Vorlesungsskript zur Linearen Algebra 1 für Physiker

Lino Haupt

21. Juli 2026

Inhaltsverzeichnis

0 Vorwort **4**
- 0.1 Die Besonderheit der Mathematik . . . 4
  - 0.1.1 Die Rolle der Beweise . . . 4
  - 0.1.2 Historisches . . . 5

1 Grundlagen **7**
- 1.1 Klassische Logik . . . 7
- 1.2 Formale Aussagenlogik . . . 10
  - 1.2.1 Syntax – Die Formeln der Aussagenlogik . . . 10
  - 1.2.2 Semantik – Die formale Bedeutung von Aussagen . . . 14
  - 1.2.3 Das Folgerungssymbol „⇒“, logische Äquivalenz und nützliche Regeln . . . 18
- 1.3 Prädikatenlogik . . . 24
  - 1.3.1 Die Schranken der Aussagenlogik . . . 24
  - 1.3.2 Atomare Aussagen in der Prädikatenlogik . . . 25
  - 1.3.3 Quantoren . . . 27
  - 1.3.4 Einschränkungen von Quantoren und Mengenlehre . . . 33
- 1.4 Grundbegriffe der Mengenlehre . . . 35
  - 1.4.1 Der Mengenbegriff . . . 35
  - 1.4.2 Elemente und Teilmengen . . . 37
  - 1.4.3 Mengen und Aussagen . . . 38
  - 1.4.4 Grundlegende Mengenoperationen . . . 39
  - 1.4.5 Familien von Mengen . . . 42
  - 1.4.6 Die Potenzmenge . . . 44
- 1.5 Relationen und Funktionen . . . 45
  - 1.5.1 Paare und Produkte . . . 45
  - 1.5.2 Allgemeine Relationen . . . 51
  - 1.5.3 Funktionen . . . 54
  - 1.5.4 Äquivalenz- und Ordnungsrelationen . . . 73

2 Abstrakte Algebra **88**
- 2.1 Gruppen . . . 88
  - 2.1.1 Allgemeines . . . 88
  - 2.1.2 Permutationsgruppen . . . 97
  - 2.1.3 Gruppenhomomorphismen . . . 102
  - 2.1.4 Das Vorzeichen einer Permutation . . . 110
- 2.2 Ringe . . . 114
- 2.3 Körper . . . 121

3 Vektorräume **126**
3.1 Definition . . . 126
3.2 Darstellungen von Vektoren . . . 132
3.2.1 Lineare Unabhängigkeit . . . 132
3.2.2 Lineare Hülle . . . 140
3.2.3 Untervektorräume . . . 142
3.2.4 Erzeugendensystem . . . 146
3.3 Basen und Dimension . . . 149
3.3.1 Was sind Basen – Existenz & Konstruktion . . . 149
3.3.2 Die Länge von Basen – Dimension . . . 153
3.3.3 Anwendungen und Rechenregeln der Dimension . . . 157

4 Lineare Abbildungen **163**
4.1 Definition . . . 163
4.2 Matrizen und die von ihnen induzierten linearen Abbildungen . . . 168
4.3 Lineare Abbildungen sind durch Erzeuger bestimmt . . . 170
4.4 Jede lineare Abbildung zwischen Standardräumen entspricht einer Matrix . . . 171
4.5 Isomorphismen, Kern und Bild . . . 174
4.6 Lineare Fortsetzung von Basiswerten . . . 179

5 Koordinaten und Basiswechsel **182**
5.1 Konjugation: umbenennen, anwenden, zurückbenennen . . . 182
5.2 Koordinatenvektoren . . . 187
5.3 Die Matrix einer linearen Abbildung bezüglich Basen . . . 192
5.4 Basiswechsel . . . 197

6 Lineare Gleichungssysteme **205**
6.1 Definition und Darstellung . . . 205
6.2 Homogener Fall . . . 208
6.2.1 Homogene Gleichungssysteme in Zeilenstufenform . . . 208
6.2.2 Elementare Zeilenoperationen . . . 212
6.2.3 Das Gaußsche Eliminationsverfahren . . . 213
6.3 Inhomogener Fall . . . 215
6.3.1 Das erweiterte Gaußverfahren . . . 217
6.3.2 Die Form der Lösungsmenge . . . 220
6.3.3 Das Rang-Kriterium für Lösbarkeit . . . 222
6.4 Invertieren von Matrizen . . . 225
6.4.1 Wie findet man eine Rechtsinverse? . . . 228
6.4.2 Invertieren mit dem erweiterten Gaußverfahren . . . 229

7 Die Determinante **234**
7.1 Determinantenfunktionen . . . 234
7.2 Berechnung mit dem Gaußverfahren . . . 240
7.3 Existenz: die Leibnizformel . . . 242
7.4 Determinante, Rang und Invertierbarkeit . . . 245
7.5 Elementarmatrizen und die Produktformel . . . 246
7.5.1 Matrizen kodieren Zeilenoperationen . . . 246
7.5.2 Elementarmatrizen und die Determinante . . . 247
7.5.3 Die Produktregel . . . 247
7.5.4 Blockmatrizen . . . 250

7.5.5 Alternativer Beweis zur Invarianz der Determinante unter Transposition 252
7.6 Laplace Entwicklung . . . 253
7.7 Die Determinante eines Endomorphismus . . . 254
7.8 Komplexe Konjugation und Determinanten . . . 256

8 Eigenwerte und Eigenvektoren 258
8.1 Definition von Eigenwerten und Eigenvektoren . . . 258
8.2 Das charakteristische Polynom . . . 264
8.3 Vielfachheiten und Diagonalisierbarkeit . . . 268
8.3.1 Vielfachheiten . . . 268
8.3.2 Mehrfache Direkte Summen . . . 269
8.3.3 Diagonalisierbarkeit . . . 270

9 Skalarprodukte 274
9.1 Euklidische Vektorräume . . . 274
9.1.1 Reelle Bilinearformen . . . 274
9.1.2 Bilinearformen als Matrizen . . . 275
9.1.3 Reelle Skalarprodukte und Normen . . . 277
9.2 Unitäre Vektorräume . . . 280
9.2.1 Komplexe Sesquilinearformen . . . 280
9.2.2 Sesquilinearformen als Matrizen . . . 281
9.2.3 Komplexe Skalarprodukte und Normen . . . 284
9.3 Orthogonalität und Orthonormalisierung . . . 285
9.4 Polarisierung und Ungleichungen . . . 290
9.5 Matrixgruppen . . . 296
9.6 Das Hurwitz-Kriterium . . . 300
9.6.1 Basiswechsel für Sesquilinearformen . . . 300
9.6.2 Diagonale Matrizen . . . 302
9.6.3 Das Hurwitz-Kriterium . . . 303
9.7 Der Spektralsatz für selbstadjungierte Endomorphismen . . . 305
9.7.1 Isometrien und Standardräume . . . 306
9.7.2 Adjungierte und selbstadjungierte Endomorphismen . . . 307
9.7.3 Existenz von Eigenwerten . . . 310
9.7.4 Invariante Unterräume . . . 311
9.7.5 Der Spektralsatz . . . 312
9.7.6 Die Hauptachsentransformation . . . 313
9.7.7 Hauptachsentransformation und Skalarprodukte . . . 316
9.8 Der Spektralsatz für normale Endomorphismen . . . 318
9.8.1 Normale Endomorphismen . . . 319
9.8.2 Adjungierte und Matrizen in Orthonormalbasen . . . 319
9.8.3 Eigenräume normaler Endomorphismen . . . 321
9.8.4 Der Spektralsatz für normale Endomorphismen . . . 323

A Noether, Mathematik und Geschichte 326

B Kommutativität und Assoziativität 328
B.1 Benachbarte Vertauschungen . . . 328
B.2 Anwendung auf kommutative Produkte . . . 331
B.3 Das allgemeine Assoziativgesetz . . . 332
B.4 Klammerungen als Bäume . . . 334

Kapitel 0

Vorwort

0.1 Die Besonderheit der Mathematik

0.1.1 Die Rolle der Beweise

Im Gegensatz zu den Naturwissenschaften kann die Mathematik keine Gegenstände der Welt als ihr Forschungsobjekt auszeichnen.

So richtig gut funktioniert das in keiner Naturwissenschaft, aber eine Biologin die befragt wird, was ihr Forschungsobjekt sei, kann zumindest versuchen auf Pflanzen und Tiere zu zeigen. Eine Physikerin kann die Newtonschen Gesetze immerhin anhand von Billiardkugeln veranschaulichen. Aber eine Mathematikerin wird sich schwertun einen Gegenstand zu finden der den Primzahlen entspricht.

Diese simple Intuition ist natürlich philosophisch sehr viel komplexer und diskutabel, denn auch die Newtonschen Gesetze, oder die Evolutionstheorie sind natürlich selber keine Gegenstände in der Welt.

Dennoch gibt es eine wichtige Konsequenz: Die Naturwissenschaften können letztlich Theorien durch Experimente überprüfen. Die (falsche) Behauptung, dass eine fallende Kugel im Vakuum schneller fällt je schwerer sie ist, lässt sich (mit erheblichem Aufwand, ein geeignetes Vakuum zu finden) prinzipiell testen und widerlegen. Diese Widerlegung durch ein Experiment nennt man *Falsifikation*. Auch hier gibt es philosophische Feinheiten, die zeigen, dass diese Falsifikation ganz so simpel wie sie scheint doch nicht ist. Es bleibt aber, dass die Naturwissenschaften das Experiment als fundamentalen Teil der Forschung haben.

Die Mathematik hat solche Experimente nicht. Natürlich könnte man die falsche Behauptung $2 + 2 = 5$ dadurch widerlegen, dass man in einen leeren Beutel zunächst 2 Kartoffeln und dann nochmal 2 Kartoffeln legt und dann nachzählt und feststellt, dass nun 4 Kartoffeln im Beutel liegen.[1] Die wahre Aussage dass $2 + 2 = 4$ gilt wird aber nicht deshalb geglaubt, weil wiederholte Experimente wie das mit den Kartoffeln stets die Aussage bestätigt haben. Das sieht man zum einen daran, dass eine Aussage wie

$$100000000000000000000000000 + 1 = 100000000000000000000000001\,.$$

wohl noch nie getestet wurde, sie aber dennoch geglaubt wird. Andererseits würde kaum jemand die Wahrheit von 2+2=4 anzweifeln wenn in einem Beutel in den man 2 Kartoffeln und dann nochmal 2 Kartoffeln gelegt hat tatsächlich 5 Kartoffeln liegen würden. Vielmehr würden die aller meisten davon ausgehen, dass man sich verzählt habe, der Beutel zu Beginn doch nicht leer sei, das Experiment sabotiert wurde etc.

[1] Bei der Durchführung dieses Experiments wurden keine Kartoffeln verletzt. Die Mathematik ist und bleibt die einzige Wissenschaft, in der man mit Kartoffeln experimentieren darf, ohne dafür einen Ethikantrag stellen zu müssen.

Diese Schwierigkeit und Besonderheit der Mathematik ist spätestens seit der griechischen Antike bekannt. Sie inspirierte Philosophen von Platon zu René Descartes über Immanuel Kant und dem in Jena wirkenden Gottlob Frege in die Gegenwart mit Penelope Maddy. Die Philosophiegeschichte ist voll von Versuchen zu klären, was mathematische Wahrheit überhaupt sei. Wir werden hier nun nicht weiter darauf eingehen und verweisen an entsprechende Vorlesungen der Philosophischen Fakultät.

Das antike Griechenland verstand nicht nur das Problem sondern präsentierte auch eine Lösung: Statt Experimente nutzt die Mathematik strenge Argumente um Wahrheit zu finden. Dabei entwickelte die Mathematik Standards dazu was ein gutes mathematisches Argument ausmacht und wie dieses von Intuition und Bauchgefühl zu unterscheiden ist.

Während bis in das 19. Jahrhundert hinein die auf Euklid zurückgehende Auffassung vorherrschte, dass ein rigoroses Argument letztlich eine geometrische Konstruktion sei, setzte sich in der Moderne die gegenläufige Auffassung durch, dass mathematische Argumente dann besonders überzeugend sind, wenn sie logische, womöglich sogar formal-logische Argumente sind.

Diese Besonderheit der Mathematik erklärt ihren besonderen Fokus auf Rigorosität, Präzision und Korrektheit.

0.1.2 Historisches

So wie die Physik hat auch die Mathematik Ende des 19. Jahrhunderts und Anfang des 20. Jahrhunderts tiefgreifende wissenschaftliche Revolutionen erlebt. Während die Revolutionen in der Physik mit den popkulturell bekannten Namen von Einstein, Schrödinger und Heisenberg verbunden sind, bleiben die ähnlich fundamentalen Umwälzungen in der Mathematik oft weniger sichtbar und erscheinen bisweilen gesichtslos.

Dabei war die Mathematik dieser Zeit alles andere als randständig: Insbesondere Göttingen entwickelte sich zu einem der bedeutendsten Zentren mathematischer Forschung weltweit. Namen wie David Hilbert, Felix Klein oder Emmy Noether stehen exemplarisch für eine Phase außergewöhnlicher intellektueller Dichte.

Die Neuerungen in der Mathematik selbst führten zu einer zunehmenden Abstraktion. Begriffe die wir in dieser Vorlesung kennenlernen, wie Vektorraum, Gruppe oder Ring wurden in ihrer heutigen Form herausgearbeitet. Diese Abstraktion war dabei nicht Selbstzweck, sondern erwies sich als außerordentlich fruchtbar: Sie ermöglichte eine Vielzahl neuer Einsichten und Entwicklungen, die aus der modernen Mathematik kaum wegzudenken sind.

Das Verständnis des abstrakten Vektorraumbegriffs und des abstrakten Gruppenbegriffs war zugleich Motor und Resultat dieses Fortschritts.

Exemplarisch dazu kann man die Mathematikerin Emmy Noether herausgreifen. Ihr Wirken war nicht nur für die abstrakte Algebra von tiefer Bedeutung sondern spielte auch für die Entwicklung der allgemeinen Relativitätstheorie und der Quantenmechanik eine nachhaltige Rolle. Im Anhang finden sich weitere Informationen zu ihrem bewegten Leben.

Da die Schulmathematik diese tiefgreifenden Veränderungen in der Mathematik nur unvollständig durchlaufen bzw. verarbeitet hat ist der Grad der Abstraktion und des Formalismus in der Hochschulmathematik selbst für mathematisch interessierte Studierende häufig ein Kulturschock.

Daher werde ich auch immer wieder historische Zusammenhänge beleuchten. Um eine Reinwaschung ebendieser Geschichte zu verhindern ist es dabei leider auch unabdingbar ebenfalls auf historische Verbrechen einzugehen, die mit diesen historischen Zusammenhängen eng verwoben sind.



Abbildung 1: **Emmy Noether** (1882–1935), eine der bedeutendsten Mathematikerinnen des 20. Jahrhunderts. Ihre Arbeiten zur abstrakten Algebra und Symmetrie hatten tiefgreifenden Einfluss auf die moderne Mathematik und Physik.

Quelle: https://commons.wikimedia.org/wiki/File:Emmy_Noether_(3x4_cropped).jpg. Publisher: Mathematical Association of America, Brooklyn Museum, Agnes Scott College.

Kapitel 1

Grundlagen

1.1 Klassische Logik

Logik war als Theorie der richtigen Argumentation seit der Antike bekannt und von Aristoteles standardisiert. Mit der neuen Aufgabe als Grundlage für mathematische Beweisführung veränderte sich auch die Logik fundamental.

Wir werden uns hier aus didaktischen Gründen nicht die moderne formale Logik in ihrer vollen Pracht und Komplexität erarbeiten, sondern eine vereinfachte, aber dennoch wirkmächtige Form darstellen.

Betrachten wir einige logische Argumente in einer Form, die dem Verständnis von Aristoteles nahekommt.

Prämisse 1 Alle Menschen sind sterblich.

Prämisse 2 Sokrates ist ein Mensch.

Konklusion Sokrates ist sterblich.

Aus den beiden Prämissen, also Annahmen, wird die Konklusion, also die Schlussfolgerung, abgeleitet. Dieses Argument könnte man vereinfacht auch so darstellen:

$$\frac{\begin{array}{c}\text{Alle Menschen sind sterblich}\\ \text{Sokrates ist ein Mensch}\end{array}}{\text{Sokrates ist sterblich}}$$

Der Ursprung der Logik als Wissenschaft lässt sich vielleicht auf die Erkenntnis zurückführen, dass wir zum Verständnis eines Arguments gar nicht wissen müssen, wer oder was ein *Sokrates* ist. Außerdem müssen wir nicht wissen, was *Menschen* sind, und schließlich auch nicht, was *sterblich* bedeutet.

Das Argument funktioniert genauso, wenn man schreibt

$$\frac{\begin{array}{c}\text{Alle Beamten sind langsam}\\ \text{Platon ist ein Beamter}\end{array}}{\text{Platon ist langsam}}$$

Wir können uns sogar völlig unbekannte Quatsch-Begriffe benutzen:

$$\frac{\begin{array}{c}\text{Alle Simsalabims sind fluselmutig}\\ \text{Quirinella ist ein Simsalabim}\end{array}}{\text{Quirinella ist fluselmutig}}$$

Nun erschließt sich uns zwar nicht mehr die Bedeutung der Aussagen, aber der Schluss bleibt stimmig. Dies führt dazu, dass man Platzhalter oder Variablen benutzen kann:

$$\frac{\begin{array}{c}\text{Alle A sind X}\\ \text{B ist ein A}\end{array}}{\text{B ist X}}$$

Leitbeispiel 1.1.1 (Logik im Labor)**.** Diese Schlussformen sind keine philosophische Antiquität: Jeder physikalische Schluss benutzt sie. Als Leitbeispiel begleitet uns deshalb ein Szenario aus dem Praktikum.

$$\frac{\begin{array}{c}\text{Alle Metalle leiten Strom}\\ \text{Kupfer ist ein Metall}\end{array}}{\text{Kupfer leitet Strom}}$$

Das ist exakt die Sokrates-Form von oben — nur mit anderem Inhalt. Und genau darum geht es: Ob dieser Schluss trägt, hängt nicht davon ab, ob wir etwas von Festkörperphysik verstehen. Die *Form* garantiert: *Wenn* beide Prämissen wahr sind, *dann* ist auch die Konklusion wahr. Ob die Prämissen wahr sind (leiten wirklich alle Metalle?), ist dagegen eine empirische Frage — dafür ist das Labor zuständig, nicht die Logik. Diese Arbeitsteilung zwischen Form und Inhalt ist die Kernidee des ganzen Kapitels. Wir spielen sie im Folgenden an jeder Schlussform einmal im Labor durch.

Wir betrachten nun ein sehr ähnliches typisches Argument.

Prämisse 1 Alle Philosophen sind Denker.

Prämisse 2 Alle Denker sind Menschen.

Konklusion Alle Philosophen sind Menschen.

Dieses Argument ist ein klassisches Beispiel für den sogenannten *Barbara*-Syllogismus.[1] Auch hier können wir die konkrete Bedeutung vollständig austauschen:

$$\frac{\begin{array}{c}\text{Alle A sind B}\\ \text{Alle B sind C}\end{array}}{\text{Alle A sind C}}$$

Ein zweites Beispiel zeigt eine andere Struktur, nämlich eine partikulare Aussage:

Prämisse 1 Alle Katzen sind Säugetiere.

Prämisse 2 Einige Haustiere sind Katzen.

Konklusion Einige Haustiere sind Säugetiere.

[1] Ich erlaube mir hier eine kleine Ergänzung zu dem Ursprung der Namen der Syllogismen: Die Namen wie *Barbara*, *Celarent*, *Darii* usw. stammen aus der mittelalterlichen Logik. Sie sind Merkwörter, in denen die Vokale die Struktur des Schlusses kodieren: *A* steht für universell bejahende Aussagen („Alle A sind B“), *E* für universell verneinende, *I* für partiell bejahende und *O* für partiell verneinende.

Das obige Argument hat die Form A–A–A, also zwei universell bejahende Prämissen und eine universell bejahende Konklusion. Als Merkregel hat man sich dann dafür den Namen Barbara ausgedacht, denn dieser hat die drei A's als seine Vokale.

Auch dies lässt sich formal darstellen als:

$$\frac{\begin{array}{c}\text{Alle A sind B}\\ \text{Einige C sind A}\end{array}}{\text{Einige C sind B}}$$

Leitbeispiel 1.1.2 (Logik im Labor: Ketten und Teilaussagen)**.** Beide Formen tragen physikalisches Gewicht. Die Barbara-Kette stapelt Klassifikationen:

$$\frac{\begin{array}{c}\text{Alle Elektronen sind Leptonen}\\ \text{Alle Leptonen sind Fermionen}\end{array}}{\text{Alle Elektronen sind Fermionen}}$$

So vererben sich Eigenschaften entlang von Begriffshierarchien: Was für alle Fermionen gilt (etwa das Pauli-Prinzip), gilt automatisch auch für Elektronen. Ob Sie wissen, was ein Lepton oder das Pauli-Prinzip ist, ist dabei übrigens absichtlich egal — genau wie bei den Simsalabims: Der Schluss trägt durch seine Form, nicht durch Fachwissen.

Die partikulare Form steckt in jeder Stichprobe:

$$\frac{\begin{array}{c}\text{Alle Edelgase sind reaktionsträge}\\ \text{Einige Bestandteile der Luft sind Edelgase}\end{array}}{\text{Einige Bestandteile der Luft sind reaktionsträge}}$$

Bemerke den Unterschied in der Reichweite: Aus „alle“ und „einige“ folgt nur „einige“. Die Logik buchhaltet automatisch mit, wie viel Allgemeinheit ein Argument höchstens transportieren kann.

Ein anderes wichtiges Argument ist der sogenannte *Modus Tollens*.[2] Dieser gehört nicht zur klassischen Syllogistik des Aristoteles, da eine der Prämissen bereits eine Implikation ist.

Prämisse 1 Wenn es regnet, dann ist die Straße nass.

Prämisse 2 Die Straße ist nicht nass.

Konklusion Also regnet es nicht.

In abstrahierter Form schreibt man:

$$\frac{\begin{array}{c}\text{Wenn A, dann B}\\ \text{Es gilt nicht B}\end{array}}{\text{Es gilt nicht A}}$$

Leitbeispiel 1.1.3 (Logik im Labor: Modus Tollens ist das Experiment)**.** Im Praktikum:

$$\frac{\begin{array}{c}\text{Wenn der Stromkreis geschlossen ist, leuchtet die Lampe}\\ \text{Die Lampe leuchtet nicht}\end{array}}{\text{Der Stromkreis ist nicht geschlossen}}$$

[2] Der Name *Modus Tollens* kommt aus dem Lateinischen und bedeutet “die verneinende Schlussweise”. Er beschreibt die Regel, dass man aus einer Implikation und der Verneinung der Konsequenz auf die Verneinung der Voraussetzung schließen darf.

Und eine Stufe größer gedacht:

$$\frac{\begin{array}{c}\text{Wenn die Theorie stimmt, zeigt das Experiment den Effekt}\\ \text{Das Experiment zeigt den Effekt nicht}\end{array}}{\text{Die Theorie stimmt nicht}}$$

Das ist die *Falsifikation* aus dem Vorwort, destilliert auf ihre logische Form: Der Modus Tollens ist die Schlussweise, mit der Experimente Theorien widerlegen. (Dass in der Praxis oft eher eine Zusatzannahme fällt — „das Messgerät war wohl kaputt“ — ändert nichts an der Form, sondern nur daran, welche Prämisse man aufgibt.)

Diese verschiedenen Formen von Aussagen und Schlussweisen wurden bereits in der antiken Logik systematisch unterschieden, insbesondere bei Aristoteles, der unterschiedliche Figuren und Modi von Syllogismen klassifizierte.

Der Schritt hin zur klassischen Logik bestand wie oben dargestellt unter anderem darin zu erkennen, dass die Schlussfolgerung auch dann funktioniert, wenn man von der konkreten Bedeutung der beteiligten Begriffe absieht. Das Studium der Logik bestand dann darin verschiedene Schlussfolgerungsarten aufzustellen und zu studieren.

Beispiel 1.1.4 (Ein verführerischer Fehlschluss)**.** Nicht jede Schlussform ist gültig, und die ungültigen tragen Anzüge, die den gültigen zum Verwechseln ähnlich sehen. Vergleiche mit dem Modus Tollens:

$$\frac{\begin{array}{c}\text{Wenn die Sicherung durchgebrannt ist, leuchtet die Lampe nicht}\\ \text{Die Lampe leuchtet nicht}\end{array}}{\text{Die Sicherung ist durchgebrannt}}$$

Hier können beide Prämissen wahr sein und die Konklusion trotzdem falsch: Vielleicht ist einfach nur die Glühbirne kaputt. Dieser Fehlschluss (klassisch: „Bejahung der Konsequenz“) verwechselt „wenn A, dann B“ mit „wenn B, dann A“.

Aber Vorsicht: Trifft die kaputte Glühbirne nicht genauso den gültigen Modus Tollens von oben? Stromkreis geschlossen, Birne kaputt, Lampe aus — Konklusion falsch? Nein, und der Unterschied ist genau der Punkt: Mit kaputter Birne ist dort die *erste Prämisse* falsch, denn „Wenn der Stromkreis geschlossen ist, leuchtet die Lampe“ stimmt mit kaputter Birne nicht mehr. Ein gültiger Schluss verspricht nur: *Sind alle Prämissen wahr*, dann ist auch die Konklusion wahr. Ein ungültiger Schluss verspricht nicht einmal das — beim Fehlschluss oben sind beide Prämissen wahr und die Konklusion trotzdem falsch.

