tupel
 - geordnetes, 8, 84
- Nachfolgeabbildung, 98
- Norm, 20, 22, 238, 239, 419
 - einer komplexen Zahl, 145
- Normalenvektor, 60
- Normalform, 357
 - für Kegelschnitte, 402
 - für Quadriken, 408
 - HESSEsche, 37, 61
 - JORDANsche, 356
 - von Matrizen, 277
 - von nilpotenten Endomorphismen, 351
- Null, 105
- Nullfolge, 132
- Nullmatrix, 176
- Nullpolynom, 157
- Nullstelle, 161
- Nullteiler, 11
- Nullvektor, 10, 174

- Oktaven, 149
- Ordnung
 - einer Gruppe, 106
- Orientierung, 285
- Orthogonalität, 419
- Orthonormalbasis, 419
- Orthonormalisierungs-Satz von GRAM und SCHMIDT, 421
- Orthonormalität, 419

- Paar
 - geordnetes, 7
 - paarweise verschieden, 82
- Parabel, 364, 366
- Paraboloid
 - elliptisches, 457
 - hyperbolisches, 456
- Paradoxon
 - vom Barbier, 83
 - von PERRON, 50
- Parallelogramm, 61, 282
- Parallelogramm-Gesetz, 24
- Parameter, 13
- Parameterdarstellung, 13, 51
- Parität, 302
- Partialsumme, 126
- PEANO-Axiome, 98
- Periodenlänge, 126

- Permutation, 298
- Permutationsgruppe, 106
- Permutationsmatrix, 303
- Pivot, 67
- Pol, 377
- Polare, 377
- Polarisierung, 382
- Polarkoordinaten, 148
- Polynom, 157
 - charakteristisches, 326
 - konstantes, 158
 - normiertes, 158
- Polynomfunktion, 157
- Positivitäts-Index, 392
- Potenzmenge, 83, 102
- Primkörper, 152
- Produkt
 - direktes, 84, 176
 - von Matrizen, 249
- Produktfolge, 133
- Punkt, 1, 7, 8

- quadratische Form, 382
- Quadrik, 397
- Quaternionen, 149
- Quotientenvektorraum, 236

- Rang
 - einer Matrix, 212
 - einer symmetrischen Bilinearform, 384
- Rang-Satz, 212
- Realteil, 145
- Rechtstranslation, 107
- Reflexivität, 94
- Regel von SARRUS, 305
- Reihe
 - geometrische, 127
- Relation, 93
- Repräsentant, 97
- Restklasse, 97
- Restklassenring, 135, 151
- Richtungsvektor, 13
- Ring, 115
 - kommutativ, 115
- Rotationsenergie, 458

- Sattelfläche, 456
- Satz
 - nach PYTHAGORAS, 29
 - vom kleinsten Element, 101
 - von der Erhaltung des Drehimpulses, 465
 - von PYTHAGORAS, 20, 23
- Scheitelpunkte
 - einer Ellipse, 367
- Scherung, 291
- Schnitt
 - DEDEKINDScher, 132
- Schubkastenprinzip, 87
- Schwerpunkt, 25
- Schwerpunkt-Satz, 26
- Seitenhalbierende, 26
- Sesquilinearform, 410
- Signum, 299
- Skalar, 9, 174
- Skalarprodukt, 11, 20, 21, 27, 418
 - kanonisches, 409
- Spalte, 66
- Spaltenrang, 211
- Spaltenraum, 211
- Spaltenvektor, 210
- Spat, 62
- Spatprodukt, 61
- Spiegelung, 318
- Sprungfunktion, 238
- Spur
 - einer Matrix, 327
- Standardbasis, 188
- Standardebene, 7
- Standardraum, 175
 - reeller, 8
- Strecke, 15
- Substitution, 64
- Summand
 - direkter, 206
- Summe
 - direkte, 204, 206
 - orthogonale, 423
 - von Untervektorräumen, 180, 203
- Summenfolge, 133
- Symmetrie, 94

- Tangentenvektor, 321
- Teilmenge, 82
 - echte, 82
- Teilung
 - mit Rest, 96
- Trägheitsellipsoid, 460, 462
- Trägheitsgesetz von SYLVESTER, 392