Daran sieht man zweierlei. Erstens: Um eine Schlussform als ungültig zu entlarven, genügt *ein einziges* inhaltliches Gegenbeispiel, in dem die Prämissen wahr sind und die Konklusion falsch ist. Zweitens: Es lohnt sich, Schlussformen mechanisch prüfen zu können, statt sich auf das Gefühl zu verlassen — genau das leistet die formale Aussagenlogik im nächsten Abschnitt.

1.2 Formale Aussagenlogik

Der Schritt zur formalen Logik lässt sich nun unter anderem dadurch kennzeichnen, dass diese starren Formen verlassen werden und auch die Wörter wie „wenn …dann“, „und“, „oder“ als eigenständige Objekte untersucht werden.

1.2.1 Syntax – Die Formeln der Aussagenlogik

Um logische Argumente systematisch untersuchen zu können, müssen wir zunächst festlegen, welche Ausdrücke wir überhaupt als *Formeln* zulassen.

Die grundlegende Idee der Aussagenlogik besteht darin, ganze Aussagen als unzerlegte Einheiten zu betrachten. Wir ersetzen konkrete Aussagen wie „Es regnet“ oder „Die Straße ist nass“ durch sogenannte *Aussagevariablen*, die wir meist mit Großbuchstaben wie $A, B, C, \ldots$ bezeichnen.

Aus solchen Aussagevariablen können wir mit Hilfe von logischen Verknüpfungen neue Aussagen zusammensetzen. Die wichtigsten dieser Verknüpfungen sind:

- $A \wedge B$ (gesprochen: „A und B“)
- $A \vee B$ (gesprochen: „A oder B“)
- $\neg A$ (gesprochen: „nicht A“)
- $A \to B$ (gesprochen: „wenn A, dann B“)

Diese Symbole erlauben es uns, komplexe Aussagen formal darzustellen.

Beispiel 1.2.1. Es stehe A für „Es regnet“ und B für „Die Straße ist nass“.

- Die Aussage „Wenn es regnet, dann ist die Straße nass“ wird zu

  $$A \to B,$$

  wobei A für „Es regnet“ und B für „Die Straße ist nass“ steht.
- Die Aussage „Es regnet und die Straße ist nass“ wird zu

  $$A \wedge B.$$

- Die Aussage „Es regnet nicht“ wird zu

  $$\neg A.$$

Auch einige der zuvor betrachteten Argumente lassen sich nun formal ausdrücken.

Beispiel 1.2.2 (Modus Tollens)**.** Das Argument

> Wenn es regnet, dann ist die Straße nass.
> Die Straße ist nicht nass.
> Also regnet es nicht.

lässt sich in der Aussagenlogik schreiben als

$$\frac{\begin{array}{c} A \to B \\ \neg B \end{array}}{\neg A}$$

Allerdings hat die Aussagenlogik auch klare Grenzen. Insbesondere können wir Aussagen wie „Alle Menschen sind sterblich“ oder „Einige Haustiere sind Katzen“ nicht direkt in dieser Sprache ausdrücken. Der Grund ist, dass solche Aussagen über *alle* oder *einige* Objekte sprechen und damit eine innere Struktur besitzen, die in der Aussagenlogik nicht sichtbar gemacht wird.

So können wir mit Aussagenlogik zwar den Schluss

$$\frac{\begin{array}{c}\text{Wenn } A\text{, dann } B.\\ \text{Nicht } B.\end{array}}{\text{Also nicht } A.}$$

formal korrekt erfassen, aber ein Argument wie

$$\frac{\begin{array}{c}\text{Alle } A \text{ sind } B.\\ \text{Alle } B \text{ sind } C.\end{array}}{\text{Also alle } A \text{ sind } C.}$$

entzieht sich dieser Darstellung, da die Beziehungen zwischen den einzelnen Objekten nicht sichtbar sind.

Um auch solche Aussagen präzise behandeln zu können, werden wir im weiteren Verlauf die Sprache erweitern. Dies führt uns zur *Prädikatenlogik*, in der wir über einzelne Objekte und ihre Eigenschaften sprechen können. Wir bleiben aber zunächst bei der Aussagenlogik um diese besser verstehen zu können.

Wir setzen uns nun näher mit den einzelnen logischen Symbolen auseinander.

Definition 1.2.3. Wir beginnen mit einer (unendlichen) Menge von atomaren Aussagen. Der Einfachheit halber bezeichnen wir die atomaren Aussagen mit lateinischen Großbuchstaben $A, B, C, \ldots$. Wir lernen nun Verknüpfungen (Junktoren) kennen, mit denen wir aus einfachen Aussagen kompliziertere bauen können. Die in diesem Prozess entstandenen (möglicherweise zusammengesetzten) Aussagen bezeichnen wir mit griechischen Kleinbuchstaben $\alpha, \beta, \ldots, \varphi, \psi, \ldots$.

Negation: Zunächst betrachten wir die Negation, also die Verneinung. Wenn α eine Aussage ist dann ist auch $\neg\alpha$ eine Aussage. Wir interpretieren $\neg\alpha$ als die Behauptung dass α falsch sei.

Konjunktion: Nun kommen wir zur Konjunktion, also dem logischen Und. Wenn α und β Aussagen sind, dann ist auch $\alpha \wedge \beta$ eine Aussage. Wir interpretieren $\alpha \wedge \beta$ als die Behauptung, dass sowohl α als auch β wahr sind. Zusammen mit der Negation können wir schon komplexe Aussagen formulieren:

$$(\neg\alpha \wedge \beta) \wedge (\neg\gamma)\,.$$

Bei zusammengesetzten Aussagen benutzen wir Klammern, um deutlich zu machen, worauf sich was bezieht. Das ist notwendig, denn

$$\neg\alpha \wedge \beta$$

und

$$\neg(\alpha \wedge \beta)$$

sind verschiedene Aussagen.

Aufgabe: Geben Sie den Aussagen α und β verschiedene alltägliche Bedeutungen. Machen Sie sich anhand von diesen Beispielen klar, dass $\neg\alpha \wedge \beta$ und $\neg(\alpha \wedge \beta)$ tatsächlich unterschiedliche Aussagen sind.

Disjunktion: Nun kommen wir zur Disjunktion, also dem logischen Oder. Wenn α und β Aussagen sind, dann ist auch $\alpha \vee \beta$ eine Aussage. Wir interpretieren $\alpha \vee \beta$ als die Behauptung, dass α oder β wahr ist. Dabei darf auch sowohl α als auch β wahr sein.

Aufgabe: Machen Sie sich klar, dass wenn α gilt, dann auch die Aussage $\alpha \vee \beta$ gilt.

Aufgabe: Weisen Sie den atomaren Aussagen A und B verschiedene alltägliche Bedeutungen zu. Vergleichen sie die resultierenden Bedeutungen von

$$(\neg A) \wedge (\neg B)$$

und

$$\neg(A \vee B)\,.$$

Was fällt ihnen dabei auf?

Implikation: Schließlich betrachten wir die Implikation, also das logische Wenn-Dann. Wenn α und β Aussagen sind, dann ist auch $\alpha \to \beta$ eine Aussage. Wir interpretieren $\alpha \to \beta$ als die Behauptung, dass wenn die Aussage α wahr ist, dann auch β wahr ist. Sollte α falsch sein, dann verstehen wir $\alpha \to \beta$ als wahr. Das liegt daran, dass wir $\alpha \to \beta$ nur dann als falsch betrachten, wenn obwohl α wahr ist, β falsch ist. Das hat die Konsequenz, dass wenn wir A als „2+2=5“ und B als „Berlin ist die Hauptstadt von Deutschland“ betrachten, die Aussage

$$A \to B$$

wahr ist.

Bi-Konditional: Wenn α und β Aussagen sind, dann ist auch $\alpha \leftrightarrow \beta$ eine Aussage. Wir interpretieren $\alpha \leftrightarrow \beta$ als die Behauptung, dass α genau dann wahr ist, wenn auch β wahr ist. Intuitiv bedeutet dies, dass α und β stets denselben Wahrheitswert haben.

Bemerkung 1.2.4. Es ist sehr wichtig zu verstehen, dass die Aussage $A \to B$ nicht behauptet, dass inhaltlich die Aussage B in irgendeiner Weise eine Konsequenz aus der Aussage A ist. Eine solche inhaltliche Implikation kann die formale Aussagenlogik nicht so einfach abbilden, da die formale Aussagenlogik die Aussagenvariablen A und B gerade nicht als weiter analysierbar betrachtet.

Generell muss man sich an die spezielle und formale Bedeutung der Symbole gewöhnen.

Leitbeispiel 1.2.5 (Die Sicherheitslogik des Lasers)**.** Als Leitbeispiel für diesen Abschnitt formalisieren wir eine Betriebsregel aus dem Laserlabor. Wir verwenden die atomaren Aussagen

L**:** „Der Laser läuft.“

S**:** „Die Schutztür ist geschlossen.“

K**:** „Die Kühlung ist aktiv.“

Die Sicherheitsregel

„Der Laser darf nur laufen, wenn die Schutztür geschlossen und die Kühlung aktiv ist“

wird zu der Formel

$$L \to (S \wedge K).$$

(Eine Vorschrift ist zunächst keine Behauptung — wir lesen sie hier als Aussage über den tatsächlichen Betrieb: Sie ist wahr, wenn sie nie verletzt wird.) Bemerke, wie viel Präzision schon die Formalisierung erzwingt: Das „nur wenn“ der Umgangssprache wird zu einer Implikation *von* L aus, nicht umgekehrt. Die Konkurrenzformel

$$(S \wedge K) \to L$$

würde etwas ganz anderes behaupten — nämlich dass der Laser laufen *muss*, sobald Tür und Kühlung in Ordnung sind. Genau das verspricht die Regel nicht. Und ganz im Sinne der letzten Bemerkung behauptet die Formel keinen inhaltlichen Zusammenhang zwischen Laser, Tür und Kühlung, sondern schließt nur bestimmte Kombinationen von Wahrheitswerten aus. Welche das sind, wird ihre Wahrheitswertetafel im nächsten Unterabschnitt beantworten.

1.2.2 Semantik – Die formale Bedeutung von Aussagen

Wahrheitswertetafeln

Bisher haben wir festgelegt, welche Ausdrücke wir als Formeln zulassen und wie wir aus einfachen Aussagen komplexe zusammensetzen können. Nun stellt sich die Frage, wie wir diesen Formeln eine *Bedeutung* zuweisen.

Die grundlegende Idee besteht darin, jeder Aussage einen Wahrheitswert zuzuordnen. Dabei unterscheiden wir zunächst zwei Möglichkeiten: „wahr“ und „falsch“.

Um zu beschreiben, wie sich die Wahrheitswerte komplexer Aussagen aus denen ihrer Bestandteile ergeben, verwenden wir sogenannte *Wahrheitswertetafeln.*

Definition 1.2.6 (Wahrheitswertetafeln)**.** Sei α eine Aussage und $A_1, \dots, A_n$ die in α vorkommenden atomaren Aussagen. Die *Wahrheitswertetafel* oder *Wahrheitswertetabelle* von α ist eine Tabelle

A_1	...	A_n	α

Wobei die Zeilen mit allen Kombinationen an Wahrheitswerten von $A_1, \dots, A_n$ (in den entsprechenden Spalten) aufgefüllt werden. In den Zeilen unter α trägt man dann den entsprechenden resultierenden Wahrheitswert ein.

Diese kann man auch als *Definition* der Bedeutung logischer Operatoren verstehen.
Die Negation ist also definiert über die Tabelle

A	$\neg A$
wahr	falsch
falsch	wahr

Das bedeutet: Ist A wahr, so ist $\neg A$ falsch, und ist A falsch, so ist $\neg A$ wahr.

Für die Konjunktion erhalten wir die folgende Definition:

A	B	$A \wedge B$
wahr	wahr	wahr
wahr	falsch	falsch
falsch	wahr	falsch
falsch	falsch	falsch

Die Aussage $A \wedge B$ ist also genau dann wahr, wenn sowohl A als auch B wahr sind.

Für die Disjunktion gilt:

A	B	$A \vee B$
wahr	wahr	wahr
wahr	falsch	wahr
falsch	wahr	wahr
falsch	falsch	falsch

Hier ist $A \vee B$ genau dann wahr, wenn mindestens eine der beiden Aussagen wahr ist.

Schließlich ergibt sich für die Implikation:

A	B	$A \to B$
wahr	wahr	wahr
wahr	falsch	falsch
falsch	wahr	wahr
falsch	falsch	wahr

Insbesondere ist zu beachten, dass $A \to B$ immer dann als wahr gilt, wenn A falsch ist.

Für das Bi-Konditional erhalten wir:

A	B	$A \leftrightarrow B$
wahr	wahr	wahr
wahr	falsch	falsch
falsch	wahr	falsch
falsch	falsch	wahr

Die Aussage $A \leftrightarrow B$ ist also genau dann wahr, wenn A und B denselben Wahrheitswert haben.

Numerische Darstellung. Oft ist es praktisch, anstelle von „wahr“ und „falsch“ die Werte 1 und 0 zu verwenden. Dabei steht

$$1 \quad \text{für wahr} \qquad \text{und} \qquad 0 \quad \text{für falsch.}$$

Die Wahrheitstafeln lassen sich dann entsprechend umschreiben. Zum Beispiel ergibt sich für die Konjunktion:

A	B	$A \wedge B$
1	1	1
1	0	0
0	1	0
0	0	0

Diese Darstellung ist besonders nützlich, wenn man formale oder algorithmische Methoden verwenden will. Ein weiterer Vorteil liegt darin, dass man durch „binäres Zählen“ alle Kombinationen von Wahrheitswerten systematisch aufzählen kann. Betrachte den folgenden Fall: Wir wollen die Tabelle für

A	B	C	D	E	$((\neg D \to (A \wedge B \wedge E)) \vee C) \to E$

ausfüllen. Hier gibt es viele Kombinationen, die man betrachten muss. Daher ist es leicht die Übersicht zu verlieren.
Aufgabe: Wie viele Kombinationen gibt es bzw. wie viele Zeilen müssen wir ausfüllen?

Ein systematischer Weg des Auffüllens geht so: Fülle in der ersten Zeile alle Spalten für Aussagenvariablen mit Nullen auf.

A	B	C	D	E	$((\neg D \to (A \wedge B \wedge E)) \vee C) \to E$
0	0	0	0	0	

danach zählen wir binär aufwärts, also

A	B	C	D	E	$((\neg D \to (A \wedge B \wedge E)) \vee C) \to E$
0	0	0	0	0	
0	0	0	0	1	
0	0	0	1	0	
0	0	0	1	1	
0	0	1	0	0	
⋮	⋮	⋮	⋮	⋮	
1	0	1	1	0	
1	0	1	1	1	
1	1	0	0	0	
⋮	⋮	⋮	⋮	⋮	
1	1	1	0	0	
1	1	1	0	1	
1	1	1	1	0	
1	1	1	1	1	

Und schließlich füllt man dann die Spalte für die zusammengesetzte Aussage auf. Für das Auffüllen dieser Spalte ist es sinnvoll die Aussage in Teile zu zerlegen.

Dies beansprucht schnell viel Platz, deshalb hat die folgende Tabelle eine sehr kleine Schriftgröße.

A	B	C	D	E	$(A \wedge B \wedge E)$	$(\neg D \to (A \wedge B \wedge E))$	$((\neg D \to (A \wedge B \wedge E)) \vee C)$	$((\neg D \to (A \wedge B \wedge E)) \vee C) \to E$
0	0	0	0	0				
0	0	0	0	1				
0	0	0	1	0				
0	0	0	1	1				
0	0	1	0	0				
⋮	⋮	⋮	⋮	⋮				
1	0	1	1	0				
1	0	1	1	1				
1	1	0	0	0				
⋮	⋮	⋮	⋮	⋮				
1	1	1	0	0				
1	1	1	0	1				
1	1	1	1	0				
1	1	1	1	1				

Leitbeispiel 1.2.7 (Die Sicherheitslogik des Lasers: die Wahrheitswertetafel)**.** Für die Betriebsregel $L \to (S \wedge K)$ aus Leitbeispiel 1.2.5 hat die Wahrheitswertetafel $2^3 = 8$ Zeilen. Binäres Zählen liefert sie systematisch:

L	S	K	$S \wedge K$	$L \to (S \wedge K)$
0	0	0	0	1
0	0	1	0	1
0	1	0	0	1
0	1	1	1	1
1	0	0	0	0
1	0	1	0	0
1	1	0	0	0
1	1	1	1	1

Diese Tafel *ist* die komplette Bedeutung der Regel: Sie verbietet genau die drei Zeilen mit dem Eintrag 0 — Laser an, aber Tür offen oder Kühlung aus. Alle anderen Kombinationen lässt sie zu, insbesondere alle vier Zeilen mit $L = 0$: Ein ausgeschalteter Laser erfüllt jede Betriebsregel. Das ist die Alltagsgestalt der Beobachtung, dass Implikationen mit falscher Prämisse wahr sind.

Definition 1.2.8 (Tautologien)**.** Eine Formel heißt *Tautologie*, wenn sie unabhängig von den Wahrheitswerten ihrer Variablen immer wahr ist.

Beispiel 1.2.9. Die Formel

$$A \vee \neg A$$

ist eine Tautologie. Denn unabhängig davon, ob A wahr oder falsch ist, ist stets mindestens einer der beiden Terme wahr.

A	$\neg A$	$A \vee \neg A$
wahr	falsch	wahr
falsch	wahr	wahr

Tautologien spielen eine zentrale Rolle in der Logik, da sie genau die Formeln sind, die unter allen möglichen Interpretationen gültig sind.

Beispiel 1.2.10. Die Formel

$$\neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B)$$

ist eine Tautologie.

Sie drückt aus, dass die Verneinung einer Oder-Aussage genau dann wahr ist, wenn beide Teilaussagen falsch sind.

Dies können wir mit einer Wahrheitswertetafel überprüfen:

A	B	$A \vee B$	$\neg(A \vee B)$	$\neg A \wedge \neg B$	$\neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B)$
wahr	wahr	wahr	falsch	falsch	wahr
wahr	falsch	wahr	falsch	falsch	wahr
falsch	wahr	wahr	falsch	falsch	wahr
falsch	falsch	falsch	wahr	wahr	wahr

Da in der letzten Spalte stets „wahr“ steht, handelt es sich um eine Tautologie.

Tautologien erlauben es uns auch, ganze Schlussmuster der Logik zu untersuchen.

Beispiel 1.2.11 (Modus Tollens)**.** Wir betrachten das bereits bekannte Schlussmuster

> Wenn es regnet, dann ist die Straße nass.
> Die Straße ist nicht nass.
> Also regnet es nicht.

In der Aussagenlogik wird dieses Argument dargestellt durch

$$\frac{\begin{array}{c} A \to B \\ \neg B \end{array}}{\neg A}$$

Um zu überprüfen, dass dieses Schlussmuster immer korrekt ist, betrachten wir die Formel

$$((A \to B) \wedge \neg B) \to \neg A.$$

Diese Formel sagt: Wenn sowohl $A \to B$ als auch $\neg B$ gelten, dann gilt auch $\neg A$.
Wir erhalten die folgende Wahrheitswertetafel:

A	B	$A \to B$	$\neg B$	$(A \to B) \wedge \neg B$	$\neg A$	$((A \to B) \wedge \neg B) \to \neg A$
wahr	wahr	wahr	falsch	falsch	falsch	wahr
wahr	falsch	falsch	wahr	falsch	falsch	wahr
falsch	wahr	wahr	falsch	falsch	wahr	wahr
falsch	falsch	wahr	wahr	wahr	wahr	wahr

Auch hier ist die letzte Spalte in jeder Zeile wahr. Also handelt es sich um eine Tautologie.

Damit sehen wir: Der Modus Tollens ist ein in der Aussagenlogik allgemeingültiges Schlussmuster.

Beispiel 1.2.12 (Junktoren als Schaltkreise)**.** Eine zweite Intuition für die Junktoren kommt aus der Elektronik. Interpretiere 1 als „Spannung liegt an“ und 0 als „keine Spannung“. Dann sind die Junktoren Bauteile, sogenannte *Gatter*:

- $\wedge$ ist eine Reihenschaltung zweier Schalter: Strom fließt nur, wenn beide geschlossen sind.
- $\vee$ ist eine Parallelschaltung: Strom fließt, sobald mindestens einer geschlossen ist.
- $\neg$ ist ein Umkehrglied, das anliegende Spannung wegschaltet und fehlende Spannung anlegt.

Eine zusammengesetzte Formel ist in diesem Bild ein Schaltkreis, und ihre Wahrheitswertetafel ist sein vollständig vermessenes Ein-Ausgabe-Verhalten: links alle möglichen Eingangssignale, rechts das jeweilige Ausgangssignal.

Zwei zentrale Begriffe werden damit greifbar. Eine *Tautologie* ist ein Schaltkreis, dessen Ausgang konstant auf 1 liegt, egal was man anlegt. Und zwei Formeln mit denselben Tafeln (dafür fällt gleich der Begriff *logisch äquivalent*) sind Schaltkreise, die an ihren Klemmen ununterscheidbar sind — man darf den einen durch den anderen ersetzen, zum Beispiel durch den billigeren mit weniger Gattern. Dass sich alle Junktoren aus wenigen Gattertypen aufbauen lassen, ist übrigens der Grund, warum Computer überhaupt rechnen können: Ein Prozessor ist Aussagenlogik in Silizium.

1.2.3 Das Folgerungssymbol „⇒“, logische Äquivalenz und nützliche Regeln

Bisher haben wir vor allem formale Aussagen selber studiert und betrachtet unter welchen Wahrheitswerten für die atomaren Aussagen diese als „wahr“ gelten.

Nun betrachten wir die verwandte aber unterschiedliche Frage wie man aus (möglicherweise formalen) Aussagen schlussfolgern kann.

Wir untersuchen also Sätze wie:

„*Wenn die Aussage $A \vee B$ und die Aussage $B \vee C$ gelten, dann gilt die Aussage B oder die Aussage $A \wedge C$.*“

Ein Versuch der Formalisierung würde möglicherweise auf die Formel

$$((A \vee B) \wedge (B \vee C)) \to (B \vee (A \wedge C))$$

stoßen.

Es gibt jedoch einen wichtigen Unterschied zwischen diesen beiden Ausdrücken. Der erste ist eine konkrete Behauptung darüber was wir tatsächlich aus Aussagen schlussfolgern können, während der zweite lediglich eine abstrakte formale Formel ist.

Wir machen den Unterschied zunächst dadurch deutlich, dass wir für letztere logische Symbole $\wedge$, $\vee$ usw. benutzen und für erstere die Wörter „und“, „oder“ usw. verwenden.

Aus den Syllogismen kennen wir bereits ein Symbol für die Schlussfolgerung und zwar die horizontale Linie. Dieses hatten wir dort ebenfalls unterschieden von Implikationen in den verwendeten Aussagen. Dies wird besonders deutlich bei dem bereits betrachteten Modus Tollens:

$$\frac{\begin{array}{c}\text{Wenn A, dann B}\\ \text{Es gilt nicht B}\end{array}}{\text{Es gilt nicht A}}$$

Hier spielt das „Wenn A, dann B“ in der ersten Zeile eine andere Rolle als die horizontale Linie als Schlussfolgerung.

Da wir sehr oft mit Schlussfolgerungen arbeiten werden führen wir ein Symbol dafür ein. Anstelle von „Aus A folgt B“ schreiben wir auch das Folgerungssymbol

$$A \Rightarrow B.$$

Dieses dient lediglich als Abkürzung. Für die anderen Bestandteile des Argumentierens wie „und“ und „oder“ begnügen wir uns mit den Wörtern die uns die natürliche Sprache bietet.

Dabei ist der Unterschied zum Junktor „$\to$“ wichtig. Der Ausdruck $A \to B$ ist selbst wieder eine formale Aussage. Dagegen bedeutet $A \Rightarrow B$, dass immer dann, wenn A wahr ist, auch B wahr ist.

Zwischen beiden Begriffen besteht ein enger Zusammenhang. Genau dann, wenn $A \to B$ immer wahr ist, folgt aus A auch B.

Theorem 1.2.13. *Für zusammengesetzte Aussagen α und β gilt*

$$\alpha \Rightarrow \beta \quad \textit{genau dann, wenn} \quad \alpha \to \beta \textit{ eine Tautologie ist.}$$

Beweis. Nach der Wahrheitstafel der Implikation ist $\alpha \to \beta$ genau dann falsch, wenn α wahr und β falsch ist. Also ist $\alpha \to \beta$ genau dann in jeder Zeile wahr, wenn es keine Zeile gibt, in der α wahr, aber β falsch ist. Das ist genau die Bedeutung von $\alpha \Rightarrow \beta$. □

Bemerkung 1.2.14. Die Symbole $\to$ und $\Rightarrow$ haben also ähnliche, aber nicht identische Bedeutungen. Der Ausdruck $\alpha \to \beta$ ist eine Aussage innerhalb unserer formalen Sprache. Dagegen beschreibt $\alpha \Rightarrow \beta$ ein Verhältnis zwischen zwei Aussagen.

Oft wollen wir aus mehreren gleichzeitig gegebenen Voraussetzungen eine Folgerung ziehen. Mehrere Voraussetzungen fassen wir dabei mit dem logischen Und zusammen. Statt

$$\alpha \to \beta \qquad \text{und} \qquad \alpha$$

schreiben wir also eine einzige Aussage

$$(\alpha \to \beta) \wedge \alpha.$$

Dadurch können wir auch Schlussregeln als Regeln zwischen einzelnen Formeln notieren.

Leitbeispiel 1.2.15 (Die Sicherheitslogik des Lasers: eine erste Folgerung)**.** Was folgt, wenn die Betriebsregel eingehalten wird *und* der Laser läuft? Wir behaupten

$$\big(L \to (S \wedge K)\big) \wedge L \;\Rightarrow\; S \wedge K.$$

Um das zu prüfen, genügt nach dem Satz über Tautologien und Folgerungen ein Blick in die Wahrheitswertetafel aus Leitbeispiel 1.2.5: Gesucht sind die Zeilen, in denen $L \to (S \wedge K)$ und L gleichzeitig wahr sind. Das ist einzig die letzte Zeile, und dort ist auch $S \wedge K$ wahr. Keine Zeile erfüllt also die Voraussetzung und verletzt die Folgerung.

Die Lesart auf der Metaebene: Wer weiß, dass die Regel gilt und der Laser läuft, darf schließen, dass die Tür geschlossen und die Kühlung aktiv ist. Das $\Rightarrow$ lebt dabei außerhalb der formalen Sprache — es ist unser Urteil *über* die Formeln, gewonnen aus ihrer Tafel. (Das verwendete Schlussmuster ist der Modus Ponens aus der folgenden Regelsammlung.)

Definition 1.2.16 (Logische Äquivalenz)**.** Wir nennen die Aussagen α und β logisch äquivalent, wenn sie für jede Zuweisung von Wahrheitswerten an die atomaren Aussagen denselben resultierenden Wahrheitswert haben. In diesem Fall schreiben wir

$$\alpha \Leftrightarrow \beta.$$

Das ist gleichbedeutend damit, dass sowohl $\alpha \Rightarrow \beta$ als auch $\beta \Rightarrow \alpha$ gilt.

Bemerkung 1.2.17. Logisch äquivalente Aussagen dürfen in Rechnungen und Beweisen gegenseitig durch einander ersetzt werden.

Die logische Äquivalenz lässt sich durch eine Wahrheitswertetafel beweisen: Zwei Formeln sind logisch äquivalent, wenn in einer gemeinsamen Wahrheitswertetafel die entsprechenden Spalten dieselben Einträge haben.

Für unsere Zwecke genügt zunächst eine kleine Sammlung nützlicher Regeln. Sie bildet kein vollständiges formales Beweissystem. Sie erlaubt uns aber, viele Aussagen bequem umzuformen oder aus stärkeren Aussagen einfachere Folgerungen zu gewinnen.

Theorem 1.2.18 (Nützliche Umformungs- und Folgerungsregeln)**.** *Seien α, β und γ beliebige Aussagen.*

1. ***Umformungsregeln.***
   - $\alpha \to \beta \Leftrightarrow \neg\alpha \vee \beta$
   - *Doppelnegationselimination:* $\neg\neg\alpha \Leftrightarrow \alpha$
   - *Die De Morgan'schen Regeln:* $\neg(\alpha \wedge \beta) \Leftrightarrow \neg\alpha \vee \neg\beta$ *und* $\neg(\alpha \vee \beta) \Leftrightarrow \neg\alpha \wedge \neg\beta$
   - *Die Assoziativgesetze:* $(\alpha \wedge \beta) \wedge \gamma \Leftrightarrow \alpha \wedge (\beta \wedge \gamma)$ *und* $(\alpha \vee \beta) \vee \gamma \Leftrightarrow \alpha \vee (\beta \vee \gamma)$
   - *Die Kommutativgesetze:* $\alpha \wedge \beta \Leftrightarrow \beta \wedge \alpha$ *und* $\alpha \vee \beta \Leftrightarrow \beta \vee \alpha$
   - *Die Distributivgesetze:* $\alpha \wedge (\beta \vee \gamma) \Leftrightarrow (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$ *und* $\alpha \vee (\beta \wedge \gamma) \Leftrightarrow (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$
2. ***Folgerungsregeln.***
   - *Und-Elimination:* $\alpha \wedge \beta \Rightarrow \alpha$ *und* $\alpha \wedge \beta \Rightarrow \beta$
   - *Modus Ponens:* $(\alpha \to \beta) \wedge \alpha \Rightarrow \beta$
   - *Modus Tollens:* $(\alpha \to \beta) \wedge \neg\beta \Rightarrow \neg\alpha$

Beweisskizze. Alle diese Regeln lassen sich mit Wahrheitstafeln überprüfen. Wir zeigen dies exemplarisch an wichtigen Beispielen.

1. **Elimination der Implikation.** Wir vergleichen die Spalten zu $\alpha \to \beta$ und $\neg\alpha \vee \beta$:

α	β	$\alpha \to \beta$	$\neg\alpha$	$\neg\alpha \vee \beta$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	1	0	1

   Die Spalten zu $\alpha \to \beta$ und $\neg\alpha \vee \beta$ stimmen überein. Also gilt

$$\alpha \to \beta \Leftrightarrow \neg\alpha \vee \beta.$$

2. **Assoziativgesetze** Wir zeigen

$$(\alpha \vee \beta) \vee \gamma \;\Leftrightarrow\; \alpha \vee (\beta \vee \gamma).$$

Die entsprechende Aussage für das logische Und ist eine Übungsaufgabe.

Betrachten wir die beiden Wahrheitswertetafeln

α	β	γ	$(\alpha \vee \beta)$	$(\alpha \vee \beta) \vee \gamma$
0	0	0	0	0
0	0	1	0	1
0	1	0	1	1
0	1	1	1	1
1	0	0	1	1
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

und

α	β	γ	$(\beta \vee \gamma)$	$\alpha \vee (\beta \vee \gamma)$
0	0	0	0	0
0	0	1	1	1
0	1	0	1	1
0	1	1	1	1
1	0	0	0	1
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

Die entsprechenden Spalten haben dieselben Einträge, also gilt die behauptete Äquivalenz.

3. **Modus Ponens in Ein-Formel-Schreibweise.** Wir betrachten die Regel

$$(\alpha \to \beta) \wedge \alpha \Rightarrow \beta.$$

Nach Theorem 1.2.13 genügt es zu zeigen, dass

$$((\alpha \to \beta) \wedge \alpha) \to \beta$$

eine Tautologie ist.

α	β	$\alpha \to \beta$	$(\alpha \to \beta) \wedge \alpha$	$((\alpha \to \beta) \wedge \alpha) \to \beta$
0	0	1	0	1
0	1	1	0	1
1	0	0	0	1
1	1	1	1	1

Also ist die letzte Spalte stets wahr. Damit gilt

$$(\alpha \to \beta) \wedge \alpha \Rightarrow \beta.$$

4. Die übrigen Regeln werden auf dieselbe Weise überprüft. Ein Teil davon eignet sich gut als Übungsaufgabe.
   Aufgabe: Prüfen Sie das erste Distributivgesetz $\alpha \wedge (\beta \vee \gamma) \Leftrightarrow (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$ mit einer Wahrheitswertetafel (acht Zeilen, wie bei den Assoziativgesetzen).

□

Leitbeispiel 1.2.19 (Die Sicherheitslogik des Lasers: Regeln anwenden)**.** Zwei der Regeln, angewandt auf die Betriebsregel $L \to (S \wedge K)$ aus Leitbeispiel 1.2.5:

De Morgan im Alarmfall. Ein Wächter soll anschlagen, sobald die Sicherheitsbedingung $S \wedge K$ verletzt ist. Nach De Morgan gilt

$$\neg(S \wedge K) \Leftrightarrow \neg S \vee \neg K \ :$$

„nicht (Tür zu und Kühlung an)" heißt „Tür offen *oder* Kühlung aus". Der Alarm braucht also zwei Sensoren, von denen jeder einzeln auslösen darf — hier ist die Umformungsregel buchstäblich ein Verdrahtungsplan.

Eine Regel zerfällt in zwei. Mit den Regeln lässt sich außerdem

$$L \to (S \wedge K) \ \Leftrightarrow \ (L \to S) \wedge (L \to K)$$

nachrechnen (eine gute Übung: Elimination der Implikation, dann Distributivgesetz). Die eine Betriebsregel ist also gleichwertig zu zwei getrennten Regeln: „Laser nur bei geschlossener Tür" und „Laser nur bei aktiver Kühlung". Genau das will man wissen, wenn zwei verschiedene Prüfstellen je eine der Bedingungen kontrollieren.

Wir betrachten jetzt ein Beispiel, wie man mittels der bisherigen Umformungs- und Ableitungsregeln weitere solche Regeln herleiten kann. Ein sehr wichtiges Beispiel ist die sogenannte Kontraposition.

Theorem 1.2.20 (Kontraposition)**.** *Für beliebige Aussagen α und β gilt*

$$\alpha \to \beta \Leftrightarrow \neg\beta \to \neg\alpha.$$

Beweis. Wir formen die linke Aussage schrittweise mit unseren Umformungsregeln um. Es gilt

$$\alpha \to \beta \Leftrightarrow \neg\alpha \vee \beta$$

nach der Elimination der Implikation.

Nun vertauschen wir die beiden Teilaussagen mit dem Kommutativgesetz für $\vee$ und erhalten

$$\neg\alpha \vee \beta \Leftrightarrow \beta \vee \neg\alpha.$$

Auf die rechte Seite wenden wir nun erneut die Elimination der Implikation an, und zwar rückwärts. Da

$$\neg\beta \to \neg\alpha \Leftrightarrow \neg(\neg\beta) \vee \neg\alpha$$

gilt, folgt mit der doppelten Negation

$$\neg(\neg\beta) \vee \neg\alpha \Leftrightarrow \beta \vee \neg\alpha.$$

Also ist insgesamt

$$\alpha \to \beta \Leftrightarrow \neg\beta \to \neg\alpha.$$ □

Bemerkung 1.2.21. Die Kontraposition ist eines der wichtigsten Schlussmuster der Mathematik. Sie erlaubt es, eine Implikation

$$\alpha \to \beta$$

dadurch zu beweisen, dass man stattdessen die äquivalente Aussage

$$\neg\beta \to \neg\alpha$$

zeigt.

Oft ist dies einfacher als ein direkter Beweis. Wenn die Aussage β schwer direkt aus α herzuleiten ist, kann es viel übersichtlicher sein zu zeigen, dass aus dem Scheitern von β notwendigerweise auch das Scheitern von α folgt.

Dieses Prinzip begegnet uns in der Mathematik immer wieder und bildet eine wichtige Grundlage vieler indirekter Beweise.

Leitbeispiel 1.2.22 (Die Sicherheitslogik des Lasers: die Sicht der Prüferin)**.** Kontraposition, angewandt auf die Betriebsregel:

$$L \to (S \wedge K) \quad \Leftrightarrow \quad \neg(S \wedge K) \to \neg L \quad \Leftrightarrow \quad (\neg S \vee \neg K) \to \neg L.$$

Dieselbe Regel, zwei Blickrichtungen: Der Bediener liest sie vorwärts („läuft der Laser, dann ist alles gesichert“), die Sicherheitsprüferin rückwärts („ist die Tür offen oder die Kühlung aus, dann ist der Laser aus“). Beide prüfen logisch exakt dasselbe — aber je nach Situation ist eine der Richtungen viel leichter zu kontrollieren. Genau diese Wahlfreiheit macht die Kontraposition auch in Beweisen so wertvoll, wie die nächsten beiden Beispiele zeigen.

Beispiel 1.2.23 (Teilbarkeit von Quadraten)**.** Wir wollen zeigen, dass wenn n^2 durch 2 teilbar ist, dass dann auch n durch zwei teilbar ist.

Ein direkter Beweis müsste aus der Teilbarkeit von n^2 durch 2, also aus $n^2 = 2 \cdot k$ für irgendeine ganze Zahl k, schlussfolgern, dass auch n durch 2 teilbar ist. Das ist möglich, aber mit unseren Mitteln nicht leicht: Jeder direkte Weg benutzt im Kern die eindeutige Primfaktorzerlegung, die uns an dieser Stelle noch nicht zur Verfügung steht.

Deutlich einfacher ist ein indirekter Beweis über Kontraposition. Wir zeigen also, dass wenn n nicht durch 2 teilbar ist, dass dann auch n^2 nicht durch 2 teilbar sein kann. Sei also n nicht durch 2 teilbar. Dann ist $n = 2 \cdot m + 1$ für eine ganze Zahl m. Daher ist

$$\begin{aligned} n^2 &= (2 \cdot m + 1)^2 \\ &= (2 \cdot m)^2 + 2 \cdot (2 \cdot m) \cdot 1 + 1^2 \\ &= 4 \cdot m^2 + 4 \cdot m + 1 \\ &= 2 \cdot (2 \cdot m^2 + 2 \cdot m) + 1\,. \end{aligned}$$

Mit $k = 2 \cdot m^2 + 2 \cdot m$ erhalten wir also $n^2 = 2 \cdot k + 1$ für eine ganze Zahl k. Daher ist n^2 nicht durch 2 teilbar.

Dieses Beispiel verdeutlicht, dass Kontraposition manchmal Beweise deutlich einfacher macht.

Beispiel 1.2.24 (Die Irrationalität von $\sqrt{2}$)**.** Wir wollen zeigen, dass aus

$$x^2 = 2$$

folgt, dass x nicht rational ist.

Wir zeigen sogar etwas Allgemeineres: Ist x^2 eine ganze Zahl aber x nicht ganzzahlig, dann ist x bereits irrational.

Aufgabe: Warum folgt daraus insbesondere die Irrationalität von $\sqrt{2}$?

Mit Theorem 1.2.20 genügt es, die kontrapositive Aussage zu zeigen. Wir verwenden die Kontraposition aber nicht direkt. Unsere Aussage hat die Form $(P \wedge Q) \to R$. Diese Form ist — nach Kontraposition und einem weiteren Argument — äquivalent zu $(\neg R \wedge Q) \to \neg P$.

Aufgabe: Rechnen Sie diese Äquivalenz mit den Umformungsregeln nach.

Wir zeigen also: Ist x rational, aber keine ganze Zahl, so kann x^2 keine ganze Zahl sein.

Sei also x rational und keine ganze Zahl. Dann gibt es ganze Zahlen a und b mit $b \neq 0$, so dass

$$x = \frac{a}{b}.$$

Wir dürfen außerdem annehmen, dass der Bruch vollständig gekürzt ist, also

$$\gcd(a, b) = 1.$$

Dabei bezeichnet $\gcd(a, b)$ den *größten gemeinsamen Teiler* von a und b; dass man jeden Bruch vollständig kürzen kann, nehmen wir aus der Schule mit.

Da x keine ganze Zahl ist, ist b kein Teiler von a. Insbesondere gilt dann $|b| > 1$. Also besitzt b einen Primfaktor p.

Weil $\gcd(a, b) = 1$ gilt, kann dieser Primfaktor p kein Teiler von a sein.

Nun ist

$$x^2 = \frac{a^2}{b^2}.$$

Aus $\gcd(a, b) = 1$ folgt auch

$$\gcd(a^2, b^2) = 1.$$

(Dieser Schritt ist die eigentliche Substanz des Beweises — er folgt unter anderem aus der eindeutigen Primfaktorzerlegung, die wir hier ebenfalls als Schulwissen ausleihen.) Insbesondere ist p ein Primfaktor von b^2, aber kein Primfaktor von a^2.

Daher kann b^2 den Zähler a^2 nicht teilen. Folglich ist

$$\frac{a^2}{b^2}$$

keine ganze Zahl. Also ist x^2 keine ganze Zahl.

Das beendet den Beweis.

Dieses Beispiel zeigt, dass die Kontraposition in mathematischen Beweisen oft eine sehr natürliche Strategie ist.

1.3 Prädikatenlogik

1.3.1 Die Schranken der Aussagenlogik

Die Aussagenlogik ist aus mehreren Gründen keine gute Grundlage für die Mathematik. Diese Gründe lassen sich damit zusammenfassen, dass Aussagenlogik nicht aussagekräftig genug ist.

Beispielsweise können wir den klassischen Syllogismus

$$\frac{\begin{array}{c}\text{Alle Menschen sind sterblich}\\ \text{Sokrates ist ein Mensch}\end{array}}{\text{Sokrates ist sterblich}}$$

nicht in der Aussagenlogik beschreiben. Grund dafür ist, dass die Aussagenlogik Aussagen nur entlang der Junktoren und der Negation aufteilen kann. „Sokrates ist sterblich“ lässt sich also nicht

weiter zerlegen. Genausowenig lassen sich „Sokrates ist ein Mensch“ und „Alle Menschen sind sterblich“ zerlegen. Wir müssen die Aussagen also jeweils als atomare Aussagen interpretieren. Der Syllogismus wird dann also zu

$$\frac{\begin{array}{c}A\\B\end{array}}{C}$$

Diese Formalisierung ist ungeeignet, da $(A \wedge B) \to C$ keine Tautologie ist. Ein Syllogismus soll aber immer wahr sein, daher verfehlt dieser Versuch das Ziel. Tatsächlich lässt sich der Syllogismus in der Aussagenlogik gar nicht sinnvoll studieren.

Wir wollen also die Aussagenlogik erweitern, um zum einen das Verhältnis von Objekten und Aussagen zu beschreiben und zum anderen auch so Konstruktionen wie „Alle x erfüllen die Eigenschaft P“ zu beschreiben.

1.3.2 Atomare Aussagen in der Prädikatenlogik

Der wesentliche Schritt von der Aussagenlogik in die Prädikatenlogik ist es atomare Aussagen zu spalten und subatomare Strukturen sichtbar zu machen.

Wir werden hier zunächst ganz informell argumentieren. In der Prädikatenlogik gibt es

- Konstantensymbole,
- Variablensymbole,
- Prädikatssymbole,
- höhere Relationssymbole und
- Funktionssymbole.

Die Konstantensymbole stehen für feste Objekte, die über alle Aussagen hinweg dasselbe referenzieren. Was als Konstante gilt, ist abhängig von der Theorie. In der Theorie der Peano-Arithmetik, also einer Theorie der natürlichen Zahlen, ist beispielsweise die Null 0 (oder die Eins 1, je nach Definition) als die kleinste natürliche Zahl eine Konstante. In der Theorie der Mengenlehre ist die leere Menge $\emptyset$ als die einzige Menge ohne Elemente eine Konstante. Wir werden uns hier die Freiheit nehmen jeden feststehenden Ausdruck, dessen Bedeutung über alle Formeln konstant bleibt als Konstante zu betrachten. Die Variablensymbole stehen für beliebige, unbestimmte Objekte. Sie stehen dabei nicht nur für die durch die Konstantensymbole referenzierten Objekte sondern auch für (mögliche) Objekte die keine eigenen Konstantensymbole haben.

Diese Objekte werden durch die Prädikats-, Relations- und Funktionssymbole zu Ausdrücken und Aussagen zusammengesetzt.

Dies werde ich nun anhand von Beispielen erklären.

Beispiel 1.3.1 (Atomare Aussagen in der Prädikatenlogik)**.**

Prädikate: *(Eigenschaften)* Aussagen wie „4 ist gerade“, „π ist irrational“ oder „Das Gleichungssystem M ist lösbar“ setzen ein Objekt mit einer Eigenschaft in Verbindung. Dadurch entstehen Aussagen. Diese Eigenschaftsschemata wie „…ist gerade“, „…ist irrational“ oder „Das Gleichungssystem …ist lösbar“ werden *Prädikate* genannt.

Die Aussage „Sokrates ist sterblich“ lässt sich so formulieren, dass man eine Konstante Sokrates einführt und ein Prädikatssymbol sterblich eingeführt wird. Wir hätten dann

die Formalisierung sterblich(Sokrates). Genauso kann man mit dem Prädikatssymbol istMensch die Aussage „Sokrates ist ein Mensch“ durch istMensch(Sokrates) formalisieren.

Die Konstanten- und Variablensymbole erlauben es über mehrere Aussagenteile hinweg auf dieselben Objekte zu referenzieren. So ist istMensch(Sokrates) → sterblich(Sokrates) eine zusammengesetzte Aussage und Sokrates referenziert in beiden Fällen dasselbe Objekt. Dies löst ein wesentliches Problem der Formalisierung des Syllogismus in der Aussagenlogik.

Relationen: *(Verhältnisse) Relationen* sind Eigenschaften die mehrere Objekte miteinander verbinden. Eine Relation heißt *n-stellig*, wenn sie n Objekte als Argumente nimmt. Beispiele für zweistellige Relationen sind „3 teilt 9“, „$\pi < 17$“, „Alice und Bob sind befreundet“. Eine dreistellige Relation ist „Die Punkte x, y und z liegen nicht auf einer Linie“.

Funktionen: *(Zuweisungen)* Anstatt Objekte direkt in Relationen und Prädikate einzusetzen, kann man sie auch vorher in eine Funktion setzen. Eine Funktion weist jedem Objekte genau ein (möglicherweise anderes) Objekt zu. Wir werden Funktionen später noch genauer definieren und studieren. Beispiele für Funktionen der reellen Zahlen in sich selber sind $f(x) := x^2$, $g(x) := -x$, $h(x) := x + 1$ oder sogar sehr wilde Abbildungen wie

$$s(x) := \begin{cases} 0 & x \text{ ist rational} \\ 1 & \text{sonst} \end{cases}.$$

So eine Aussage wie „n^2 ist gerade“ setzt n nicht direkt in das Prädikat „…ist gerade“ ein sondern setzt n zunächst in die Quadratfunktion ein.

Nun haben wir die atomaren Aussagen in der Prädikatenlogik. Bemerke, dass obwohl man die atomaren Aussagen in subatomare Bestandteile wie Prädikate, Objekte und Funktionen zerlegen kann, keine dieser Bestandteile für sich genommen eine Aussage ist. Die atomaren Aussagen lassen sich nun wie in der Aussagenlogik mit den Junktoren und der Negation verknüpfen.

Beispiel 1.3.2 (Die aussagenlogischen Verknüpfungen in der Prädikatenlogik)**.** Wir können nun Aussagen treffen wie

- „$3 < \pi \wedge \pi < 4$“ wobei die Atome „$3 < \pi$“ und „$\pi < 4$“ verknüpft werden. Eine Abkürzung für solche Aussagen wäre „$3 < \pi < 4$“, wir werden häufig Aussagen so zusammenziehen. Es ist dennoch wichtig zu verstehen, dass es sich formal um zwei getrennte Aussagen handelt.
- „istTeilVon(Sokrates, Menschen) → sterblich(Sokrates)“ ist eine Formalisierung von „Sokrates ist ein Mensch, also ist Sokrates sterblich“.
- „(2 teilt n^2) → (2 teilt n)“ ist eine Formalisierung von „Wenn 2 ein Teiler von n^2 ist, dann ist 2 auch ein Teiler von n“. Bemerke, dass n hier keine Konstante sondern eine Variable ist.

  Streng genommen ist „(2 teilt n^2) → (2 teilt n)“ also keine fertige Aussage. Insbesondere ist sie nicht wahr oder falsch, sondern ein Schema, das für jede konkrete Wahl von n wahr oder falsch ist.

  Solche Formeln heißen *offen*. Die Variable n heißt *ungebunden*. Wir werden bald sehen wie man Formeln schließen und Variablen binden kann.

1.3.3 Quantoren

Wir haben gesehen, dass es in der Prädikatenlogik Formeln mit ungebundenen Variablen gibt. Solche Ausdrücke sind keine Aussagen, da ihr Wahrheitswert nicht festgelegt ist, sondern vom eingesetzten Wert der Variablen abhängt. Man bezeichnet sie daher als Aussageschemata oder Prädikate.

Eine naheliegende Möglichkeit, aus einem solchen Ausdruck eine Aussage zu machen, besteht darin, die Variable durch ein konkretes Konstantensymbol zu ersetzen. So erhält man eine geschlossene Formel.

Oft möchte man jedoch gerade Aussagen formulieren, die nicht von einem konkreten Objekt handeln, sondern allgemein oder für einige gelten.

Hier kommen die Quantoren ins Spiel. Sie erlauben es, Variablen zu binden und dadurch aus Aussageschemata wieder Aussagen zu erzeugen.

In der klassischen Prädikatenlogik gibt es zwei grundlegende Quantoren: den Existenzquantor und den Allquantor.

Definition 1.3.3 (Existenzquantor)**.** Sei $P(n)$ ein Aussageschema mit einer ungebundenen Variablen n. Dann ist

$$\exists n \,:\, P(n)$$

eine Aussage mit der Bedeutung: „Es gibt einen Wert k für n, für den $P(k)$ wahr ist."

Intuitiv kann man dies auch lesen als: „Es gibt ein Objekt n, so dass $P(n)$ gilt."

Die Aussage $\exists n \,:\, P(n)$ ist genau dann wahr, wenn es mindestens ein Objekt gibt, für das das Aussageschema erfüllt ist.

Definition 1.3.4 (Allquantor)**.** Sei $P(n)$ ein Aussageschema mit einer ungebundenen Variablen n. Dann ist

$$\forall n \,:\, P(n)$$

eine Aussage mit der Bedeutung: „Für alle Werte k von n, ist $P(k)$ wahr."

Intuitiv kann man dies auch lesen als: „Für alle Objekte n, gilt $P(n)$."

Die Aussage $\forall n \,:\, P(n)$ ist genau dann wahr, wenn für jedes Objekt das Aussageschema erfüllt ist.

Beispiel 1.3.5. Betrachte die Aussageformel $n < k \to n < k + 1$. Diese enthält sowohl n als auch k als ungebundene Variablen. Die Aussage $\forall n \,:\, n < k \to n < k + 1$ enthält n als gebundene und k als ungebundene Variable. Die Aussage $\forall k \,:\, \forall n \,:\, n < k \to n < k + 1$ enthält keine ungebundenen Variablen.

Beispiel 1.3.6. Die Reihenfolge der Quantoren spielt eine große Rolle: Wir betrachten als Objekte die natürlichen Zahlen und $<$ als das Symbol für „kleiner als".

Die Aussage

$$\forall k \,:\, \exists n \,:\, k < n$$

behauptet, dass es für jede Zahl eine größere Zahl gibt. Diese Aussage ist wahr.

Die Aussage

$$\exists n \,:\, \forall k \,:\, k < n$$

behauptet, dass es eine Zahl gibt, die größer als alle anderen ist. Diese Aussage ist falsch.