- Tragheitstensor, 460
- Transformationsformel
 - für Bilinearformen, 383
 - für hermitesche Formen, 410
 - für lineare Abbildungen, 275
 - für Quadriken, 400
- Transformationsmatrix, 273
- Transitivität, 94
- Translation, 9, 394
- Transposition, 302
- Trigonalisierbarkeit, 339
- Tripel
 - geordnetes, 7
- Umformung
 - symmetrische, 388
- Unbekannte, 12
- Unbestimmte, 157
- Ungleichung
 - von CAUCHY-SCHWARZ, 27, 40, 44
- Untergruppe, 112
- Unterraum
 - affiner, 231
- Unterring, 122
- Untervektorraum, 52, 177
 - aufgespannter, 180
 - invarianter, 338
 - zyklischer, 350
- Urbild, 85
- Ursprung, 7, 9
- Vektor, 9
 - negativer, 10
 - normierter, 22
 - senkrechter, 28, 31, 33, 43, 59, 420
- Vektorfeld, 321
- Vektorprodukt, 11, 41
- Vektorraum, 10, 174
 - dualer, 269
 - endlich erzeugter, 188
 - euklidischer, 418
 - unitärer, 418
- Vereinigung, 83
- Verknüpfung
 - assoziative, 103
 - innere, 103
 - kommutative, 103
- Verknüpfungstafel, 107
- Vielfachheit
 - einer Nullstelle, 165
 - eines Eigenwertes, 332
- Vorperiode, 126
- Vorzeichenregel, 115, 166
- Winkel, 20, 27
 - orientierter, 284
- Winkelgeschwindigkeit, 458
- Wohldefiniiertheit, 111
- Wurzelsatz von VIETA, 166
- Zahl
 - ganze, 2, 110, 111
 - komplexe, 6
 - konjugiert komplexe, 145
 - natürliche, 2, 98
 - positive, 124, 136
 - rationale, 3, 119, 121
 - reelle, 6, 134
- Zahlbereich, 6
- Zahlenebene, 143
- Zahlkörper, 149
- ZASSENHAUS-Algorithmus, 210
- Zeile, 66
- Zeilenrang, 211
- Zeilenraum, 211
- Zeilenstufenform, 67
- Zeilenumformung, 74
- Zeilenvektor, 210
- Zentripetalkraft, 464
- Ziffer, 5, 117
- Zylinder, 457

Symbolverzeichnis

$a := b$	a ist definiert durch b	\mathbb{C}	komplexe Zahlen, 6, 144
$A \Rightarrow B$	aus A folgt B	$\mathbb{Z}/m\mathbb{Z}$	Restklassenring, 151
$A \Leftrightarrow B$	A und B sind gleichwertig	\mathbb{F}_p	Körper mit p Elementen, 152
\rightarrow, \mapsto	Abbildungspfeile, 85	\mathbb{K}	\mathbb{R} oder \mathbb{C}
$\{ \}$	Mengenklammern, 82	K^*	K ohne Null, 120
\emptyset	leere Menge, 82	K^n	Standardraum, 175
\in	Element, 82	\mathcal{K}	kanonische Basis, 188
\subset	Teilmenge, 82	$S(X), S_n$	symmetrische Gruppe, 106
\subsetneq	echte Teilmenge, 82	A_n	alternierende Gruppe, 304
\cup	Vereinigung, 83	$M(m \times n; K)$	Raum der Matrizen, 176
\cap	Durchschnitt, 84	$GL(n; K)$	allgemeine lineare Gruppe, 256
\setminus	Differenzmenge, 84	$O(n)$	orthogonale Gruppe, 430
\times	direktes Produkt, 84 oder Vektorprodukt, 41	$SO(n)$	spezielle orthogonale Gruppe, 430
$\langle \ , \ \rangle$	Skalarprodukt, 20, 409, 418	$U(n)$	unitäre Gruppe, 430
$\ \ \ $	Norm, 20, 409	$K[X]$	Polynomring, 157
$d(\ , \)$	Abstand, 22	A'	erweiterte Matrix, 396
\sphericalangle	Winkel, 27	A^{-1}	inverse Matrix, 255
\perp	senkrecht, 28	${}^t A$	transponierte Matrix, 211
\circ	Komposition von Abbildungen, 87	$A^\#$	komplementäre Matrix, 311
\sim	äquivalent, 93	E_i^j	Basismatrix, 183
\equiv	kongruent, 94	E_n	Einheitsmatrix, 252
$\#$	Anzahl der Elemente, 82	M_B^A, M_B	darstellende Matrizen, 243, 381
$+$	Summe von Unterräumen 180, 203	T_B^A	Transformationsmatrix, 273
\oplus	direkte Summe, 204	Φ_B	Koordinatensystem, 242
\bigoplus	orthogonale Summe, 423	P_F	charakt. Polynom von F , 326
π	Kreiszahl, 129	Abb	Abbildungen, 103, 175
i	imaginäre Einheit, 144	char	Charakteristik, 153
\mathbf{o}	Nullvektor, 10, 174	deg	Grad, 157
e_i	kanonischer Basisvektor, 10, 188	det	Determinante, 287
f^{-1}	Urbild oder Umkehrabbildung, 85	dim	Dimension, 192
$f M$	Einschränkung, 86	Eig	Eigenraum, 316
id_M	identische Abbildung, 85	Hau	Hauptraum, 344
$n!$	Fakultät, 106	End	Endomorphismen, 227
$\vec{p}\vec{q}$	Translation, 393	Hom	Homomorphismen, 226
\mathbb{N}	natürliche Zahlen, 2, 82, 98	Ker	Kern, 220
\mathbb{N}^*	natürliche Zahlen ohne Null, 2	Lös	Lösungsmenge, 67, 231
\mathbb{Z}	ganze Zahlen, 2, 110	ord	Ordnung, 106
\mathbb{Q}	rationale Zahlen, 3, 119	rang	Rang, 212, 384
\mathbb{R}	reelle Zahlen, 6, 134	sign	Signum, 299
\mathbb{R}_+	reelle Zahlen ≥ 0	Span	aufgespannter Vektorraum, 180