Aufgabe: Was sagen die Aussagen $\forall n \,:\, \exists k \,:\, k < n$ und $\exists k \,:\, \forall n \,:\, k < n$?

Bemerkung 1.3.7. Wenn $n_1, n_2, \ldots$ die möglichen Werte von n sind, dann kann man sich $\forall n : P(n)$ anschaulich vorstellen wie eine (unendliche) „Und-Verknüpfung“

$$P(n_1) \wedge P(n_2) \wedge \ldots .$$

Dies ist jedoch nur eine Intuition: Eine solche unendliche Verknüpfung ist keine Formel, da wir keine unendlich langen Formeln erlauben.

Analog kann man sich auch $\exists n : P(n)$ anschaulich vorstellen wie eine (unendliche) „Oder-Verknüpfung“

$$P(n_1) \vee P(n_2) \vee \ldots .$$

Wieder ist dies nur eine Intuition, da wir unendlich lange Formeln nicht erlauben.

Leitbeispiel 1.3.8 (Messrauschen und Messdauer)**.** Als Leitbeispiel begleitet uns eine Frage aus dem Labor mit einem Messgerät für Gravitationswellen. Es treten zwei verschiedene Sorten von Objekten auf: mögliche *Rauschamplituden* A (die Intensität des Grundrauschens durch vorbeifahrende Autos etc.) und mögliche *Messdauern* L, gemessen in Tagen. Der Allquantor läuft gleich über die Amplituden, der Existenzquantor über die Dauern — dass Quantoren über verschiedene Bereiche laufen dürfen, machen die eingeschränkten Quantoren am Ende des Kapitels präzise. Wir betrachten die Relation $G(A, L)$ mit der Bedeutung „bei Rauschamplitude A reichen L Messtage, um die ersten beiden Nachkommastellen der Messgröße zu bestimmen“.

Zwei Behauptungen über das Labor:

$$\text{(a)} \quad \forall A : \exists L : G(A, L) \qquad\qquad \text{(b)} \quad \exists L : \forall A : G(A, L)$$

Aussage (a) sagt: *Egal wie schlimm das Rauschen: Wenn man lang genug misst, kommt man an die ersten beiden Nachkommastellen.* Das ist bescheiden und häufig wahr, die notwendige Messzeit kann aber extrem lang werden. Aussage (b) sagt: *Es gibt eine maximale Messdauer L, die unabhängig von der Amplitude des Rauschens die ersten beiden Nachkommastellen liefert*. Das ist viel stärker.

Der einzige Unterschied zwischen (a) und (b) ist die Reihenfolge der Quantoren — das Phänomen aus dem letzten Beispiel, jetzt mit praktischen Konsequenzen. Die Merkregel: In (a) darf die Dauer L von der Rauschamplitude A abhängen, in (b) muss *eine* Dauer L für alle Rauschamplituden zugleich funktionieren. Dieses Muster — abhängige gegen uniforme Schranken — wird Ihnen in der Analysis ständig begegnen, etwa als Unterschied zwischen Stetigkeit und gleichmäßiger Stetigkeit.

Definition 1.3.9 (Umformungsregeln für Quantoren)**.** Wir definieren die folgenden Umformungsregeln:

Negation Für jedes Aussageschema $P(x)$ mit x als ungebundener Variablen gilt

$$\neg(\exists x : P(x)) \iff \forall x : \neg P(x)$$

und

$$\neg(\forall x : P(x)) \iff \exists x : \neg P(x) .$$

Aufgabe: Vergleiche das mit den De Morgan'schen Regeln.

Kommutativität gleicher Quantoren Für jedes Aussageschema $P(x, y)$ mit x und y als ungebundenen Variablen gilt

$$\forall x : \forall y : P(x, y) \iff \forall y : \forall x : P(x, y)$$

und

$$\exists x : \exists y : P(x, y) \iff \exists y : \exists x : P(x, y) .$$

Distribution Es seien $P(x)$ und $Q(x)$ Aussageschemata mit x als ungebundener Variable. Dann gilt

$$(\forall x : P(x)) \wedge (\forall x : Q(x)) \iff \forall x : (P(x) \wedge Q(x))$$

und

$$(\exists x : P(x)) \vee (\exists x : Q(x)) \iff \exists x : (P(x) \vee Q(x))$$

Aufgabe: Vergleiche das mit den Assoziativgesetzen.

Aufgabe: Machen Sie sich anhand von Beispielen klar, weshalb die obigen Rechenregeln gelten.
Aufgabe: Machen Sie sich anhand eines Beispiels klar, weshalb die Aussagen

$$\forall x : (P(x) \vee Q(x))$$

und

$$(\forall x : P(x)) \vee (\forall x : Q(x))$$

unterschiedlich sind.

Bemerkung 1.3.10. Der Name einer gebundenen Variablen spielt keine Rolle. So haben die Aussagen $\forall x : P(x)$ und $\forall y : P(y)$ die gleiche Bedeutung.

Leitbeispiel 1.3.11 (Alle Schwäne sind weiß: Falsifikation)**.** Ein Naturgesetz ist eine Allaussage: Es behauptet etwas über *alle* Fälle, nicht nur über die zufällig schon beobachteten. Die Faustregel der europäischen Naturkunde des 17. Jahrhunderts „alle Schwäne sind weiß“ — formal

$$\forall x : \big(\mathsf{Schwan}(x) \to \mathsf{weiß}(x)\big)$$

— galt als gesichert, bis in Australien schwarze Schwäne gefunden wurden. Was leistet dieser eine Fund? Die Negationsregel beantwortet das mechanisch:

$$\neg\big(\forall x : (\mathsf{Schwan}(x) \to \mathsf{weiß}(x))\big) \iff \exists x : \big(\mathsf{Schwan}(x) \wedge \neg\, \mathsf{weiß}(x)\big).$$

Zum Widerlegen einer Allaussage genügt also *ein einziges* Gegenbeispiel. Bemerke, wie die Negation aus dem $\to$ ein $\wedge$ macht: Der Zeuge muss ein Schwan sein *und* nicht weiß. Der Quantorenschritt ist dabei unsere neue Negationsregel; der innere Schritt $\neg(\alpha \to \beta) \Leftrightarrow \alpha \wedge \neg\beta$ ist reine Aussagenlogik und folgt aus drei Regeln des letzten Kapitels:

$$\neg(\alpha \to \beta) \Leftrightarrow \neg(\neg\alpha \vee \beta) \Leftrightarrow \neg\neg\alpha \wedge \neg\beta \Leftrightarrow \alpha \wedge \neg\beta$$

(Elimination der Implikation, De Morgan, Doppelnegation). Ein schwarzer Rabe widerlegt nichts — er erfüllt die Prämisse $\mathsf{Schwan}(x)$ gar nicht erst.

Das ist exakt die logische Struktur der Falsifikation aus dem Vorwort: Naturgesetze sind Allaussagen („alle Körper, alle Zeiten, alle Orte …“), und deshalb kann ein einzelnes Experiment sie widerlegen, aber kein noch so großer Stapel bestätigender Beobachtungen sie beweisen. Für den *Beweis* einer Allaussage über unendlich viele Fälle braucht es andere Werkzeuge: die Schlussregeln gleich — und später die Induktion.

Definition 1.3.12 (Schlussregeln für Quantoren)**.** Sei $P(x)$ ein Aussageschema.

1. **All-Elimination.** Aus

   $$\forall x : P(x)$$

   folgt für jedes Objekt a

   $$P(a).$$

2. **Existenz-Einführung.** Aus
$$P(a)$$
folgt
$$\exists x : P(x).$$

3. **All-Einführung.** Wenn man für ein beliebig gewähltes Objekt a gezeigt hat, dass
$$P(a)$$
gilt, dann darf man folgern, dass
$$\forall x : P(x)$$
gilt.

   Hier ist wichtig, dass a wirklich beliebig gewählt ist und keine besonderen zusätzlichen Eigenschaften von a benutzt wurden. Insbesondere darf keines der Zeichen in P irgendwie von a abhängen. Siehe Beispiel 1.3.16.

4. **Existenz-Elimination.** Angenommen, es gilt
$$\exists x : P(x).$$
   Dann darf man für den weiteren Beweis mit einem neuen Namen b arbeiten, der vorher nirgendwo vorkam, und $P(b)$ als Arbeitshypothese benutzen.

   Gelingt es unter dieser Annahme, eine geschlossene Formel zu beweisen, in der b nicht vorkommt, so darf man diese Formel aus
$$\exists x : P(x)$$
   schlussfolgern.

Leitbeispiel 1.3.13 (Fall im Vakuum: die Schlussregeln)**.** Die Falsifikation in Leitbeispiel 1.3.11 zeigte die eine Seite des Allquantors: *ein* Gegenbeispiel widerlegt eine Allaussage. Die vier Schlussregeln zeigen die andere Seite — wie man mit Allaussagen *arbeitet* und sie sogar gewinnt. Als Gesetz betrachten wir Galileis Behauptung „im Vakuum fallen alle Körper gleich schnell“, also $\forall x : F(x)$ mit $F(x) =$ „x fällt mit der Beschleunigung g“. Das präzisiert „gleich schnell“: alle Körper mit *derselben* Beschleunigung. (Der Wert g gilt nahe der Erdoberfläche; auf dem Mond fällt ebenfalls alles gleich schnell, nur mit kleinerem g.)

Zwei der Regeln benutzt man dabei völlig selbstverständlich. Die *All-Elimination* wendet das Gesetz an: Aus $\forall x : F(x)$ folgt $F(\text{Feder})$ — vom Naturgesetz zum konkreten Körper in der Hand. Die *Existenz-Einführung* meldet einen Befund: Aus „*dieser* Körper fällt nicht mit g“ folgt $\exists x : \neg F(x)$ — so wird aus einer einzelnen Messung der Kandidat für ein Gegenbeispiel.

Heikel sind die beiden anderen Regeln, und zwar aus symmetrischen Gründen. Die *All-Einführung* verlangt, dass das betrachtete Objekt wirklich *beliebig* war: Ein einzelner Fallversuch beweist noch kein Naturgesetz. Genau hier steckt die Kunst des Experiments. Lässt man im Hörsaal Feder und Hammer fallen, so ist der Körper eben *nicht* beliebig — er trägt die Eigenschaft „spürt Luftwiderstand“, und die Feder bleibt zurück. Erst die Idealisierung, das Vakuum, streift einige der Eigenschaften ab, die einen Körper vom anderen unterscheiden. Was hoffentlich übrig bleibt, ist ein Körper ohne besondere Eigenschaften: ein physikalischer Stellvertreter für das „beliebig gewählte a“ der All-Einführung. Ob man von allen wesentlichen Eigenschaften abstrahiert hat, ist dennoch eine Frage die gestellt werden kann. Das Experiment versucht über Idealisierung den *beliebigen* Vertreter zu wählen, die Mathematik ist von solchen empirischen Fragen befreit.

Die *Existenz-Elimination* verlangt spiegelbildlich, dass man dem Zeugen keine Eigenschaften unterstellt, die nicht aus der bloßen Existenzaussage stammen: Aus der Behauptung, dass *nicht* alle Körper gleich schnell fallen folgt nicht, dass Feder und Stahlkugel unterschiedlich schnell fallen.

Wie beide Fehler im Detail aussehen, zeigen die folgenden Beispiele.

Beispiel 1.3.14 (Existenz-Elimination: zulässige Verwendung)**.** Wir zeigen: Aus

$$\exists x : P(x)$$

folgt

$$\exists y : P(y).$$

Beweis. Angenommen, es gilt

$$\exists x : P(x).$$

Wir führen einen neuen Namen a ein und arbeiten mit der Annahme

$$P(a).$$

Aus

$$P(a)$$

folgt mit der Existenz-Einführung

$$\exists y : P(y).$$

Diese Aussage ist geschlossen und enthält a nicht. Also dürfen wir aus

$$\exists x : P(x)$$

die Aussage

$$\exists y : P(y)$$

schlussfolgern. □

Wir zeigen nun eine etwas interessantere Aussage: Aus

$$\exists x : \neg P(x)$$

und

$$\forall x : P(x) \vee Q(x)$$

folgt

$$\exists x : Q(x)\,.$$

Beweis. Angenommen es gilt

$$\exists x : \neg P(x)$$

Wir führen einen neuen Namen a ein und arbeiten mit der Annahme $\neg P(a)$. Nun können wir aus der Annahme

$$\forall x : P(x) \vee Q(x)$$

insbesondere mit der All-Elimination auch

$$P(a) \vee Q(a)$$

schlussfolgern. Aus $\neg P(a)$ und $P(a) \vee Q(a)$ folgern wir $Q(a)$. Nun können wir mit der Existenz-Einführung auch

$$\exists x : Q(x)$$

schlussfolgern. □

Beispiel 1.3.15 (Existenz-Elimination: unzulässige Verwendung)**.** Das folgende Scheinargument ist falsch: Die Behauptung

$$\exists x : (x \text{ ist gerade})$$

ist über den natürlichen Zahlen wahr. Nun wähle ich das „neue“ Symbol 7, das wir bisher nicht verwendet haben und schlussfolgere dass

$$7 \text{ ist gerade}$$

gilt. Das ist natürlich falsch, da 7 gar kein neues Symbol ist, sondern eine feststehende Bedeutung hat.

Beispiel 1.3.16 (Ein subtiler Fehler bei der Existenz-Elimination und All-Einführung)**.** Wir betrachten die natürlichen Zahlen. Die Aussage

$$\forall x : \exists y : x < y$$

ist wahr.

Ein **falsches Scheinargument** könnte nun so aussehen:

Scheinbeweis. Sei a beliebig. Dann gilt

$$\exists y : a < y.$$

Wir führen einen neuen Namen b ein und nehmen an, dass

$$a < b$$

gilt.

Da a beliebig war, folgern wir

$$\forall x : x < b.$$

Mit Existenz-Einführung erhalten wir

$$\exists y : \forall x : x < y.$$

□

Der Fehler liegt darin, dass der gewählte Zeuge b von a abhängen darf. Für verschiedene Werte von a kann man also verschiedene Werte von b benötigen.

Daher darf man aus

$$\forall x : \exists y : x < y$$

nicht auf

$$\exists y : \forall x : x < y$$

schließen. Tatsächlich ist die erste Aussage in $\mathbb{N}$ wahr, die zweite aber falsch.

Beispiel 1.3.17 (All-Einführung: zulässige Verwendung)**.** Wir zeigen: Aus

$$\forall x : P(x)$$

folgt

$$\forall x : (P(x) \vee Q(x)).$$

Beweis. Angenommen, es gilt

$$\forall x : P(x).$$

Sei nun a ein beliebig gewähltes Objekt. Dann folgt aus der All-Elimination

$$P(a).$$

Daraus folgt

$$P(a) \vee Q(a).$$

Da a beliebig war, dürfen wir mit der All-Einführung schließen:

$$\forall x : (P(x) \vee Q(x)).$$ □

Beispiel 1.3.18 (All-Einführung: unzulässige Verwendung)**.** Das folgende Scheinargument ist falsch:

Wir betrachten die natürlichen Zahlen. Sei a eine gerade Zahl. Dann gilt:

$$a \text{ ist gerade.}$$

Also:

$$\forall x : (x \text{ ist gerade}).$$

Der Fehler besteht darin, dass a nicht beliebig gewählt wurde. Es wurde bereits vorausgesetzt, dass a gerade ist. Daher darf man nicht auf eine Allaussage schließen.

1.3.4 Einschränkungen von Quantoren und Mengenlehre

Wir haben bisher immer die Quantoren über alle Objekte laufen lassen und vorher lediglich gesagt, was die Objekte sein sollen. So haben wir beispielsweise gesagt: „ Es seien die Objekte die natürliche Zahlen. Dann ist die Formel $\forall n : \exists m : n < m$ wahr. “

In der formalen Logik studiert man inwiefern man die Mengen der Objekte durch die Formeln alleine festlegen kann.

Beispiel 1.3.19 (Peano-Axiome)**.** So sind beispielsweise die Peano-Axiome[3] heute die allgemein akzeptierte *Definition* der natürlichen Zahlen. Axiome sind dabei eine Liste von Aussagen die eine Struktur ausmachen.

Diese benutzen ein Konstantensymbol N (zu interpretieren als 0) — Vorsicht: Dieses Symbol N hat nichts mit der Menge $\mathbb{N}$ zu tun, es ist nur ein Name für die Null — und ein Funktionssymbol S (zu interpretieren als die Nachfolgeroperation $S(n) = n + 1$). Außerdem benutzt es das Gleichheitssymbol $=$ in der üblichen Bedeutung. Da die Peano-Axiome die natürlichen Zahlen erst definieren sollen ist es das Ziel der Axiome die Eigenschaften der 0 und der Nachfolgeroperation zu charakterisieren. Genau genommen charakterisieren die Axiome die natürlichen Zahlen *einschließlich* der Null, also die Menge $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$. In diesem Skript zählt die Null nicht zu $\mathbb{N}$; wo es auf den Unterschied ankommt, schreiben wir $\mathbb{N}_0$.

Eine moderne Darstellung der Axiome wäre:

[3] Giuseppe Peano (1858–1932) war ein italienischer Mathematiker, Logiker und Linguist. Er ist vor allem für seine Peano-Axiome bekannt, die die Grundlagen der natürlichen Zahlen formalisieren, sowie für seine Beiträge zur mathematischen Logik und Notation. Peano entwickelte eine präzise Symbolik für die Logik und beeinflusste die Entwicklung der modernen Mengenlehre und formalen Logik. Außerdem studierte er die Genauigkeit von Approximationen von Integralen und fand eine stetige Kurve, die die ganze Ebene ausfüllte (die Peano-Kurve).

Eigenschaft von N: „0 ist kein Nachfolger“:

$$\neg\exists x \,:\, (S(x) = N)$$

Eigenschaft von S: „Unterschiedliche Zahlen haben unterschiedliche Nachfolger“:

$$\forall x \,:\, \forall y \,:\, (S(x) = S(y) \to x = y)$$

Induktionsaxiom: „Wenn man iterativ alle Nachfolger von der Null nimmt hat man alle Zahlen:“
Für jedes Prädikat φ das sich aus den logischen Symbolen und N sowie S bauen lässt gilt

$$\Big(\varphi(N) \wedge \forall x \,:\, (\varphi(x) \to \varphi(S(x)))\Big) \to \forall x \,:\, \varphi(x)\,.$$

Dieses Axiom ist das tiefgreifendste, weil es probiert die Gesamtheit aller unendlich vielen natürlichen Zahlen zu beschreiben. Die Idee ist: Gilt eine Aussage für die Null und *vererbt* sie sich von jeder Zahl auf ihren Nachfolger, dann gilt sie für alle natürlichen Zahlen.

Eine wichtige Beweistechnik verwendet nun das Induktionsaxiom nicht als Charakterisierung der natürlichen Zahlen sondern als Trick um eine Aussage für alle natürlichen Zahlen zu zeigen.

Die Idee ist es die natürlichen Zahlen als eine unendliche Kette von Dominosteinen zu verstehen. Wenn man weiß, dass jeder Stein der fällt auch den nächsten Stein umwerfen wird, reicht es den ersten Stein umzuwerfen um alle Steine umzuwerfen.

Angenommen man will also zeigen, dass ein Prädikat φ für alle natürlichen Zahlen gilt. Wenn man nun zeigen kann, dass aus $\varphi(n)$ auch $\varphi(n+1)$ folgt, dann reicht es $\varphi(0)$ zu zeigen.

Dieser Ansatz spielt in den Grundlagen der modernen Mathematik eine wichtige Rolle. Wenn man etwas axiomatisch begründen will, dann darf man sich auf keine Intuition zu den Grundbegriffen verlassen sondern alles in den Axiomen ausdrücken. Dies wurde von David Hilbert im Falle der Geometrie so auf den Punkt gebracht.

„ Man muß jederzeit an Stelle von ‚Punkte, Geraden, Ebenen‘ [auch] ‚Tische, Stühle, Bierseidel‘ sagen können “

Dieser Ansatz ist in der reinen Mathematik sehr fruchtbar. Er erfordert aber eine große Maschinerie an Technik und erfordert es die bisherige Intuition durch eine rein logische Intuition zu ersetzen. Daher eignet sich dieser Ansatz nur schwer für eine Grundvorlesung. Tatsächlich arbeiten auch die meisten Mathematiker in der Praxis nicht so.

Wir wählen einen anderen Ansatz: Wir arbeiten innerhalb des Rahmens der Mengenlehre. Dies ist eine Theorie die Kollektionen von mathematischen Objekten als eigenständige Objekte studiert. Oder um es mit Felix Hausdorff zu sagen: Mengen sind „Vielheit als Einheit“ gedacht. Die Mengenlehre erlaubt uns die Objekte mit denen wir arbeiten wollen (in einem abstrakten Sinn) zu konstruieren. Dennoch wird uns die axiomatische Methode in weniger radikaler Form immer wieder begegnen.

Bevor wir uns der Mengenlehre selber widmen werden wir die Notation beschreiben. Mengen kann man zum einen direkt über die Angabe der Objekte und der geschweiften Klammern { und } definieren. Die Menge, die die Zahlen 1, 3 und 2878 enthält, schreibt man als

$$\{1, 3, 2878\}\,.$$

Um zu sagen „x ist ein Element von A“ schreiben wir

$$x \in A\,.$$

Ein paar Mengen fassen wir erstmal als einfach gegeben auf: Mit $\mathbb{N}$ bezeichnen wir die Menge aller natürlichen Zahlen, mit $\mathbb{Q}$ die Menge aller rationalen Zahlen und mit $\mathbb{R}$ die Menge aller reellen Zahlen.

Ist A eine Menge und φ ein Prädikat, so ist $\{x \in A \mid \varphi(x)\}$ die Menge aller x aus A die $\varphi(x)$ erfüllen. So ist beispielsweise

$$\{n \in \mathbb{N} \mid 2 \text{ teilt } n\}$$

die Menge aller geraden Zahlen.

Sobald wir Mengen haben stellt sich die Frage: Wie kann man Quantoren auf Mengen einschränken?

Manchmal will man sagen „Für alle natürlichen Zahlen gilt …“ oder „Es gibt eine rationale Zahl …“. Als Abkürzung dafür verwendet man „$\forall n \in \mathbb{N} : \ldots$“ oder „$\exists q \in \mathbb{Q} : \ldots$“. Aber wie kann man das auf die bisherigen Symbole zurückführen?

Definition 1.3.20 (Eingeschränkte Quantoren)**.** Sei A eine Menge und φ ein Prädikat.

Die Schreibweise

$$\forall x \in A : \varphi(x)$$

ist definiert als

$$\forall x : (x \in A \to \varphi(x)) .$$

Aufgabe: Machen Sie sich klar, dass diese Definition die Bedeutung erfasst. Welche Eigenschaft von $\to$ spielt hier eine wichtige Rolle?

Die Schreibweise

$$\exists x \in A : \varphi(x)$$

ist definiert als

$$\exists x : (x \in A \wedge \varphi(x)) .$$

Aufgabe: Machen Sie sich klar, dass diese Definition die Bedeutung erfasst. Warum verwenden wir hier nicht ebenfalls $\to$ anstelle von $\wedge$?

Beispiel 1.3.21 (Derselbe Satz, zwei Welten)**.** Eingeschränkte Quantoren machen sichtbar, dass eine Formel allein noch keinen Wahrheitswert hat — es kommt darauf an, worüber quantifiziert wird. Betrachte

$$\forall x \in \mathbb{N} : x^2 \geq x \qquad \text{und} \qquad \forall x \in \mathbb{R} : x^2 \geq x.$$

Die erste Aussage ist wahr: Jede natürliche Zahl erfüllt $x \geq 1$, und Multiplikation dieser Ungleichung mit x liefert $x^2 \geq x$. Die zweite Aussage ist falsch, und nach der Negationsregel genügt dafür ein einziger Zeuge: $x = \frac{1}{2}$ erfüllt $x^2 = \frac{1}{4} < \frac{1}{2}$.

Auch physikalisch ist die Abhängigkeit vom Grundbereich Alltag: „Alle Ladungen sind ganzzahlige Vielfache der Elementarladung“ — wahr für freie Teilchen, falsch, sobald man die Quarks im Inneren der Protonen mitzählt. Wer eine Allaussage behauptet oder prüft, muss also zuerst klären, über welche Menge sie läuft. Genau dafür sind die eingeschränkten Quantoren da.

1.4 Grundbegriffe der Mengenlehre

1.4.1 Der Mengenbegriff

Definition 1.4.1. Eine *Menge* ist eine Zusammenfassung von wohlunterschiedenen Objekten, den sogenannten *Elementen* der Menge.

Bemerkung 1.4.2. Für uns ist vor allem wichtig:

- Eine Menge ist durch ihre *Elemente* bestimmt.
- Der *Name* einer Menge ist egal, nur ihr *Inhalt* zählt.
- Reihenfolge spielt keine Rolle, Mehrfachnennungen auch nicht.

Leitbeispiel 1.4.3 (Der Teilchenzoo)**.** Als Leitbeispiel für diesen Abschnitt nehmen wir einen kleinen Ausschnitt aus dem Teilchenzoo der Physik:

$$M := \{e, \mu, \nu, \gamma, p, n\},$$

also Elektron, Myon, Neutrino, Photon, Proton und Neutron. Für die Mengenlehre sind das einfach sechs Objekte — sie fragt nicht, was ein Elektron *ist*.

Schon die Grundregeln von eben haben hier Biss: Es gilt $\{e, \mu\} = \{\mu, e\}$ (eine Teilchenliste ist keine Rangliste), und $\{e, e, \gamma\} = \{e, \gamma\}$ (zweimal nennen erschafft kein zweites Teilchen).

Interessant wird der Zoo durch seine *Eigenschaften*: geladen oder ungeladen, massiv oder masselos, Lepton oder nicht. Jede solche Eigenschaft liefert eine eigene Menge, etwa die Menge der elektrisch geladenen Teilchen $G = \{e, \mu, p\}$. Der ganze Abschnitt handelt davon, wie man mit solchen Mengen arbeitet: wie Eigenschaften und Teilmengen einander entsprechen, wie sich „und“, „oder“ und „nicht“ in Mengenoperationen übersetzen — und wie viele Teilmengen es überhaupt gibt.

Bemerkung 1.4.4 (Zur Geschichte des Mengenbegriffs)**.** Der Mengenbegriff ist der grundlegendste Begriff der modernen Mathematik. Dennoch ist er ein, im Vergleich zum Alter der Mathematik, sehr neuer Begriff. Die meiste Zeit kam die Mathematik ohne den Mengenbegriff aus, heute ist er kaum wegzudenken.

Erst im 19. Jahrhundert wurde der Mengenbegriff systematisch entwickelt, insbesondere durch Georg Cantor. Cantor untersuchte ursprünglich Probleme der Analysis, zum Beispiel die Frage nach der Eindeutigkeit von Fourierreihen, und wurde dabei gezwungen, unendliche Sammlungen von Zahlen genauer zu verstehen.

Dabei entstand eine revolutionäre Idee: Unendliche Mengen können selbst wieder als mathematische Objekte betrachtet und miteinander verglichen werden. So zeigte Cantor etwa, dass es unterschiedlich große Unendlichkeiten gibt.

Diese neuen Ideen führten jedoch zunächst zu erheblichen Paradoxien, zum Beispiel dem sogenannten Russell'schen Paradoxon. Dieses Paradoxon traf den Logiker Gottlob Frege besonders hart: Frege arbeitete in Jena und versuchte, die gesamte Mathematik auf eine logische Grundlage zu stellen. Kurz vor der Veröffentlichung seines Hauptwerks wurde ihm das Paradoxon von Bertrand Russell mitgeteilt, wodurch sein Ansatz in eine schwere Krise geriet.

Dies machte deutlich, dass ein zu naiver Umgang mit Mengen zu Widersprüchen führen kann.

Die moderne Mathematik verwendet daher heute axiomatische Systeme der Mengenlehre, um den Mengenbegriff präzise zu kontrollieren. Trotz dieser formalen Absicherung bleibt die grundlegende Intuition erhalten: Eine Menge ist eine „Vielheit als Einheit“.

Beispiel 1.4.5.

$$A = \{1, 2, 3\}, \qquad B = \{3, 2, 1\}, \qquad C = \{1, 2, 2, 3\}.$$

Dann gilt

$$A = B = C,$$

denn alle drei Mengen enthalten genau dieselben 3 Elemente. Jedoch wäre

$$D = \{1, \{2\}, 3\}$$

eine andere Menge.

Beispiel 1.4.6 (Gleichheit trotz anderer Schreibweise)**.**

$$\{x \in \mathbb{Z} \mid x^2 = 1\} = \{-1, 1\}.$$

Beispiel 1.4.7 (Gleichheit trotz anderer Namen)**.**

$$A = \{1, 2, 3\}, \qquad M = \{3, 2, 1\}.$$

Dann gilt $A = M$.

Beispiel 1.4.8. Die Menge der geraden natürlichen Zahlen kann man schreiben als

$$E = \{0, 2, 4, 6, 8, \dots\}.$$

Oder beschreibend:

$$E = \{n \in \mathbb{N}_0 \mid n \text{ ist gerade}\}.$$

Definition 1.4.9. Eine Menge, die keine Elemente enthält, nennen wir die leere Menge und schreiben $\emptyset$ oder $\{\}$.

Bemerkung 1.4.10. Da Mengen durch ihre Elemente eindeutig bestimmt sind, gibt es nur eine einzige leere Menge.

Beispiel 1.4.11. $A := \emptyset$ und $B := \{\emptyset\}$ sind nicht die gleiche Menge. Das mag verwundern, aber A hat keine Elemente und B hat genau ein Element (und zwar A).

1.4.2 Elemente und Teilmengen

Ist x ein Element der Menge A, so schreiben wir

$$x \in A.$$

Ist x kein Element von A, so schreiben wir

$$x \notin A.$$

Daher gilt also auch

$$\neg(x \in A) \Leftrightarrow x \notin A.$$

Definition 1.4.12. Für zwei Mengen A und B heißt A eine *Teilmenge* von B, wenn jedes Element von A auch ein Element von B ist. Man schreibt

$$A \subseteq B.$$

Formal:

$$A \subseteq B \iff \forall x : (x \in A \to x \in B).$$

Beispiel 1.4.13. Die folgenden Teilmengenbeziehungen gelten:

$$\{1, 2\} \subseteq \{1, 2, 3\}, \qquad \{2, 4, 6\} \subseteq \mathbb{N}.$$

Definition 1.4.14. Zwei Mengen A und B heißen gleich, wenn sie dieselben Elemente besitzen:

$$A = B \iff \forall x : (x \in A \leftrightarrow x \in B).$$

Lemma 1.4.15. *Es gilt genau dann $A = B$, wenn sowohl $A \subseteq B$ als auch $B \subseteq A$ gilt.*

Beweisidee. Wir zeigen die Behauptung durch logische Umformungen:

$$\begin{aligned} A = B &\iff \forall x : (x \in A \leftrightarrow x \in B) \iff \forall x : ((x \in A \to x \in B) \wedge (x \in B \to x \in A)) \\ &\iff \forall x : (x \in A \to x \in B) \wedge \forall x : (x \in B \to x \in A) \iff A \subseteq B \wedge B \subseteq A \end{aligned}$$

□

Leitbeispiel 1.4.16 (Der Teilchenzoo: Teilmengen und Gleichheit)**.** Im Teilchenzoo Leitbeispiel 1.4.3 bilden

$$L = \{e, \mu, \nu\} \quad \text{(die Leptonen)} \qquad \text{und} \qquad F = \{e, \mu, \nu, p, n\} \quad \text{(die Fermionen)}$$

zwei Teilmengen von M. Es gilt $L \subseteq F$: Jedes Element von L liegt auch in F. Die Umkehrung gilt nicht, denn $p \in F$, aber $p \notin L$. Nach dem Lemma ist damit automatisch $L \neq F$.

Bei endlich vielen Teilchen ist eine Inklusion billig zu prüfen: Man geht die Elemente der Reihe nach durch. Der eigentliche Wert des Lemmas zeigt sich erst, wenn die beiden Mengen nicht als Liste, sondern durch *Eigenschaften* gegeben sind. Dann wird jede der beiden Inklusionen zu einer Allaussage, die man wirklich beweisen muss — wie das nächste Beispiel zeigt.

Beispiel 1.4.17 (Gleichheit über doppelte Inklusion)**.** Wir verlassen den Zoo für einen Moment. Sei Q die Menge der Quadrate, R die Menge der Rechtecke (Vierecke mit vier rechten Winkeln) und D die Menge der Rauten (Vierecke mit vier gleich langen Seiten). Wir behaupten

$$Q = R \cap D.$$

Nach dem Lemma zerfällt das in zwei Inklusionen, und keine davon ist geschenkt:

$Q \subseteq R \cap D$**:** „Jedes Quadrat ist ein Rechteck und eine Raute." Man muss aus der Definition des Quadrats beide Eigenschaften herleiten, die vier rechten Winkel *und* die vier gleich langen Seiten.

$R \cap D \subseteq Q$**:** „Ein Viereck, das zugleich rechtwinklig und gleichseitig ist, ist ein Quadrat." Das ist die eigentliche Rückrichtung.

Erst beide Inklusionen zusammen ergeben die Mengengleichheit. Zwei ganz verschieden formulierte Beschreibungen — „Quadrat" auf der einen, „rechtwinklig und gleichseitig" auf der anderen Seite — liefern dieselbe Menge. Dass eine Menge nur ihren Inhalt kennt und die Formulierung vergisst, ist dabei kein Verlust, sondern der Punkt.

1.4.3 Mengen und Aussagen

Der Zusammenhang zwischen Mengen und Aussagen ist zentral.

Beispiel 1.4.18. Betrachte

$$A = \{x \in \mathbb{R} \mid x > 0\}.$$

Dann ist die Aussage

$$x \in A$$

äquivalent zu

$$x > 0 \wedge x \in \mathbb{R}.$$

Wenn implizit verstanden wird, dass $x > 0$ bedeutet, dass $x \in \mathbb{R}$ ist (oder wir grundsätzlich annehmen, dass $x \in \mathbb{R}$ gilt), so gilt

$$x \in A \iff x > 0\,.$$

Allgemein: Gibt man eine Menge durch eine Eigenschaft an,

$$A = \{x \in M \mid P(x)\},$$

dann ist

$$x \in A \iff (x \in M \wedge P(x)).$$

Bemerkung 1.4.19 (Russell'sches Paradoxon)**.** Bemerke, dass wir stets bestehende Mengen mittels Eigenschaften gefiltert haben. Es ist extrem natürlich auch zu versuchen die Menge von *allem* zu bilden. Oder, äquivalent dazu, zu jeder Aussage φ eine Menge zu bilden.

Das ist aber unmöglich! Betrachte das (zugegebenerweise etwas ungewöhnliche, aber doch sinnvolle) Prädikat

$$\varphi(x) := (x \notin x)\,.$$

Die Aussage $\varphi(x)$ ist also wahr, wenn x eine Menge ist und sich nicht selber enthält. Nehmen wir an, dass es zu der Eigenschaft φ eine Menge gibt und nennen wir sie Ω,[4] also

$$\Omega = \{x \mid \varphi(x)\}\,.$$

Nun stellen wir uns die Frage ob $\varphi(\Omega)$ gilt. Angenommen es gilt $\varphi(\Omega)$. Dann gilt per Definition von Ω dass $\Omega \in \Omega$. Aber was bedeutet $\varphi(\Omega)$? $\varphi(\Omega)$ bedeutet nach Definition von φ genau dass $\Omega \notin \Omega$. Das ist ein Widerspruch. Es bleibt noch der andere Fall, dass $\neg\varphi(\Omega)$ gilt. Dann gilt per Definition von φ genau $\Omega \in \Omega$. Aber per Definition von Ω folgt aus $\neg\varphi(\Omega)$ dass $\Omega \notin \Omega$. Auch das ist ein Widerspruch.

Der einzige Ausweg ist, dass es Ω nicht geben darf. Die moderne Mathematik löst das indem Mengen nur aus bereits auf vorheriger Stufe „konstruierten" Mengen bestehen dürfen. Eine Menge aller Mengen kann es nicht geben, da diese sich selber enthalten würde, aber eine Menge kann ja nicht früher als diese Menge selbst konstruiert worden sein.

1.4.4 Grundlegende Mengenoperationen

Definition 1.4.20. Für Mengen A und B definiert man:

$$A \cup B = \{x \mid x \in A \vee x \in B\} \qquad \text{(Vereinigung)},$$

$$A \cap B = \{x \mid x \in A \wedge x \in B\} \qquad \text{(Schnitt)},$$

$$A \setminus B = \{x \mid x \in A \wedge x \notin B\} \qquad \text{(Differenz)}.$$

[4] Ω wird „Omega" gelesen.

Beispiel 1.4.21 (Logischer Blick auf den Schnitt)**.** Die Aussage

$$x \in \{x \in \mathbb{R} \mid x > 0\} \cap \{x \in \mathbb{R} \mid x < 2\}$$

bedeutet genau

$$x > 0 \wedge x < 2.$$

Also ist die Menge gleich

$$\{x \in \mathbb{R} \mid 0 < x < 2\}.$$

Beispiel 1.4.22. Seien

$$A = \{1, 2, 3, 4\}, \qquad B = \{3, 4, 5\}.$$

Dann ist

$$A \cup B = \{1, 2, 3, 4, 5\},$$
$$A \cap B = \{3, 4\},$$
$$A \setminus B = \{1, 2\}.$$

Beispiel 1.4.23 (Intervalle: Mengenoperationen auf der Zahlengeraden)**.** Die Operationen wirken genauso auf unendlichen Mengen, zum Beispiel auf Intervallen reeller Zahlen. Für

$$A = [0, 2] = \{x \in \mathbb{R} \mid 0 \leq x \leq 2\} \qquad \text{und} \qquad B = [1, 3]$$

gilt

$$A \cup B = [0, 3], \qquad A \cap B = [1, 2], \qquad A \setminus B = \{x \in \mathbb{R} \mid 0 \leq x < 1\}.$$

Hier lohnt sich das Bild auf der Zahlengeraden: Vereinigung heißt *zusammenlegen*, Schnitt heißt *Überlappung*, Differenz heißt *wegradieren*. Bemerke das Detail beim Wegradieren: Der Punkt 1 gehört zu B und wird deshalb mit entfernt — aus dem abgeschlossenen Intervall wird ein halboffenes.

Bemerkung 1.4.24. Die Mengenoperationen sind direkt durch die aussagenlogischen Verknüpfungen gegeben! Wir haben

$$x \in A \cup B \iff x \in A \vee x \in B$$

und

$$x \in A \cap B \iff x \in A \wedge x \in B$$

sowie

$$x \in A \setminus B \iff x \in A \wedge \neg(x \in B).$$

Theorem 1.4.25. *Für alle Mengen A, B, C gelten:*

Kommutativitätsgesetze:

$$A \cup B = B \cup A \quad \textit{und} \quad A \cap B = B \cap A,$$

Assoziativitätsgesetze:

$$(A \cup B) \cup C = A \cup (B \cup C) \quad \textit{und} \quad (A \cap B) \cap C = A \cap (B \cap C).$$

Distributivitätsgesetze:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad \textit{und} \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Beweisidee. Wir zeigen, dass für alle x gilt, dass $x \in A \cup B \Leftrightarrow x \in B \cup A$:

$$x \in A \cup B \Leftrightarrow x \in A \vee x \in B \Leftrightarrow x \in B \vee x \in A \Leftrightarrow x \in B \cup A$$

Wir können den Beweis auch in den Mengenklammern führen: Es gilt

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

und

$$B \cap A = \{x \mid x \in B \wedge x \in A\} \ .$$

Aufgrund des Kommutativitätsgesetzes für Aussagen sind die Aussagen, die die Mengen definieren, äquivalent. Das bedeutet, dass die Mengen gleich sind.
Aufgabe: Warum genau?

Die Assoziativgesetze folgen aus den entsprechenden Gesetzen der Logik. Aufgabe: Wie genau?
Genauso folgen die Distributivgesetze. Eines davon zeigen wir noch als Beispiel:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Wir zeigen für jedes x:

$$x \in A \cap (B \cup C) \iff x \in (A \cap B) \cup (A \cap C).$$

Nun:

$$\begin{aligned} x \in A \cap (B \cup C) &\iff (x \in A) \wedge (x \in B \cup C) \\ &\iff (x \in A) \wedge \big((x \in B) \vee (x \in C)\big) \\ &\iff \big((x \in A) \wedge (x \in B)\big) \vee \big((x \in A) \wedge (x \in C)\big) \\ &\iff x \in (A \cap B) \cup (A \cap C). \end{aligned}$$

Also sind die Mengen gleich.

□

Bemerkung 1.4.26. Egal welche Methoden wir nutzen, es ist wichtig zu verstehen, dass alle diese Rechenregeln der Mengenlehre sofort aus den Regeln der Aussagenlogik folgen!

Es hilft vielleicht sich vorzustellen, dass man, um Gleichheit von Mengen zu zeigen, in die Welt der Logik übersetzt, dort dann die Gesetze der Logik anwendet und schließlich zurückübersetzt. Wir werden es noch öfter erleben, dass bestimmte mathematische Fragen sich in andere mathematische Fragen übersetzen lassen.

Definition 1.4.27. Betrachten wir eine Teilmenge A einer feststehenden Obermenge X, so bezeichnen wir die Differenz $X \setminus A$ auch als das Komplement von A (in X) und schreiben

$$A^c := X \setminus A = \{x \in X \mid x \notin A\}$$

Die Komplementbildung entspricht daher der aussagenlogischen Negation.

Bemerkung 1.4.28. Es ist von größter Wichtigkeit eine feste Obermenge zu wählen. Denn das allgemeine Komplement existiert nicht: Falls A und $B := \{x \mid x \notin A\}$ beides Mengen sind, so ist auch $A \cup B$ eine Menge. Aber $A \cup B$ enthält alles. Nach dem Russell'schen Paradoxon Bemerkung 1.4.19 kann $A \cup B$ keine Menge sein.
Die Obermenge taucht in A^c nicht auf. Diese Notation ist also nur dann zulässig, wenn die Obermenge festgelegt ist.

Beispiel 1.4.29 (Eine Menge, keine Aussage)**.** Seien A und B Teilmengen einer Menge M. Dann ist

$$C = \{x \in M \mid x \in A \to x \in B\}$$

nicht dasselbe wie $A \subseteq B$. Denn C ist eine Menge und $A \subseteq B$ ist eine Aussage.
Aufgabe: Stellen Sie C durch die bisher definierten Mengenoperationen dar! (Erinnerung aus der Aussagenlogik: $\alpha \to \beta \Leftrightarrow \neg\alpha \vee \beta$.)

Theorem 1.4.30 (De-Morgan-Regeln)**.** *Sei X als Obermenge festgelegt. Für $A, B \subseteq X$ gilt:*

$$(A \cup B)^c = A^c \cap B^c \quad \textit{und} \quad (A \cap B)^c = A^c \cup B^c\,.$$

Beweis. Wir führen es wieder auf die Logik zurück:

$$\begin{aligned} x \in (A \cup B)^c &\iff x \notin A \cup B \\ &\iff \neg\big((x \in A) \vee (x \in B)\big) \\ &\iff (x \notin A) \wedge (x \notin B) \\ &\iff x \in A^c \cap B^c. \end{aligned}$$

□

1.4.5 Familien von Mengen

Bisher hatten wir einzelne Mengen A, B, C. Oft betrachtet man aber eine ganze *Familie* von Mengen.

Bemerkung 1.4.31. Der Begriff *Familie* ist kein Fachterminus. Er wird lediglich gebraucht um darauf hinzuweisen, dass die Elemente der Familie sich auf irgendeine Weise ähnlich sind. Bei Mengen hat sich der Begriff durchgesetzt um nicht „Mengen von Mengen" sagen zu müssen. Für die Zwecke dieses Abschnitts — Vereinigungen und Schnitte — dürfen wir eine Familie von Mengen einfach als eine Menge auffassen, die selber Mengen enthält: Es zählt nur, *welche* Mengen vorkommen. (Wo es dagegen auf die Beschriftung ankommt — etwa wenn dieselbe Menge unter zwei verschiedenen Indizes auftreten soll — fasst man Familien stattdessen als Funktionen von der Indexmenge auf. Das können wir präzise machen, sobald Funktionen definiert sind.)

Sei I eine Indexmenge, und zu jedem $i \in I$ gehört genau eine Menge A_i. Dann gibt es eine Menge Z mit

$$B \in Z \iff \exists i \in I : B = A_i\,.$$

Aufgabe: Es gibt nur eine solche Menge Z, aber warum?
Wir schreiben dann $\{A_i \mid i \in I\}$ für diese eindeutig bestimmte Menge Z.

Bemerkung 1.4.32. Die Zuweisung zwischen $i \in I$ und A_i muss definierbar sein. In allen von uns betrachteten Fällen wird das so sein. Tatsächlich kann ich natürlich kein Beispiel einer nicht-definierbaren Zuweisung geben. Daher ist diese Einschränkung in der Praxis kein Problem (außer man redet über alle möglichen Zuweisungen).

Bemerkung 1.4.33. Der Begriff *Indexmenge* ist ebenfalls ein Begriff ohne formale Bedeutung. Jede Menge kann formal eine Indexmenge sein. Vielmehr hat der Begriff eine pragmatische Bedeutung: Wenn I als Indexmenge bezeichnet wird, wird deutlich gemacht, dass die $i \in I$ hier lediglich als Zeichen dienen. Die eigentliche Bedeutung der $i \in I$ ist für den Zweck egal. Wenn man eine Reihe an Stühlen mit Zahlen abzählt, dann haben die Stühle die eine Primzahl tragen nicht unbedingt eine besondere Eigenschaft. Auch der Stuhl mit der 13 ist vermutlich nicht gefährlicher als der Stuhl mit der 14. Um deutlich zu machen, dass die Zahlen hier nur als Nummerierung und nicht in ihrer Bedeutung als konkrete Größen benutzt werden könnte man sagen, „Die Zahlen dienen nur als Indexmenge".

Beispiel 1.4.34. Jede Stuhlreihe im Hörsaal enthält eine Menge von Studierenden. Damit ich die Reihen unterscheiden kann, gebe ich ihnen Namen wie

Reihe 1, Reihe 2, ...

oder etwa

Reihe A, Reihe B, ...

Ich könnte auch Emojis benutzen, oder Tiernamen oder Elemente des Periodensystems usw. Tatsächlich könnte ich sogar eine jede Reihe mit sich selber beschriften.

Beispiel 1.4.35. Wir definieren $A_i = \{i\}$ für $i \in \mathbb{N}$. Dann erhalten wir die Mengen $\{1\}, \{2\}, ...$

Beispiel 1.4.36. Ist $I = \{1, 2, 3\}$, so schreibt man für die Familie auch

$$(A_i)_{i \in I}.$$

Die runden Klammern betonen die Beschriftung durch I. Für Vereinigung und Schnitt zählt aber nur, welche Mengen vorkommen — also die Menge $\{A_1, A_2, A_3\}$.

Definition 1.4.37. Für eine Mengenfamilie $(A_i)_{i \in I}$ definiert man:

$$\bigcup_{i \in I} A_i = \{x \mid \exists i \in I \ : \ x \in A_i\},$$
$$\bigcap_{i \in I} A_i = \{x \mid \forall i \in I \ : \ x \in A_i\}.$$

Wir definieren, dass für jede Mengenfamilie auch diese (potentiell unendlichen) *Vereinigungen und Schnitte* wieder Mengen sind.

Bemerkung 1.4.38. Wir können $\bigcup_{i \in I} A_i$ als (potentiell unendliche) Reihe an Vereinigungen

$$A_{i_1} \cup A_{i_2} \cup ...$$

verstehen. Aber nicht jede Indexmenge lässt sich durchnummerieren (das werden wir später noch sehen). Vergleiche das mit Bemerkung 1.3.7.

Bemerkung 1.4.39. Da $(A_i)_{i \in I}$ nichts anderes ist als die Menge

$$\{A_i \mid i \in I\}$$

können wir anstelle von $\bigcup_{i \in I} A_i$ auch

$$\bigcup \{A_i \mid i \in I\}$$

schreiben. In der reinen Mengenlehre ist jedes Objekt eine Menge. Also ist jede Menge eine Menge von Mengen. Insbesondere können wir für jede Menge X die Vereinigung $\bigcup X$ schreiben. Dabei ist

$$\bigcup X = \bigcup \{A \mid A \in X\} = \bigcup_{A \in X} A\,.$$

Analog können wir auch $\bigcap X$ schreiben.

Beispiel 1.4.40. Sei für $i \in \mathbb{N}$

$$A_i = \{i, i+1, i+2, \dots\}.$$

Dann gilt

$$\bigcup_{i \in \mathbb{N}} A_i = \mathbb{N},$$

aber

$$\bigcap_{i \in \mathbb{N}} A_i = \emptyset,$$

denn keine natürliche Zahl liegt in *allen* Mengen A_i.

1.4.6 Die Potenzmenge

Bevor wir Begriffe wie „Relation“ und „Funktion“ formal einführen können, benötigen wir noch einige Begriffe aus der Mengenlehre. Der wichtigste neue Gedanke ist, dass wir nicht nur Elemente einer Menge betrachten, sondern auch Teilmengen, geordnete Paare und Mengen von geordneten Paaren.

Definition 1.4.41 (Potenzmenge)**.** Sei X eine Menge. Die *Potenzmenge* von X ist die Menge aller Teilmengen von X. Wir schreiben dafür

$$\mathfrak{P}(X)\,.$$

Formal bedeutet das:

$$A \in \mathfrak{P}(X) \iff A \subseteq X.$$

Beispiel 1.4.42. Sei

$$X = \{1, 2\}.$$

Dann ist

$$\mathfrak{P}(X) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}.$$

Die Elemente von $\mathfrak{P}(X)$ sind also selbst wieder Mengen.

Beispiel 1.4.43. Sei $n \in \mathbb{N}$ und $X_n := \{1, \dots, n\}$. Dann ist die Potenzmenge von X_n die Menge aller Teilmengen von X_n. Wie viele Elemente hat diese Menge?

Beispiel 1.4.44. Für die leere Menge gilt

$$\mathfrak{P}(\emptyset) = \{\emptyset\}.$$

Das ist wichtig: Die leere Menge hat keine Elemente, aber sie hat genau eine Teilmenge, nämlich sich selbst.

Bemerkung 1.4.45 (Was bedeutet „alle Teilmengen“?)**.** In der Formulierung „die Menge aller Teilmengen“ steckt ein kleiner fundamentaler Zauber. Es ist nämlich nicht selbstverständlich, was genau mit „allen“ Teilmengen gemeint ist. Bei endlichen Mengen, kann man sich überlegen, wann man fertig ist. Bei unendlichen Mengen dagegen, gibt es keine Methode um zu überprüfen, dass man alle Teilmengen gefunden hat. Wir deklarieren also, dass wie durch Zauberhand tatsächlich „alle“ Teilmengen in dieser Menge vereint sind.

Formal ist $\mathfrak{P}(X)$ als Menge eindeutig dadurch charakterisiert, dass für jede Menge A gilt

$$A \in \mathfrak{P}(X) \iff A \subseteq X.$$

Das definiert $\mathfrak{P}(X)$ eindeutig. Aber für unendliche Mengen X (nicht einmal für $X = \mathbb{N}$) können wir $\mathfrak{P}(X)$ nicht konkreter beschreiben.

In der Praxis ist das natürlich kein Problem, da wir einfach die definierende Formel benutzen können und nicht alle Elemente der Potenzmenge einzeln zusammensammeln wollen.

1.5 Relationen und Funktionen

1.5.1 Paare und Produkte

Relationen und Funktionen werden in der Mengenlehre kodiert als Mengen von geordneten Paaren (interpretiert als Input und Output).

Definition 1.5.1 (Geordnete Paare)**.** Ein *geordnetes Paar* ist ein Objekt, das aus einem ersten und einem zweiten Objekt besteht.

Wir schreiben ein Paar mit erstem Eintrag a und zweitem Eintrag b als

$$(a, b).$$

Dabei sind zwei Paare genau dann gleich, wenn ihre ersten und ihre zweiten Einträge gleich sind:

$$(a, b) = (c, d) \iff a = c \wedge b = d.$$

Beispiel 1.5.2. Es gilt

$$(1, 2) \neq (2, 1).$$

Die Reihenfolge spielt bei Paaren also eine Rolle.

Dagegen gilt für Mengen

$$\{1, 2\} = \{2, 1\}.$$

Ein geordnetes Paar ist also nicht einfach dasselbe wie eine zweielementige Menge.

Bemerkung 1.5.3 (Eine Standardkodierung von Paaren)**.** In der Mengenlehre möchte man oft alle mathematischen Objekte als Mengen auffassen. Daher kann man geordnete Paare durch Mengen *kodieren*.

Eine Standardkodierung ist die sogenannte *Kuratowski-Kodierung*:

$$\langle a, b \rangle := \big\{\{a\}, \{a, b\}\big\}.$$

Dann erfüllt $\langle a, b \rangle$ genau die Eigenschaften, die wir von dem Paar (a, b) verlangen:

$$\langle a, b \rangle = \langle c, d \rangle \iff a = c \wedge b = d.$$

Die Idee ist: Aus

$$\{\{a\}, \{a, b\}\}$$

kann man den ersten Eintrag a wiedererkennen, weil a in beiden inneren Mengen vorkommt. Wenn der erste Eintrag bekannt ist, kann man auch den zweiten Eintrag b aus $\{a, b\}$ zurückgewinnen.

Wir schreiben also $(a, b) := \langle a, b \rangle$. Diese Definition ist nicht die eigentliche Bedeutung eines Paares. Sie ist nur eine technische Kodierung, die genau die gewünschte Gleichheitsregel erfüllt.

Daher dürfen wir uns im Alltag einfach vorstellen, dass (a, b) ein Objekt mit einem ersten und einem zweiten Eintrag ist. Die Kodierung zeigt nur, dass diese Vorstellung innerhalb der Mengenlehre realisiert werden kann und wir nicht noch zusätzliche Operationen hinzufügen müssen.

Definition 1.5.4 (Kartesisches Produkt)**.** Seien X und Y Mengen. Das *kartesische Produkt* von X und Y ist die Menge aller geordneten Paare, deren erster Eintrag aus X und deren zweiter Eintrag aus Y stammt.

Wir schreiben

$$X \times Y := \{(x, y) \mid x \in X \wedge y \in Y\}.$$

Also gilt

$$(x, y) \in X \times Y \iff x \in X \wedge y \in Y.$$

Bemerkung 1.5.5 (Warum existiert das kartesische Produkt als Menge?)**.** Wenn wir die Kuratowski-Kodierung verwenden, dann gilt für $x \in X$ und $y \in Y$:

$$(x, y) = \big\{\{x\}, \{x, y\}\big\}.$$

Da x und y Elemente von $X \cup Y$ sind, sind $\{x\}$ und $\{x, y\}$ Teilmengen von $X \cup Y$. Also gilt

$$\{x\}, \{x, y\} \in \mathfrak{P}(X \cup Y).$$

Damit ist

$$(x, y) \subseteq \mathfrak{P}(X \cup Y).$$

Also gilt

$$(x, y) \in \mathfrak{P}(\mathfrak{P}(X \cup Y)).$$

Das kartesische Produkt kann daher als Teilmenge von $\mathfrak{P}(\mathfrak{P}(X \cup Y))$ aufgefasst werden:

$$X \times Y = \{p \in \mathfrak{P}(\mathfrak{P}(X \cup Y)) \mid \exists x \in X : \exists y \in Y : p = (x, y)\}.$$

Diese Bemerkung ist vor allem dafür da, um zu sehen, dass $X \times Y$ wirklich eine Menge ist. Im normalen Rechnen denken wir einfach an Paare (x, y).

Beispiel 1.5.6 (Endliches kartesisches Produkt)**.** Seien

$$X = \{1, 2\} \qquad \text{und} \qquad Y = \{a, b\}.$$

Dann gilt

$$X \times Y = \{(1, a), (1, b), (2, a), (2, b)\}.$$

Beispiel 1.5.7 (Die Reihenfolge der Faktoren zählt)**.** Im Allgemeinen gilt

$$X \times Y \neq Y \times X.$$

Zum Beispiel ist

$$\{1\} \times \{2\} = \{(1, 2)\},$$

aber

$$\{2\} \times \{1\} = \{(2, 1)\}.$$

Da

$$(1, 2) \neq (2, 1),$$

sind diese beiden Mengen verschieden.

Beispiel 1.5.8 (Produkte mit der leeren Menge)**.** Für jede Menge X gilt

$$X \times \emptyset = \emptyset \qquad \text{und} \qquad \emptyset \times X = \emptyset.$$

Denn es gibt kein Paar, dessen zweiter beziehungsweise erster Eintrag aus der leeren Menge stammt.

Beispiel 1.5.9 (Kartesische Produkte und Koordinaten)**.** Das kartesische Produkt

$$\mathbb{R} \times \mathbb{R}$$

besteht aus allen Paaren reeller Zahlen. Ein Element von $\mathbb{R} \times \mathbb{R}$ hat also die Form

$$(x, y)$$

mit $x, y \in \mathbb{R}$.

Wir können $\mathbb{R} \times \mathbb{R}$ als die Ebene auffassen. Der erste Eintrag beschreibt dann die horizontale Koordinate, der zweite Eintrag die vertikale Koordinate.

Beispiel 1.5.10 (Quadrate und Rechtecke)**.** Das Produkt

$$[0, 1] \times [0, 1]$$

beschreibt das Einheitsquadrat in der Ebene.

Das Produkt

$$[0, 3] \times [0, 2]$$

beschreibt ein Rechteck mit Breite 3 und Höhe 2.

Beispiel 1.5.11 (Wahrheitswerte)**.** Sei

$$W = \{\text{wahr}, \text{falsch}\}.$$

Dann besteht

$$W \times W$$

aus allen möglichen Paaren von Wahrheitswerten:

$$W \times W = \{(\text{wahr}, \text{wahr}), (\text{wahr}, \text{falsch}), (\text{falsch}, \text{wahr}), (\text{falsch}, \text{falsch})\}.$$

Diese Menge taucht zum Beispiel implizit bei Wahrheitstafeln mit zwei Aussagen auf.

Beispiel 1.5.12 (Zeilen und Spalten)**.** Seien

$$I = \{1, \dots, m\} \qquad \text{und} \qquad J = \{1, \dots, n\}.$$

Dann beschreibt

$$I \times J$$

die Menge aller möglichen Positionen in einem rechteckigen Schema mit m Zeilen und n Spalten.

Später können wir damit zum Beispiel die Einträge einer Matrix indizieren. Ein Matrixeintrag a_{ij} gehört dann zur Position

$$(i, j) \in I \times J.$$

Beispiel 1.5.13 (Studierende und Aufgaben)**.** Sei S die Menge der Studierenden in einer Übung und sei A die Menge der Aufgaben auf einem Übungsblatt. Dann besteht

$$S \times A$$

aus allen Paaren

$$(s, a),$$

wobei s eine studierende Person und a eine Aufgabe ist.

Ein solches Paar kann man lesen als: „Person s bearbeitet Aufgabe a“. Daran sieht man schon, warum kartesische Produkte für Relationen wichtig werden.

Beispiel 1.5.14 (Das Produkt einer Menge mit sich selbst)**.** Für jede Menge X ist

$$X \times X$$

die Menge aller Paare von Elementen aus X.

Ein besonders wichtiges Beispiel ist die sogenannte Diagonale:

$$\Delta_X := \{(x, x) \mid x \in X\}.$$

Sie enthält genau die Paare, bei denen erster und zweiter Eintrag gleich sind.

Auch dies ist bereits ein erstes Beispiel für eine Relation.

Bemerkung 1.5.15 (Descartes und die kartesischen Koordinaten)**.** Das Wort *kartesisch* erinnert an René Descartes. Sein lateinischer Name war Cartesius.

Die Idee der kartesischen Koordinaten besteht darin, Punkte der Ebene durch Zahlenpaare zu beschreiben. Ein Punkt wird also nicht nur geometrisch gezeichnet, sondern durch ein Paar

$$(x, y) \in \mathbb{R} \times \mathbb{R}$$

dargestellt.

Dadurch entsteht eine tiefe Verbindung zwischen Geometrie und Algebra: Geometrische Objekte können durch Gleichungen beschrieben werden, und Gleichungen können als geometrische Objekte sichtbar gemacht werden. Zum Beispiel beschreibt eine Gleichung wie

$$x^2 + y^2 = 1$$

einen Kreis in der Ebene.

Dies war ein revolutionärer Schritt. Geometrische Probleme konnten nun mit algebraischen Methoden untersucht werden, und algebraische Rechnungen erhielten eine geometrische Bedeutung. Genau diese Verbindung führt später zur analytischen Geometrie.

Historisch ist die Entwicklung nicht nur mit Descartes verbunden, sondern auch mit anderen Mathematikern wie Pierre de Fermat. Der Name „kartesisch“ erinnert aber bis heute an diesen großen Perspektivwechsel.

Definition 1.5.16 (Mehrfache kartesische Produkte)**.** Seien $X_1, \dots, X_n$ Mengen. Das *kartesische Produkt* von $X_1, \dots, X_n$ ist die Menge aller n-Tupel

$$(x_1, \dots, x_n),$$

wobei der erste Eintrag aus X_1, der zweite Eintrag aus X_2, und allgemein der i-te Eintrag aus X_i stammt.

Wir schreiben

$$X_1 \times \cdots \times X_n := \{(x_1, \dots, x_n) \mid x_1 \in X_1 \wedge \cdots \wedge x_n \in X_n\}.$$

Also gilt

$$(x_1, \dots, x_n) \in X_1 \times \cdots \times X_n \iff x_1 \in X_1 \wedge \cdots \wedge x_n \in X_n.$$

Bemerkung 1.5.17 (Klammerung bei mehrfachen Produkten)**.** Formal haben wir bisher nur geordnete Paare eingeführt. Daher müsste man ein Tripel eigentlich durch geschachtelte Paare kodieren, zum Beispiel als

$$((a, b), c)$$

oder als

$$(a, (b, c)).$$

Diese beiden Objekte sind formal nicht dasselbe. Sie sind unterschiedlich geklammerte Paare.

In der Praxis wollen wir aber nicht, dass die Klammerung eine eigene mathematische Information trägt. Wir identifizieren daher solche geschachtelten Schreibweisen mit dem Tripel

$$(a, b, c).$$

Die Bedeutung ist: Es gibt einen ersten, einen zweiten und einen dritten Eintrag.

Allgemeiner betrachten wir ein n-Tupel

$$(a_1, \dots, a_n)$$

als ein Objekt mit genau n geordneten Einträgen. Dabei gilt die Gleichheitsregel

$$(a_1, \dots, a_n) = (b_1, \dots, b_n) \iff a_1 = b_1 \wedge \cdots \wedge a_n = b_n.$$

Streng mengentheoretisch kann man n-Tupel durch geschachtelte Paare kodieren. Für unsere Zwecke ist aber nur diese Gleichheitsregel wichtig.

Definition 1.5.18 (Potenzen von Mengen)**.** Sei X eine Menge und sei $n \in \mathbb{N}$. Wenn alle Faktoren in einem kartesischen Produkt gleich X sind, dann schreiben wir

$$X^n := \underbrace{X \times \cdots \times X}_{n\text{-mal}}.$$

Die Elemente von X^n sind also genau die n-Tupel

$$(x_1, \dots, x_n),$$

deren Einträge alle in X liegen.

Beispiel 1.5.19. Für $X = \{0, 1\}$ gilt

$$X^3 = \{0, 1\}^3.$$

Die Elemente sind genau die Tripel aus Nullen und Einsen:

$$\begin{aligned}\{0, 1\}^3 = \{&(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1),\\ &(1, 0, 0), (1, 0, 1), (1, 1, 0), (1, 1, 1)\}.\end{aligned}$$

Beispiel 1.5.20 (Wahrheitstafeln und $\{0, 1\}^n$)**.** Betrachte atomare Aussagen

$$A_1, \dots, A_n.$$

Für jede dieser Aussagen gibt es zwei mögliche Wahrheitswerte: wahr oder falsch.

Wir kodieren diese beiden Wahrheitswerte durch

$$1 = \text{wahr} \qquad \text{und} \qquad 0 = \text{falsch}.$$

Eine vollständige Belegung der Aussagen $A_1, \dots, A_n$ mit Wahrheitswerten ist dann ein n-Tupel

$$(\varepsilon_1, \dots, \varepsilon_n) \in \{0, 1\}^n.$$

Dabei beschreibt ε_i den Wahrheitswert von A_i.

Zum Beispiel bedeutet

$$(1, 0, 1) \in \{0, 1\}^3,$$

dass A_1 wahr, A_2 falsch und A_3 wahr ist.

Die Zeilen einer Wahrheitstafel für n atomare Aussagen entsprechen also genau den Elementen von

$$\{0, 1\}^n.$$

Bemerkung 1.5.21 (Warum hat $\{0, 1\}^n$ genau 2^n Elemente?)**.** Für jeden Eintrag eines Tupels

$$(\varepsilon_1, \dots, \varepsilon_n) \in \{0, 1\}^n$$

gibt es genau zwei Möglichkeiten:

$$0 \qquad \text{oder} \qquad 1.$$

Für den ersten Eintrag gibt es also 2 Möglichkeiten. Für jeden dieser Fälle gibt es für den zweiten Eintrag wieder 2 Möglichkeiten. Damit gibt es für die ersten beiden Einträge

$$2 \cdot 2$$

Möglichkeiten.

Führt man dieses Argument fort, dann erhält man für n Einträge insgesamt

$$\underbrace{2 \cdot 2 \cdots 2}_{n\text{-mal}} = 2^n$$

Möglichkeiten.

Wenn wir für eine endliche Menge A mit $\mathrm{card}(A)$ die Anzahl der Elemente bezeichnen, gilt

$$\mathrm{card}(\{0, 1\}^n) = 2^n.$$

Das erklärt auch die Schreibweise X^n. Wenn X endlich ist und $\mathrm{card}(X) = m$ gilt, dann hat

$$X^n$$

genau

$$m^n$$

Elemente. Die Größe wird also tatsächlich potenziert.

Bemerkung 1.5.22 (Warum heißt es kartesisches Produkt?)**.** Die Bezeichnung *Produkt* ist nicht zufällig. Bezeichnen wir wieder für eine endliche Menge A mit $\mathsf{card}(A)$ die Anzahl der Elemente. Wenn X und Y endliche Mengen sind, dann gilt

$$\mathsf{card}(X \times Y) = \mathsf{card}(X) \cdot \mathsf{card}(Y).$$

Man erhält nämlich für jedes Element von X alle möglichen Elemente von Y als zweite Komponente.

Allgemeiner gilt für endliche Mengen $X_1, \dots, X_n$:

$$\mathsf{card}(X_1 \times \cdots \times X_n) = \mathsf{card}(X_1) \cdots \mathsf{card}(X_n).$$

Das kartesische Produkt übersetzt also die Idee des unabhängigen Kombinierens in Mengen. Die Anzahl der Möglichkeiten multipliziert sich.

1.5.2 Allgemeine Relationen

Definition 1.5.23 (Relation)**.** Seien X und Y Mengen. Eine *Relation* zwischen X und Y ist eine Teilmenge R von $X \times Y$. Eine Relation zwischen X und X heißt auch *Relation auf X*.

Bemerkung 1.5.24. Bemerke, dass wir, um zu prüfen ob R eine Relation zwischen X und Y ist, nur testen müssen ob $R \subseteq X \times Y$ gilt. Das Wort „Relation“ beschreibt also keine besondere Eigenschaften solcher Teilmengen. Offenkundig wird nicht jede Relation eine tiefgehende Interpretation haben. Vielmehr ist das Wort „Relation“ wieder vor allem ein Hinweis darauf, dass wir R als etwas, das Elemente von X mit Elementen von Y verbindet, interpretieren sollen. Um diese Interpretation noch mehr zu betonen, schreiben wir auch

$$xRy \ :\Longleftrightarrow (x, y) \in R\,.$$

Dabei interpretieren wir R als eine Art zweistelliges Prädikat. Die Notation soll an die Notationen $x < y$ oder $x = y$ erinnern.

Leitbeispiel 1.5.25 (Die Geburtstagsfunktion)**.** Das folgende Beispiel wird uns durch den ganzen Abschnitt begleiten. Es ist absichtlich kein mathematisches Beispiel: Alle zentralen Begriffe dieses Abschnitts stecken bereits in einer Situation, die wir jeden Tag im Hörsaal vor uns haben.

Sei J die Menge aller Studierenden eines fiktiven Jahrgangs, sagen wir mit 200 Personen. Sei T die Menge aller 366 Kalendertage (den 29. Februar zählen wir großzügig mit). Auf dem kartesischen Produkt $J \times T$ betrachten wir die Relation

$$G \ := \{(p, t) \in J \times T \mid p \text{ hat am Kalendertag } t \text{ Geburtstag}\}\,,$$

und auf $J \times J$ die Relation

$$R \ := \{(p, q) \in J \times J \mid p \text{ und } q \text{ haben am selben Kalendertag Geburtstag}\}\,.$$

Beide Relationen sind völlig harmlos und jedem vertraut. Genau deshalb eignen sie sich als Prüfstein: An ihnen werden wir alle kommenden Begriffe konkret durchspielen. Drei Leitfragen begleiten uns dabei.

1. Was unterscheidet G strukturell von R? (Antwort: G ist eine *Funktion* in Verkleidung.)
2. Wie viel Information über eine Person vergisst die Zuordnung „Person $\mapsto$ Geburtstag“? (Das führt zu Bild, Injektivität und Surjektivität.)

3. Welche Struktur trägt „am selben Tag Geburtstag haben“? (Das führt zu Äquivalenzrelationen und Partitionen — und ganz am Ende des Abschnitts zurück zu *G*.)

Beispiel 1.5.26 (Relationen in der Mathematik)**.** Relationen begegnen uns überall in der Mathematik.

1. Die Gleichheit auf einer Menge X ist die Relation

$$\Delta_X = \{(x, x) \mid x \in X\} \subseteq X \times X.$$

   Wie bereits erwähnt nennt man Δ_X auch die *Diagonale* von X.

2. Die Kleiner-Relation auf $\mathbb{R}$ ist

$$< \;=\; \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < y\}.$$

3. Die Teilbarkeitsrelation auf $\mathbb{Z}$ ist

$$\mid \;=\; \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \text{ teilt } b\}.$$

   Die Aussage $3 \mid 12$ bedeutet also:

$$(3, 12) \in \mid .$$

4. Für eine feste natürliche Zahl n ist Kongruenz modulo n eine Relation auf $\mathbb{Z}$:

$$a \equiv b \mod n \iff n \mid (a - b).$$

5. Auf $A \times \mathfrak{P}(A)$ ist auch eine Relation E gegeben durch

$$(b, B) \in E \iff b \in B\,.$$

   Man nennt E auch die Elementrelation und schreibt manchmal $\in = E$.

6. Auf der Potenzmenge $\mathfrak{P}(X)$ einer Menge X gibt es die Teilmengenrelation T

$$T \;\subseteq\; \mathfrak{P}(X) \times \mathfrak{P}(X)\,.$$

   Dabei gilt

$$A \subseteq B \iff (A, B) \in T.$$

   Wenn wir T mit $\subseteq$ identifizieren können wir die herrlich verrückte Formel

$$\subseteq \subseteq\; \mathfrak{P}(X) \times \mathfrak{P}(X)\,.$$

   schreiben. Daher muss man mit solchen Identifikationen aufpassen. Aber manchmal ersparen sie einem viel Schreibarbeit.

7. Im $\mathbb{R}^3$ ist Orthogonalität eine Relation:

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

   Dabei ist $\langle v, w\rangle \;:=\; v_1w_1 + v_2w_2 + v_3w_3$ das Standardskalarprodukt. Später werden wir Skalarprodukte genauer studieren.

8. In der Geometrie kann man die Relation

$$P \text{ liegt auf } g$$

zwischen Punkten P und Geraden g betrachten. Dies ist eine Relation zwischen der Menge aller Punkte und der Menge aller Geraden.

9. Für jedes Paar von Mengen (X, Y) ist auch $X \times Y$ eine Relation zwischen X und Y. Dabei steht jedes Element mit jedem anderen Element in Relation.

Beispiel 1.5.27 (Relationen in der normalen Welt)**.** Auch viele alltägliche Verhältnisse lassen sich als Relationen auffassen.

1. „Person p wohnt in Stadt s“ ist eine Relation zwischen Personen und Städten.
2. „Person p ist mit Person q befreundet“ ist eine Relation auf der Menge der Personen.
3. „Person p hat Buch b ausgeliehen“ ist eine Relation zwischen Personen und Büchern.
4. „Studentische Person s besucht Veranstaltung v“ ist eine Relation zwischen Studierenden und Lehrveranstaltungen.
5. „Datei d liegt in Ordner o“ ist eine Relation zwischen Dateien und Ordnern.
6. „E-Mail e wurde an Person p geschickt“ ist eine Relation zwischen E-Mails und Personen.
7. „Tier t gehört zu Art a“ ist eine Relation zwischen Tieren und Arten.

Nicht jede Relation verbindet Elemente eindeutig miteinander. Eine Person kann mehrere Bücher ausgeliehen haben, eine Veranstaltung kann von vielen Studierenden besucht werden, und eine E-Mail kann an mehrere Personen geschickt worden sein.

Definition 1.5.28 (Totalität und Eindeutigkeit von Relationen)**.** Seien X und Y Mengen, und sei

$$R \subseteq X \times Y$$

eine Relation zwischen X und Y.

1. Die Relation R heißt *linkstotal*, wenn jedes Element von X zu mindestens einem Element von Y in Relation steht:
$$\forall x \in X : \exists y \in Y : xRy.$$
2. Die Relation R heißt *rechtstotal*, wenn jedes Element von Y von mindestens einem Element von X getroffen wird:
$$\forall y \in Y : \exists x \in X : xRy.$$
3. Die Relation R heißt *linkseindeutig*, wenn jedes Element von Y von höchstens einem Element von X getroffen wird:
$$\forall x_1, x_2 \in X : \forall y \in Y : (x_1 R y \wedge x_2 R y) \Longrightarrow x_1 = x_2.$$
4. Die Relation R heißt *rechtseindeutig*, wenn jedes Element von X mit höchstens einem Element von Y in Relation steht:
$$\forall x \in X : \forall y_1, y_2 \in Y : (x R y_1 \wedge x R y_2) \Longrightarrow y_1 = y_2.$$

Bemerkung 1.5.29 (Links und rechts)**.** Die Begriffe *links* und *rechts* beziehen sich auf die beiden Seiten des kartesischen Produkts

$$X \times Y.$$

Die Elemente von X stehen links im Paar, die Elemente von Y stehen rechts im Paar.

- *Linkstotal* bedeutet: Alle linken Elemente kommen vor.
- *Rechtstotal* bedeutet: Alle rechten Elemente werden getroffen.
- *Linkseindeutig* bedeutet: Ein rechtes Element kommt von höchstens einem linken Element.
- *Rechtseindeutig* bedeutet: Ein linkes Element geht zu höchstens einem rechten Element.

Die Begriffe sind am Anfang etwas gewöhnungsbedürftig. Die Eselsbrücke ist: *Totalität* sagt, dass alle Elemente einer Seite benutzt werden. *Eindeutigkeit* sagt, dass von der anderen Seite aus höchstens ein Element dieser Seite möglich ist.

Leitbeispiel 1.5.30 (Die Geburtstagsfunktion: Totalität und Eindeutigkeit)**.** Wir prüfen die vier Eigenschaften an der Relation G aus Leitbeispiel 1.5.25.

- G ist *linkstotal*: Jede Person hat mindestens einen Geburtstag. (Niemand ist nie geboren.)
- G ist *rechtseindeutig*: Jede Person hat höchstens einen Geburtstag. (Niemand ist zweimal geboren.)
- G ist *nicht rechtstotal*: Bei 200 Personen und 366 Tagen bleiben zwangsläufig Tage übrig, an denen niemand Geburtstag hat.
- G ist im Allgemeinen *nicht linkseindeutig*: Sobald zwei Personen am selben Tag Geburtstag haben, wird ein rechtes Element von zwei linken getroffen.

Die Kombination „linkstotal und rechtseindeutig“ liest sich zusammen als: *Jede Person hat genau einen Geburtstag*. Diese Kombination ist so wichtig, dass sie im nächsten Unterabschnitt einen eigenen Namen bekommt.

Die Relation R auf $J \times J$ verhält sich ganz anders: Sie ist linkstotal und rechtstotal (jede Person hat am selben Tag wie sie selbst Geburtstag), aber weder links- noch rechtseindeutig, sobald irgendein Geburtstag geteilt wird.

1.5.3 Funktionen

Definition 1.5.31 (Funktion)**.** Seien X und Y Mengen. Eine *Funktion von X nach Y* ist ein Tripel

$$f = (X, Y, \Gamma_f),$$

wobei

$$\Gamma_f \subseteq X \times Y$$

eine linkstotale und rechtseindeutige Relation ist.

Die Menge X heißt *Definitionsbereich* von f. Die Menge Y heißt *Wertebereich* oder *Zielmenge* von f. Die Relation Γ_f heißt der *Graph* von f.

Wir schreiben

$$f\colon\ X \to Y.$$

Für $x \in X$ bezeichnet $f(x)$ das eindeutig bestimmte Element $y \in Y$, für das

$$(x, y) \in \Gamma_f$$

gilt.

Bemerkung 1.5.32 (Warum ist eine Funktion ein Tripel?)**.** Es reicht nicht immer, nur den Graphen einer Funktion zu kennen. Der Wertebereich ist Teil der Daten.

Zum Beispiel haben die beiden Funktionen

$$f\colon \mathbb{R} \to \mathbb{R}, \qquad f(x) = x^2,$$

und

$$g\colon \mathbb{R} \to [0, \infty), \qquad g(x) = x^2,$$

denselben Graphen als Menge von Paaren. Trotzdem sind sie als Funktionen verschieden, weil sie verschiedene Wertebereiche haben.

Diese Unterscheidung ist subtil, aber manchmal wichtig: Die Funktion g ist rechtstotal, die Funktion f aber nicht.

Häufig lässt man den Definitions- und Wertebereich aber einfach weg, wenn er keine Rolle spielt.

Bemerkung 1.5.33 (Der moderne Funktionsbegriff)**.** Diese Definition ist ein sehr allgemeiner Funktionsbegriff. Eine Funktion muss hier nicht durch eine Rechenvorschrift gegeben sein. Sie muss auch nicht stetig, berechenbar, oder zeichnerisch darstellbar sein. Eine Funktion muss nicht einmal durch eine Formel beschreibbar sein.

Entscheidend ist nur: Jedem Element des Definitionsbereichs wird genau ein Element des Wertebereichs zugeordnet.

Historisch ist dieser allgemeine Begriff relativ spät entstanden. Im 17. und 18. Jahrhundert dachte man bei Funktionen oft an Größen, die von anderen Größen abhängen, oder an Ausdrücke, die durch Formeln gegeben sind. Bei Euler waren Funktionen typischerweise noch stark mit analytischen Ausdrücken verbunden.

Im 19. Jahrhundert erzwangen Probleme aus der Analysis, insbesondere Fourierreihen und unstetige Beispiele, einen freieren Funktionsbegriff. Ein wichtiger Schritt ist mit Dirichlet verbunden: Eine Funktion kann jedem x eines Bereichs ein eindeutig bestimmtes y zuordnen, ohne dass diese Zuordnung durch eine einfache Formel gegeben sein muss.

Erst mit der Entwicklung der Mengenlehre bei Cantor, Dedekind, Frege und anderen wurde es natürlich, Funktionen als Mengen von geordneten Paaren zu verstehen. Im 20. Jahrhundert wurde diese Sichtweise durch die axiomatische Mengenlehre und die strukturelle Sprache der modernen Mathematik weiter stabilisiert.

Der moderne Funktionsbegriff trennt also die Idee der Zuordnung radikal von der Idee einer Rechenvorschrift. Das ist einer der Gründe, warum er so mächtig ist.

Leitbeispiel 1.5.34 (Die Geburtstagsfunktion ist eine Funktion)**.** Die Relation G aus Leitbeispiel 1.5.25 ist linkstotal und rechtseindeutig. Das Tripel (J, T, G) ist also tatsächlich eine Funktion

$$\mathrm{geb}\colon J \to T, \qquad \mathrm{geb}(p) = \text{der Kalendertag, an dem } p \text{ Geburtstag hat.}$$

Ab jetzt nennen wir sie die *Geburtstagsfunktion*.

Zwei Beobachtungen passen genau zur bisherigen Diskussion.

1. geb ist eine Funktion ganz ohne „Rechenvorschrift“: Es gibt keine Formel, die aus einer Person ihren Geburtstag berechnet. Die Zuordnung ist trotzdem für jede Person eindeutig festgelegt — genau das ist der moderne Funktionsbegriff aus der letzten Bemerkung.

2. Der Wertebereich ist Teil des Tripels und damit Teil der Funktion. Das Tripel (J, T', G), in dem T' nur die tatsächlich vorkommenden Geburtstage enthält, hätte denselben Graphen, wäre aber eine *andere* Funktion. Warum diese Unterscheidung sinnvoll ist, sehen wir bei der Surjektivität.

Beispiel 1.5.35 (Funktionen)**.** Die folgenden Beispiele sind Funktionen.

1. Die Identität auf einer Menge X ist die Funktion

$$\mathrm{Id}_X : X \to X, \qquad \mathrm{Id}_X(x) = x.$$

   Ihr Graph ist die Diagonale

$$\Gamma_{\mathrm{Id}_X} = \Delta_X.$$

2. Die Quadratfunktion

$$f : \mathbb{R} \to \mathbb{R}, \qquad f(x) = x^2,$$

   ist eine Funktion. Jeder reellen Zahl wird genau eine reelle Zahl zugeordnet.

3. Die Betragsfunktion

$$B : \mathbb{R} \to [0, \infty), \qquad B(x) = |x|,$$

   ist eine Funktion.

4. Für Mengen X und Y und jedes feste Element $y_0 \in Y$ gibt es die konstante Funktion

$$c_{y_0} : X \to Y, \qquad c_{y_0}(x) = y_0.$$

   Auch die Abbildung $y_0 \mapsto c_{y_0}$ ist eine Funktion. Aufgabe: Was ist der Definitions- und Wertebereich?

5. Ist $A \subseteq X$, dann ist die sogenannte „Inklusionsabbildung“

$$\iota : A \to X, \qquad \iota(a) = a,$$

   eine Funktion.

6. Für Mengen X und Y ist die Projektion auf die erste Komponente

$$\pi_1 : X \times Y \to X, \qquad \pi_1(x, y) = x,$$

   eine Funktion.

7. Für Mengen X und Y ist die Projektion auf die zweite Komponente

$$\pi_2 : X \times Y \to Y, \qquad \pi_2(x, y) = y,$$

   eine Funktion.

8. Sei $W = \bigcup_{n \in \mathbb{N}} \{0, 1\}^n$ die Menge aller endlichen Wörter die aus 0 und 1 bestehen. Die Länge eines Wortes ist eine Funktion

$$\ell : W \to \mathbb{N},$$

   wobei $\ell(w)$ die Anzahl der Zeichen des Wortes $w \in W$ ist.

9. Wenn jede Person genau eine Matrikelnummer besitzt, dann ist die Zuordnung

$$\text{Person} \longmapsto \text{Matrikelnummer}$$

   eine Funktion von der Menge der Studierenden in die Menge der Matrikelnummern.

10. Die Zuordnung
$$n \longmapsto n^2$$
ist eine Funktion von $\mathbb{N}$ nach $\mathbb{N}$.

11. Die Zuordnung
$$A \longmapsto \operatorname{card}(A)$$
ist eine Funktion von der Menge aller endlichen Teilmengen einer festen Menge X nach $\mathbb{N}_0$.

12. Die Funktion
$$\mathbb{1}_A : X \to \{0,1\}, \qquad \mathbb{1}_A(x) = \begin{cases} 1, & x \in A, \\ 0, & x \notin A, \end{cases}$$
heißt *Indikatorfunktion* und manchmal auch *charakteristische Funktion* der Teilmenge $A \subseteq X$.

Beispiel 1.5.36 (Relationen, die keine Funktionen sind)**.** Die folgenden Relationen sind keine Funktionen.

1. Die Relation
$$R = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid x < y\}$$
ist keine Funktion von $\mathbb{R}$ nach $\mathbb{R}$. Zu einem festen x gibt es nämlich viele y mit $x < y$.

2. Die Relation
$$R = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid y^2 = x\}$$
ist keine Funktion von $\mathbb{R}$ nach $\mathbb{R}$. Für $x = 1$ gibt es zwei mögliche Werte, nämlich $y = 1$ und $y = -1$. Für $x = -1$ gibt es gar keinen reellen Wert y.

3. Die Relation
$$R = \{(p,b) \mid \text{Person } p \text{ hat Buch } b \text{ ausgeliehen}\}$$
ist im Allgemeinen keine Funktion. Eine Person kann kein Buch, ein Buch oder mehrere Bücher ausgeliehen haben.

4. Die Relation
$$R = \{(p,q) \mid p \text{ ist ein Geschwister von } q\}$$
ist im Allgemeinen keine Funktion. Eine Person kann mehrere Geschwister haben.

Definition 1.5.37 (Bild)**.** Sei
$$f : X \to Y$$
eine Funktion. Für eine Teilmenge $A \subseteq X$ definieren wir das *Bild* von A unter f durch
$$f(A) := \{f(a) \mid a \in A\}.$$
Insbesondere heißt
$$f(X) = \{f(x) \mid x \in X\}$$
das *Bild* von f.

Bemerkung 1.5.38 ($f(a)$ vs. $f(\{a\})$)**.** Das Bild eines Elements des Definitionsbereichs ist selber ein Element im Wertebereich. Sei also $x \in X$ und $f : X \to Y$. Dann ist $f(x) \in Y$.

Anders verhält es sich bei dem Bild der Menge $\{x\}$. Dieses ist die Menge $\{f(x)\}$ und damit kein Element, sondern eine Teilmenge von Y.

Definition 1.5.39 (Urbild)**.** Sei

$$f\colon X \to Y$$

eine Funktion. Für eine Teilmenge $B \subseteq Y$ definieren wir das *Urbild* von B unter f durch

$$f^{-1}(B) := \{x \in X \mid f(x) \in B\}.$$

Bemerkung 1.5.40 (Achtung: das Urbild $f^{-1}(B)$ ist keine Umkehrfunktion)**.** Das Urbild $f^{-1}(B)$ ist für *jede* Funktion definiert und bezeichnet eine *Menge* — nämlich alles, was f nach B hineinschickt. Diese Menge kann leer sein, ein Element enthalten oder viele.

Später in diesem Abschnitt lernen wir die *Umkehrfunktion* kennen, die ebenfalls f^{-1} geschrieben wird — sie existiert aber nur für bijektive Funktionen. Die beiden Schreibweisen vertragen sich: Wenn die Umkehrfunktion existiert, ist das Urbild $f^{-1}(B)$ genau das Bild von B unter der Umkehrfunktion (Übung). Das Urbild gibt es dagegen *immer*, auch wenn f nicht bijektiv ist.

Leitbeispiel 1.5.41 (Die Geburtstagsfunktion: Bild und Urbild)**.** Für die Geburtstagsfunktion $\mathrm{geb}\colon J \to T$ ist

$$\mathrm{geb}(J) = \{t \in T \mid \text{mindestens eine Person hat am Tag } t \text{ Geburtstag}\}$$

die Menge der *tatsächlich vorkommenden* Geburtstage. Bei 200 Personen und 366 Tagen gilt sicher $\mathrm{geb}(J) \neq T$: Das Bild kann höchstens 200 Tage enthalten, mindestens 166 Tage kommen also nicht vor. Der Wertebereich T und das Bild $\mathrm{geb}(J)$ sind zwei verschiedene Dinge.

Genauso interessant ist die umgekehrte Blickrichtung. Für einen festen Tag $t \in T$ ist

$$\mathrm{geb}^{-1}(\{t\}) = \{p \in J \mid \mathrm{geb}(p) = t\}$$

das *Urbild* von $\{t\}$ (üblich ist auch der Name „die *Faser* von geb über t“). Anschaulich: geb sortiert den Jahrgang in 366 Schubladen, eine pro Kalendertag. Wir schreiben $F_t := \mathrm{geb}^{-1}(\{t\})$. Das Urbild F_t ist der Inhalt der Schublade t, und das Bild $\mathrm{geb}(J)$ ist die Menge der Tage, deren Schublade nicht leer ist.

Dieses Bild lohnt sich zu merken: *Jede* Funktion sortiert ihren Definitionsbereich auf diese Weise in Schubladen. Am Ende des Abschnitts bekommt das Sortieren in Schubladen einen offiziellen Namen.

Definition 1.5.42 (Einschränkung einer Funktion)**.** Sei

$$f\colon X \to Y$$

eine Funktion, und sei $A \subseteq X$. Die *Einschränkung* von f auf A ist die Funktion

$$f|_A\colon A \to Y, \qquad f|_A(a) = f(a).$$

Ihr Graph ist

$$\Gamma_{f|_A} = \Gamma_f \cap (A \times Y).$$

Bemerkung 1.5.43 (Einschränkung des Wertebereichs)**.** Manchmal möchte man nicht den Definitionsbereich, sondern den Wertebereich verkleinern.

Sei

$$f\colon X \to Y$$

eine Funktion, und sei $B \subseteq Y$. Wenn

$$f(X) \subseteq B$$

gilt, dann kann man dieselbe Zuordnung auch als Funktion

$$f\colon\ X \to B$$

auffassen.

Streng genommen ändert sich dabei die Funktion als Tripel, weil sich der Wertebereich ändert. Der Graph bleibt aber derselbe.

Beispiel 1.5.44 (Einschränkungen)**.** Die Quadratfunktion

$$f\colon\ \mathbb{R} \to \mathbb{R}, \qquad f(x) = x^2,$$

ist auf ganz $\mathbb{R}$ nicht eindeutig umkehrbar.

Schränkt man aber den Definitionsbereich auf $[0, \infty)$ ein, dann erhält man

$$f|_{[0,\infty)}\colon\ [0, \infty) \to \mathbb{R}, \qquad f|_{[0,\infty)}(x) = x^2.$$

Schränkt man außerdem den Wertebereich auf $[0, \infty)$ ein, dann erhält man die Funktion

$$[0, \infty) \to [0, \infty), \qquad x \longmapsto x^2.$$

Definition 1.5.45 (Injektivität)**.** Eine Funktion

$$f\colon\ X \to Y$$

heißt *injektiv*, wenn unterschiedliche Elemente von X auch unterschiedliche Werte in Y haben.

Formal bedeutet das:

$$\forall x_1, x_2 \in X\ :\ f(x_1) = f(x_2) \Longrightarrow x_1 = x_2.$$

Äquivalent dazu:

$$x_1 \neq x_2 \Longrightarrow f(x_1) \neq f(x_2).$$

In der Sprache der Relationen bedeutet das: Der Graph Γ_f ist linkseindeutig.

Definition 1.5.46 (Surjektivität)**.** Eine Funktion

$$f\colon\ X \to Y$$

heißt *surjektiv*, wenn jedes Element des Wertebereichs tatsächlich als Wert angenommen wird.

Formal bedeutet das:

$$\forall y \in Y\ :\ \exists x \in X\ :\ f(x) = y.$$

Äquivalent dazu:

$$f(X) = Y.$$

In der Sprache der Relationen bedeutet das: Der Graph Γ_f ist rechtstotal.

Definition 1.5.47 (Bijektivität)**.** Eine Funktion

$$f\colon\ X \to Y$$

heißt *bijektiv*, wenn sie injektiv und surjektiv ist.

In der Sprache der Relationen bedeutet das: Der Graph Γ_f ist gleichzeitig linkstotal, rechtstotal, linkseindeutig und rechtseindeutig.

Also: Jedes Element von X hat genau ein Bild in Y, und jedes Element von Y kommt von genau einem Element aus X.

Beispiel 1.5.48 (Injektiv, surjektiv, bijektiv)**.**

1. Die Identität
$$\mathrm{Id}_X\colon\ X \to X$$
ist bijektiv.

2. Die Inklusion
$$\iota\colon\ A \to X, \qquad \iota(a) = a,$$
ist injektiv. Sie ist genau dann surjektiv, wenn $A = X$ gilt.

3. Die Quadratfunktion
$$f\colon\ \mathbb{R} \to \mathbb{R}, \qquad f(x) = x^2,$$
ist nicht injektiv, denn
$$f(1) = f(-1).$$
Sie ist auch nicht surjektiv, denn es gibt kein $x \in \mathbb{R}$ mit
$$x^2 = -1.$$

4. Die Funktion
$$g\colon\ \mathbb{R} \to [0, \infty), \qquad g(x) = x^2,$$
ist surjektiv, aber nicht injektiv.

5. Die Funktion
$$h\colon\ [0, \infty) \to [0, \infty), \qquad h(x) = x^2,$$
ist bijektiv.

6. Die Exponentialfunktion
$$\exp\colon\ \mathbb{R} \to (0, \infty), \qquad x \longmapsto e^x,$$
ist bijektiv.

7. Die Funktion
$$\sin\colon\ \mathbb{R} \to \mathbb{R}$$
ist weder injektiv noch surjektiv.

8. Die Funktion
$$\sin\colon\ \mathbb{R} \to [-1, 1]$$
ist surjektiv, aber nicht injektiv.

9. Die Einschränkung
$$\sin|_{[-\frac{\pi}{2},\frac{\pi}{2}]}\colon [-\frac{\pi}{2},\frac{\pi}{2}] \to [-1,1]$$
ist bijektiv.

10. Ist Y nicht leer und $y_0 \in Y$, dann ist die konstante Funktion
$$c\colon X \to Y, \qquad c(x) = y_0,$$
genau dann injektiv, wenn X höchstens ein Element hat. Sie ist genau dann surjektiv, wenn $Y = \{y_0\}$ gilt.

Leitbeispiel 1.5.49 (Die Geburtstagsfunktion: injektiv, surjektiv, bijektiv?)**.** Die drei Begriffe lassen sich an der Geburtstagsfunktion geb : $J \to T$ wörtlich übersetzen.

- geb ist *injektiv* genau dann, wenn keine zwei Personen am selben Tag Geburtstag haben — wenn also jede Schublade aus Leitbeispiel 1.5.41 höchstens eine Person enthält. Injektivität bedeutet: *Es geht keine Information verloren.* Aus dem Geburtstag ließe sich die Person eindeutig rekonstruieren.
- geb ist *surjektiv* genau dann, wenn an jedem der 366 Tage jemand Geburtstag hat — wenn also keine Schublade leer bleibt. Mit 200 Personen ist das unmöglich.
- *Bijektiv* wäre geb nur in einem Jahrgang mit exakt 366 Personen und perfekt verteilten Geburtstagen: jede Schublade genau einmal besetzt.

Zwei Beobachtungen mit mehr Tiefgang:

1. Stellen wir uns kurz einen größeren Jahrgang vor: Ab 367 Personen ist geb *garantiert* nicht mehr injektiv, denn 367 Personen verteilen sich auf 366 Schubladen, also enthält irgendeine Schublade mindestens zwei Personen. Dieses Argument heißt *Schubfachprinzip* und ist trotz seiner Harmlosigkeit ein erstaunlich starkes Beweiswerkzeug.
2. Schon bei 200 Personen wäre Injektivität zwar möglich, aber extrem unwahrscheinlich. (Bereits ab 23 Personen ist ein geteilter Geburtstag wahrscheinlicher als keiner — das sogenannte *Geburtstagsparadoxon*. Es ist kein echtes Paradoxon, sondern eine Erinnerung daran, wie schlecht unsere Intuition für Wahrscheinlichkeiten kalibriert ist. Rechnen müssen Sie das hier nicht — Wahrscheinlichkeiten sind in diesem Skript kein Stoff.)

Und noch einmal der Wertebereich: Die Funktion geb : $J \to T$ ist nicht surjektiv, aber die Funktion $J \to \mathrm{geb}(J)$ mit derselben Zuordnung ist es. Surjektivität ist keine Eigenschaft der Zuordnung allein, sondern hängt am gewählten Wertebereich — genau deshalb steckt der Wertebereich mit im Tripel.

Definition 1.5.50 (Komposition von Funktionen)**.** Seien
$$f\colon X \to Y \qquad \text{und} \qquad g\colon Y \to Z$$
Funktionen. Die *Komposition* von f und g ist die Funktion
$$g \circ f\colon X \to Z$$
mit
$$(g \circ f)(x) = g(f(x)).$$

Lemma 1.5.51 (Assoziativität der Komposition)**.** *Seien $h : A \to B$, $g : B \to C$ und $f : C \to D$ Funktionen. Dann gilt*

$$(f \circ g) \circ h = f \circ (g \circ h).$$

Beweis. Wir zeigen Gleichheit von Funktionen, indem wir die Auswertung auf beliebigen Elementen vergleichen.

Sei also $x \in A$ beliebig. Dann gilt

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))).$$

Andererseits ist

$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))).$$

Damit stimmen beide Seiten für alle $x \in A$ überein, also sind die Funktionen gleich. □

Bemerkung 1.5.52. Im obigen Beweis passiert in gewisser Weise „gar nicht so viel“: Die Klammern spielen keine echte Rolle, weil die Reihenfolge der Auswertung fest vorgegeben ist.

Egal wie man klammert, für jedes x erhält man immer denselben Ausdruck

$$f \circ g \circ h(x) = f(g(h(x))).$$

Die Komposition liest sich also von rechts nach links: Zuerst wird h angewendet, dann g, dann f.

Definition 1.5.53 (Umkehrfunktion)**.** Sei

$$f\colon X \to Y$$

eine Funktion. Eine Funktion

$$g : Y \to X$$

heißt *Umkehrfunktion* von f, wenn

$$g \circ f = \mathrm{Id}_X$$

und

$$f \circ g = \mathrm{Id}_Y$$

gilt.

Wenn eine Umkehrfunktion existiert, dann schreiben wir sie als

$$f^{-1} : Y \to X.$$

Bemerkung 1.5.54 (Links- und Rechtsinverse)**.** Sei

$$f\colon X \to Y$$

eine Funktion.

Eine Funktion

$$g : Y \to X$$

heißt *Linksinverse* von f, wenn

$$g \circ f = \mathrm{Id}_X$$

gilt. Sie steht in der Komposition links von f.

Eine Funktion

$$h\colon\ Y \to X$$

heißt *Rechtsinverse* von f, wenn

$$f \circ h = \mathrm{Id}_Y$$

gilt. Sie steht in der Komposition rechts von f.

Eine Umkehrfunktion ist also gleichzeitig Links- und Rechtsinverse.

Proposition 1.5.55 (Injektivität und Linksinversen)**.** *Sei*

$$f\colon\ X \to Y$$

eine Funktion.

Wenn f eine Linksinverse besitzt, dann ist f injektiv.

Ist umgekehrt $X \neq \emptyset$ und f injektiv, dann besitzt f eine Linksinverse.

Beweis. Sei zunächst

$$g\colon\ Y \to X$$

eine Linksinverse von f. Dann gilt

$$g \circ f = \mathrm{Id}_X.$$

Seien nun $x_1, x_2 \in X$ mit

$$f(x_1) = f(x_2).$$

Wenden wir g auf beide Seiten an, dann erhalten wir

$$g(f(x_1)) = g(f(x_2)).$$

Da $g \circ f = \mathrm{Id}_X$ gilt, folgt

$$x_1 = x_2.$$

Also ist f injektiv.

Für die Umkehrung sei nun $X \neq \emptyset$, und sei f injektiv. Wähle ein festes Element $x_0 \in X$.

Wir definieren

$$g\colon\ Y \to X$$

folgendermaßen. Wenn $y \in f(X)$ gilt, dann gibt es wegen der Definition des Bildes ein $x \in X$ mit

$$f(x) = y.$$

Wegen der Injektivität von f ist dieses x eindeutig. Wir setzen dann

$$g(y) = x.$$

Wenn $y \notin f(X)$ gilt, setzen wir

$$g(y) = x_0.$$

Dann gilt für jedes $x \in X$:

$$g(f(x)) = x.$$

Also gilt

$$g \circ f = \mathrm{Id}_X.$$

Damit ist g eine Linksinverse von f. □

Bemerkung 1.5.56 (Der leere Definitionsbereich)**.** Die Voraussetzung $X \neq \emptyset$ in der Rückrichtung ist nur wegen eines Randfalls nötig.

Die eindeutige Funktion

$$\emptyset \to Y$$

ist immer injektiv. Wenn aber $Y \neq \emptyset$ gilt, kann es keine Funktion

$$Y \to \emptyset$$

geben. Dann kann also auch keine Linksinverse existieren.

Proposition 1.5.57 (Surjektivität und Rechtsinverse)**.** *Sei*

$$f\colon X \to Y$$

eine Funktion.

Wenn f eine Rechtsinverse besitzt, dann ist f surjektiv.

Umgekehrt gilt: Wenn f surjektiv ist und man für jedes $y \in Y$ ein Element $x \in X$ mit $f(x) = y$ wählen kann, dann besitzt f eine Rechtsinverse.

Beweis. Sei zunächst

$$h\colon Y \to X$$

eine Rechtsinverse von f. Dann gilt

$$f \circ h = \mathrm{Id}_Y.$$

Sei $y \in Y$. Dann gilt

$$y = \mathrm{Id}_Y(y) = (f \circ h)(y) = f(h(y)).$$

Also gibt es ein Element von X, nämlich $h(y)$, das unter f auf y abgebildet wird. Daher ist f surjektiv.

Für die Umkehrung sei f surjektiv. Dann gibt es für jedes $y \in Y$ mindestens ein $x \in X$ mit

$$f(x) = y.$$

Wählen wir für jedes y ein solches Element und nennen es $h(y)$, dann erhalten wir eine Funktion

$$h\colon Y \to X$$

mit

$$f(h(y)) = y$$

für alle $y \in Y$. Also gilt

$$f \circ h = \mathrm{Id}_Y.$$

Damit ist h eine Rechtsinverse von f. □

Bemerkung 1.5.58 (Auswahlaxiom)**.** Bei endlichen Mengen und bei konkret angegebenen Funktionen ist die Wahl von $h(y)$ meistens völlig harmlos. Bei beliebigen unendlichen Mengen steckt in der Aussage „wähle für jedes y ein Element seines Urbilds“ ein mengentheoretisches Auswahlprinzip, das Auswahlaxiom.

Für diese Vorlesung ist vor allem die Idee wichtig: Eine Rechtsinverse wählt zu jedem Element des Wertebereichs ein Element seines Urbilds aus.

Proposition 1.5.59 (Bijektivität und Umkehrfunktionen)**.** *Sei*

$$f\colon X \to Y$$

eine Funktion. Dann ist f genau dann bijektiv, wenn f eine Umkehrfunktion besitzt.

Beweis. Angenommen, f besitzt eine Umkehrfunktion

$$g\colon Y \to X.$$

Dann gilt

$$g \circ f = \mathrm{Id}_X$$

und

$$f \circ g = \mathrm{Id}_Y.$$

Aus der ersten Gleichung folgt, dass f eine Linksinverse besitzt. Also ist f injektiv.

Aus der zweiten Gleichung folgt, dass f eine Rechtsinverse besitzt. Also ist f surjektiv.

Damit ist f bijektiv.

Sei umgekehrt f bijektiv. Dann gibt es für jedes $y \in Y$ genau ein $x \in X$ mit

$$f(x) = y.$$

Wir definieren

$$g\colon Y \to X$$

durch

$$g(y) = \text{das eindeutig bestimmte } x \in X \text{ mit } f(x) = y.$$

Dann gilt für jedes $x \in X$:

$$g(f(x)) = x.$$

Also gilt

$$g \circ f = \mathrm{Id}_X.$$

Außerdem gilt für jedes $y \in Y$:

$$f(g(y)) = y.$$

Also gilt

$$f \circ g = \mathrm{Id}_Y.$$

Damit ist g eine Umkehrfunktion von f. □

Bemerkung 1.5.60 (Eindeutigkeit der Umkehrfunktion)**.** Wenn eine Umkehrfunktion existiert, dann ist sie eindeutig.

Angenommen,

$$g, h\colon Y \to X$$

sind beide Umkehrfunktionen von

$$f\colon X \to Y.$$

Dann gilt

$$g \circ f = \mathrm{Id}_X, \qquad f \circ h = \mathrm{Id}_Y.$$

Daher folgt

$$g = g \circ \mathrm{Id}_Y = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{Id}_X \circ h = h.$$

Also gibt es höchstens eine Umkehrfunktion.

Beispiel 1.5.61 (Umkehrfunktionen)**.**

1. Die Funktion
$$f\colon \mathbb{R} \to \mathbb{R}, \qquad f(x) = x + 3,$$
ist bijektiv. Ihre Umkehrfunktion ist
$$f^{-1}\colon \mathbb{R} \to \mathbb{R}, \qquad f^{-1}(y) = y - 3.$$

2. Die Funktion
$$f\colon \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{0\}, \qquad f(x) = \frac{1}{x},$$
ist bijektiv und ihre eigene Umkehrfunktion.

3. Die Funktion
$$f\colon [0, \infty) \to [0, \infty), \qquad f(x) = x^2,$$
ist bijektiv. Ihre Umkehrfunktion ist
$$f^{-1}(y) = \sqrt{y}.$$

4. Die Funktion
$$\exp\colon \mathbb{R} \to (0, \infty)$$
ist bijektiv. Ihre Umkehrfunktion ist
$$\log\colon (0, \infty) \to \mathbb{R}.$$

5. Die Funktion
$$f\colon \mathbb{R} \to [0, \infty), \qquad f(x) = x^2,$$
hat keine Umkehrfunktion. Sie ist zwar surjektiv, aber nicht injektiv.

6. Die Funktion
$$f\colon [0, \infty) \to \mathbb{R}, \qquad f(x) = x^2,$$
hat keine Umkehrfunktion. Sie ist zwar injektiv, aber nicht surjektiv.

7. Die Funktion
$$f\colon \mathbb{R} \to \mathbb{R}, \qquad f(x) = x^3,$$
ist bijektiv. Ihre Umkehrfunktion ist
$$f^{-1}(y) = \sqrt[3]{y}.$$

Beispiel 1.5.62 (Injektiv oder surjektiv allein genügt nicht)**.** Wir betrachten zwei sehr kleine Beispiele.

1. Seien
$$A = \{1\} \quad \text{und} \quad B = \{1, 2\}.$$
Wir definieren
$$f : A \to B, \quad f(1) = 1.$$
Dann ist f injektiv. Das ist klar, denn in A gibt es nur ein Element.

Die Funktion f ist aber nicht surjektiv. Das Element $2 \in B$ wird von keinem Element aus A getroffen.

Nach dem Satz über Linksinverse besitzt f eine Linksinverse. Eine solche Linksinverse ist zum Beispiel

$$l : B \to A, \quad l(1) = 1, \quad l(2) = 1.$$

Dann gilt tatsächlich

$$(l \circ f)(1) = l(f(1)) = l(1) = 1.$$

Also gilt

$$l \circ f = \mathrm{Id}_A .$$

Die Funktion f besitzt aber keine Rechtsinverse. Denn eine Rechtsinverse wäre eine Funktion

$$r : B \to A$$

mit

$$f \circ r = \mathrm{Id}_B .$$

Dann müsste insbesondere

$$(f \circ r)(2) = 2$$

gelten. Aber für jedes $x \in A$ gilt

$$f(x) = 1.$$

Also kann $f(r(2))$ niemals gleich 2 sein. Daher gibt es keine Rechtsinverse.

Insbesondere besitzt f keine Umkehrfunktion.

2. Seien nun

$$A = \{1, 2\} \quad \text{und} \quad B = \{1\}.$$

Wir definieren

$$g : A \to B, \quad g(1) = 1, \quad g(2) = 1.$$

Dann ist g surjektiv. Das einzige Element von B wird getroffen.

Die Funktion g ist aber nicht injektiv. Denn

$$1 \neq 2, \quad \text{aber} \quad g(1) = g(2).$$

Nach dem Satz über Rechtsinverse besitzt g eine Rechtsinverse. Eine solche Rechtsinverse ist zum Beispiel

$$r : B \to A, \quad r(1) = 1.$$

Dann gilt

$$(g \circ r)(1) = g(r(1)) = g(1) = 1.$$

Also gilt

$$g \circ r = \mathrm{Id}_B .$$

Die Funktion g besitzt aber keine Linksinverse. Denn eine Linksinverse wäre eine Funktion

$$l : B \to A$$

mit

$$l \circ g = \mathrm{Id}_A .$$

Dann müsste gelten

$$(l \circ g)(1) = 1 \quad \text{und} \quad (l \circ g)(2) = 2.$$

Da aber

$$g(1) = g(2) = 1$$

ist, wäre dies

$$l(1) = 1 \quad \text{und} \quad l(1) = 2.$$

Das ist unmöglich. Daher gibt es keine Linksinverse.

Insbesondere besitzt auch g keine Umkehrfunktion.

Bemerkung 1.5.63. Diese Beispiele zeigen: Eine Umkehrfunktion ist stärker als nur eine Linksinverse oder nur eine Rechtsinverse.

Eine Funktion kann injektiv sein und trotzdem keine Umkehrfunktion besitzen. Dann fehlt im Allgemeinen die Surjektivität.

Eine Funktion kann surjektiv sein und trotzdem keine Umkehrfunktion besitzen. Dann fehlt im Allgemeinen die Injektivität.

Eine echte Umkehrfunktion muss beides gleichzeitig leisten: Sie muss sowohl Links- als auch Rechtsinverse sein.

Definition 1.5.64 (Menge der Funktionen nach $\{0,1\}$)**.** Sei A eine Menge. Wir schreiben

$$\{0,1\}^A$$

für die Menge aller Funktionen von A nach $\{0,1\}$. Also:

$$\{0,1\}^A := \{f \mid f\colon\ A \to \{0,1\} \text{ ist eine Funktion}\}.$$

Ein Element von $\{0,1\}^A$ ist also keine Zahl, sondern eine Funktion

$$f\colon\ A \to \{0,1\}.$$

Definition 1.5.65 (Indikatorfunktionen Revisited)**.** Sei A eine Menge, und sei $B \subseteq A$. Die *Indikatorfunktion* von B ist die Funktion

$$\mathbb{1}_B\colon\ A \to \{0,1\}$$

mit

$$\mathbb{1}_B(a) = \begin{cases} 1, & a \in B, \\ 0, & a \notin B. \end{cases}$$

Die Indikatorfunktion speichert also für jedes Element von A, ob es zu B gehört oder nicht.

Proposition 1.5.66 (Teilmengen und Indikatorfunktionen)**.** *Sei A eine Menge. Dann gibt es eine kanonische Bijektion*

$$\mathfrak{P}(A) \longrightarrow \{0,1\}^A.$$

Sie ordnet jeder Teilmenge ihre Indikatorfunktion zu.

Beweis. Wir definieren zunächst eine Abbildung

$$\Phi : \mathfrak{P}(A) \to \{0,1\}^A$$

durch

$$\Phi(B) = \mathbb{1}_B$$

für alle $B \subseteq A$.

Wir definieren außerdem eine Abbildung

$$\Psi : \{0,1\}^A \to \mathfrak{P}(A)$$

durch

$$\Psi(f) = \{a \in A \mid f(a) = 1\}.$$

Die Menge $\Psi(f)$ ist also die Menge aller Elemente von A, die von f auf 1 abgebildet werden.

Wir zeigen nun, dass Φ und Ψ invers zueinander sind.

Sei zuerst $B \subseteq A$. Dann gilt für jedes $a \in A$:

$$a \in \Psi(\Phi(B)) \iff \Phi(B)(a) = 1.$$

Nach Definition von Φ ist $\Phi(B) = \mathbb{1}_B$. Also gilt

$$a \in \Psi(\Phi(B)) \iff \mathbb{1}_B(a) = 1.$$

Nach Definition der Indikatorfunktion gilt

$$\mathbb{1}_B(a) = 1 \iff a \in B.$$

Zusammen erhalten wir

$$a \in \Psi(\Phi(B)) \iff a \in B.$$

Da dies für alle $a \in A$ gilt, folgt

$$\Psi(\Phi(B)) = B.$$

Also gilt

$$\Psi \circ \Phi = \mathrm{Id}_{\mathfrak{P}(A)}.$$

Sei nun umgekehrt

$$f \in \{0,1\}^A.$$

Wir müssen zeigen, dass

$$\Phi(\Psi(f)) = f$$

gilt. Zwei Funktionen sind gleich, wenn sie denselben Definitionsbereich, denselben Wertebereich und dieselben Werte an allen Stellen haben.

Beide Funktionen

$$\Phi(\Psi(f)) \qquad \text{und} \qquad f$$

sind Funktionen von A nach $\{0,1\}$. Es genügt also zu zeigen, dass sie an jeder Stelle $a \in A$ denselben Wert haben.

Sei $a \in A$. Dann gilt

$$\Phi(\Psi(f))(a) = \mathbb{1}_{\Psi(f)}(a).$$

Nach Definition der Indikatorfunktion gilt

$$\mathbb{1}_{\Psi(f)}(a) = 1 \iff a \in \Psi(f).$$

Nach Definition von Ψ gilt

$$a \in \Psi(f) \iff f(a) = 1.$$

Also gilt

$$\Phi(\Psi(f))(a) = 1 \iff f(a) = 1.$$

Da sowohl $\Phi(\Psi(f))(a)$ als auch $f(a)$ Elemente von $\{0, 1\}$ sind, folgt daraus bereits

$$\Phi(\Psi(f))(a) = f(a).$$

Da dies für alle $a \in A$ gilt, folgt

$$\Phi(\Psi(f)) = f.$$

Also gilt

$$\Phi \circ \Psi = \mathrm{Id}_{\{0,1\}^A}.$$

Damit sind Φ und Ψ invers zueinander. Insbesondere ist Φ eine Bijektion. □

Bemerkung 1.5.67 (Was hier abstrakt passiert)**.** Die Proposition sagt nicht, dass eine Teilmenge dasselbe Objekt ist wie eine Funktion. Eine Teilmenge $B \subseteq A$ und ihre Indikatorfunktion

$$\mathbb{1}_B \colon A \to \{0, 1\}$$

sind formal verschiedene mathematische Objekte.

Die Proposition sagt aber, dass beide Objekte dieselbe Information enthalten.

Die Teilmenge B beantwortet für jedes $a \in A$ die Frage:

„Gehört a zu B?“

Die Indikatorfunktion $\mathbb{1}_B$ beantwortet dieselbe Frage durch den Wert 1 oder 0.

Wir wechseln also zwischen zwei Darstellungsformen derselben Information:

$$\text{Teilmengen von } A \qquad \longleftrightarrow \qquad \{0, 1\}\text{-wertige Funktionen auf } A.$$

Das ist bereits ein sehr abstrakter Gedanke. Wir betrachten nicht nur konkrete Elemente, sondern ganze Arten, Information zu kodieren.

Definition 1.5.68 (Tupel als Funktionen)**.** Sei

$$I_n := \{1, \dots, n\}.$$

Ein Element von

$$\{0, 1\}^{I_n}$$

ist eine Funktion

$$f \colon I_n \to \{0, 1\}.$$

Eine solche Funktion können wir als n-Tupel schreiben:

$$f \longleftrightarrow (f(1), \dots, f(n)).$$

Dadurch identifizieren wir

$$\{0, 1\}^{I_n}$$

mit

$$\{0, 1\}^n.$$

Proposition 1.5.69. *Sei*

$$I_n = \{1, \dots, n\}.$$

Dann gibt es eine kanonische Bijektion

$$\mathfrak{P}(I_n) \longrightarrow \{0,1\}^n.$$

Sie ist gegeben durch

$$B \longmapsto (\mathbb{1}_B(1), \dots, \mathbb{1}_B(n)).$$

Beweis. Aus der vorherigen Proposition erhalten wir eine Bijektion

$$\mathfrak{P}(I_n) \longrightarrow \{0,1\}^{I_n}, \qquad B \longmapsto \mathbb{1}_B.$$

Außerdem haben wir eine Bijektion

$$\{0,1\}^{I_n} \longrightarrow \{0,1\}^n, \qquad f \longmapsto (f(1), \dots, f(n)).$$

Die Verkettung dieser beiden Bijektionen ist wieder eine Bijektion. Sie ist gegeben durch

$$B \longmapsto (\mathbb{1}_B(1), \dots, \mathbb{1}_B(n)).$$

□

Beispiel 1.5.70. Sei

$$I_4 = \{1, 2, 3, 4\}.$$

Betrachte die Teilmenge

$$B = \{1, 3, 4\}.$$

Dann ist

$$\mathbb{1}_B(1) = 1, \qquad \mathbb{1}_B(2) = 0, \qquad \mathbb{1}_B(3) = 1, \qquad \mathbb{1}_B(4) = 1.$$

Also entspricht B dem Tupel

$$(1, 0, 1, 1) \in \{0,1\}^4.$$

Umgekehrt entspricht das Tupel

$$(0, 1, 1, 0)$$

der Teilmenge

$$\{2, 3\} \subseteq I_4.$$

Bemerkung 1.5.71 (Warum die Schreibweise $\{0,1\}^n$ passt)**.** Wir haben nun zwei Sichtweisen auf

$$\{0,1\}^n.$$

Einerseits ist

$$\{0,1\}^n$$

die Menge aller n-Tupel aus Nullen und Einsen.

Andererseits ist

$$\{0,1\}^{I_n}$$

die Menge aller Funktionen

$$I_n \to \{0,1\}.$$

Diese beiden Sichtweisen sind äquivalent, weil eine Funktion

$$f\colon \{1,\dots,n\} \to \{0,1\}$$

vollständig durch die Werte

$$f(1),\dots,f(n)$$

bestimmt ist.

Die Exponentenschreibweise ist also nicht zufällig: Wenn A endlich ist, dann gilt

$$\mathsf{card}(\{0,1\}^A) = 2^{\mathsf{card}(A)}.$$

Für jedes Element von A hat eine Funktion nach $\{0,1\}$ genau zwei Wahlmöglichkeiten. Diese Wahlmöglichkeiten multiplizieren sich.

Beispiel 1.5.72 (Wahrheitstafeln)**.** Betrachte atomare Aussagen

$$A_1,\dots,A_n.$$

Eine Wahrheitsbelegung dieser atomaren Aussagen ist eine Funktion

$$\nu\colon I_n \to \{0,1\},$$

wobei

$$\nu(i) = 1$$

bedeutet, dass A_i wahr ist, und

$$\nu(i) = 0$$

bedeutet, dass A_i falsch ist.

Die Menge aller Wahrheitsbelegungen ist also

$$\{0,1\}^{I_n}.$$

Durch die Identifikation mit Tupeln können wir sie auch als

$$\{0,1\}^n$$

schreiben.

Eine Zeile einer Wahrheitstafel ist also genau ein Element von

$$\{0,1\}^n.$$

Beispiel 1.5.73 (Wahrheitsbelegungen als Teilmengen)**.** Zu einer Wahrheitsbelegung

$$\nu\colon I_n \to \{0,1\}$$

gehört die Teilmenge

$$T_\nu := \{i \in I_n \mid \nu(i) = 1\}.$$

Diese Menge T_ν enthält genau die Indizes der atomaren Aussagen, die unter ν wahr sind.

Umgekehrt definiert jede Teilmenge

$$T \subseteq I_n$$

eine Wahrheitsbelegung

$$\mathbb{1}_T : I_n \to \{0,1\}.$$

Dabei gilt:

$$\mathbb{1}_T(i) = 1 \iff i \in T.$$

Die Teilmenge T sagt also: Genau die Aussagen A_i mit $i \in T$ sind wahr.

Damit entsprechen sich die folgenden drei Dinge:

Teilmengen von I_n

$\{0,1\}$-wertige Funktionen auf I_n

Zeilen einer Wahrheitstafel mit n atomaren Aussagen

also

$$\mathfrak{P}(I_n) \cong \{0,1\}^{I_n} \cong \{0,1\}^n.$$

Bemerkung 1.5.74 (Die abstrakte Moral)**.** Wir haben nun mehrere mathematische Objekte, die formal verschieden sind, aber dieselbe Information tragen.

Eine Teilmenge

$$T \subseteq \{1, \dots, n\}$$

speichert, welche Indizes ausgewählt sind.

Eine Funktion

$$\mathbb{1}_T : \{1, \dots, n\} \to \{0,1\}$$

speichert dieselbe Information durch Nullen und Einsen.

Ein Tupel

$$(\varepsilon_1, \dots, \varepsilon_n) \in \{0,1\}^n$$

speichert dieselbe Information als Liste.

Eine Zeile einer Wahrheitstafel speichert dieselbe Information als Belegung atomarer Aussagen.

Der abstrakte Schritt besteht darin, diese verschiedenen Darstellungen nicht miteinander zu verwechseln, aber ihre kanonischen Bijektionen zu erkennen. Mathematik arbeitet sehr oft genau so: Man trennt sauber zwischen Objekten, und identifiziert sie dann kontrolliert, wenn sie dieselbe Struktur oder dieselbe Information tragen.

1.5.4 Äquivalenz- und Ordnungsrelationen

Definition 1.5.75 (Äquivalenzrelation und Ordnungsrelation)**.** Sei A eine Menge und sei $R \subseteq A \times A$ eine Relation auf A.

Die Relation R heißt *reflexiv*, wenn für alle $a \in A$ gilt:

$$aRa.$$

Die Relation R heißt *symmetrisch*, wenn für alle $a, b \in A$ gilt:

$$aRb \implies bRa.$$

Die Relation R heißt *antisymmetrisch*, wenn für alle $a, b \in A$ gilt:

$$aRb \text{ und } bRa \implies a = b.$$

Die Relation R heißt *transitiv*, wenn für alle $a, b, c \in A$ gilt:

$$aRb \text{ und } bRc \implies aRc.$$

Eine Relation heißt *Äquivalenzrelation*, wenn sie reflexiv, symmetrisch und transitiv ist.

Eine Relation heißt *Ordnungsrelation* oder *partielle Ordnung*, wenn sie reflexiv, antisymmetrisch und transitiv ist.

Bemerkung 1.5.76. Äquivalenzrelationen und Ordnungsrelationen sind zwei der wichtigsten Arten von Relationen.

Eine Äquivalenzrelation beschreibt, wann zwei Objekte in einem bestimmten Sinne als gleich angesehen werden. Eine Ordnungsrelation beschreibt, wann ein Objekt in einem bestimmten Sinne kleiner, einfacher, enthalten in oder vor einem anderen Objekt liegt. Der Unterschied zwischen Symmetrie und Antisymmetrie ist dabei zentral. Bei einer Äquivalenzrelation darf man in beide Richtungen gehen. Wenn a äquivalent zu b ist, dann ist auch b äquivalent zu a. Bei einer Ordnungsrelation ist das im Allgemeinen nicht so. Wenn sowohl $a \leq b$ als auch $b \leq a$ gilt, dann müssen a und b bereits gleich sein.

Beispiel 1.5.77 (Gleichheit als einfachste Äquivalenzrelation)**.** Sei A eine Menge. Die Gleichheitsrelation auf A ist definiert durch

$$aRb \quad :\Longleftrightarrow \quad a = b.$$

Diese Relation ist eine Äquivalenzrelation. Sie ist reflexiv, denn für alle $a \in A$ gilt $a = a$. Sie ist symmetrisch, denn aus $a = b$ folgt $b = a$. Sie ist transitiv, denn aus $a = b$ und $b = c$ folgt $a = c$.

Beispiel 1.5.78 (Brüche als Äquivalenzklassen von Paaren)**.** Wir betrachten Paare natürlicher Zahlen

$$(a, b)$$

mit

$$a \in \mathbb{N} \quad \text{und} \quad b \in \mathbb{N}.$$

Wir denken dabei an das Paar (a, b) als den Bruch

$$\frac{a}{b}.$$

Auf der Menge

$$A := \mathbb{N} \times \mathbb{N}$$

definieren wir eine Relation $\sim$ durch

$$(a, b) \sim (c, d) \quad :\Longleftrightarrow \quad ad = bc.$$

Diese Relation beschreibt, wann zwei Brüche denselben Wert haben.

Zum Beispiel gilt

$$(1, 2) \sim (2, 4),$$

denn

$$1 \cdot 4 = 2 \cdot 2.$$

Ebenso gilt

$$(2, 3) \sim (10, 15),$$

denn

$$2 \cdot 15 = 3 \cdot 10.$$

Die Relation $\sim$ ist reflexiv.
Für jedes $(a, b) \in A$ gilt nämlich

$$ab = ba.$$

Also gilt

$$(a, b) \sim (a, b).$$

Die Relation $\sim$ ist symmetrisch.
Wenn

$$(a, b) \sim (c, d)$$

gilt, dann gilt

$$ad = bc.$$

Also gilt auch

$$cb = da.$$

Damit folgt

$$(c, d) \sim (a, b).$$

Die Relation $\sim$ ist transitiv.
Seien

$$(a, b) \sim (c, d) \quad \text{und} \quad (c, d) \sim (e, f).$$

Dann gilt

$$ad = bc \quad \text{und} \quad cf = de.$$

Wir wollen zeigen, dass

$$(a, b) \sim (e, f)$$

gilt. Dazu müssen wir zeigen:

$$af = be.$$

Aus $ad = bc$ folgt durch Multiplikation mit f:

$$adf = bcf.$$

Aus $cf = de$ folgt durch Multiplikation mit b:

$$bcf = bde.$$

Also gilt

$$adf = bde.$$

Da $d \neq 0$ ist, dürfen wir durch d kürzen und erhalten

$$af = be.$$

Also gilt

$$(a, b) \sim (e, f).$$

Damit ist $\sim$ eine Äquivalenzrelation.

Bemerkung 1.5.79. In diesem Beispiel sieht man sehr schön, warum Äquivalenzrelationen wichtig sind.

Die Paare

$$(1,2),(2,4),(3,6),(10,20)$$

sind als Paare verschieden. Als Brüche beschreiben sie aber denselben Wert.

Eine Äquivalenzrelation erlaubt uns also, zwischen tatsächlicher Gleichheit und Gleichheit in einem bestimmten Sinne zu unterscheiden.

Beispiel 1.5.80 (Kongruenz modulo n)**.** Sei $n \in \mathbb{N}$.

Auf $\mathbb{Z}$ definieren wir eine Relation $\equiv_n$ durch

$$a \equiv_n b \quad :\Longleftrightarrow \quad n \text{ teilt } a-b.$$

Man sagt dann: a ist kongruent zu b modulo n.

Zum Beispiel gilt

$$17 \equiv_5 2,$$

denn

$$17 - 2 = 15$$

ist durch 5 teilbar. Ebenso gilt

$$-1 \equiv_5 4,$$

denn

$$-1 - 4 = -5$$

ist durch 5 teilbar.

Die Relation $\equiv_n$ ist eine Äquivalenzrelation. Sie ist reflexiv, denn

$$a - a = 0$$

ist durch n teilbar. Sie ist symmetrisch, denn wenn n die Zahl $a-b$ teilt, dann teilt n auch

$$b - a = -(a-b).$$

Sie ist transitiv, denn wenn n die Zahlen $a-b$ und $b-c$ teilt, dann teilt n auch ihre Summe

$$(a-b)+(b-c) = a-c.$$

Beispiel 1.5.81 (Verschiedene Gleichheitsbegriffe für Dreiecke)**.** Wir betrachten Dreiecke in der Ebene $\mathbb{R}^2$.

Ein Dreieck kann man zum Beispiel als Teilmenge der Ebene auffassen, nämlich als die von drei nicht auf einer Geraden liegenden Punkten aufgespannte Dreiecksfläche.

Je nachdem, welche geometrischen Veränderungen wir erlauben, erhalten wir verschiedene Äquivalenzrelationen.

1. **Gleichheit als Teilmenge.**

   Zwei Dreiecke T und T' heißen gleich, wenn sie als Mengen gleich sind:

   $$T \sim_1 T' \quad :\Longleftrightarrow \quad T = T'.$$

   Das ist die gewöhnliche Gleichheit von Mengen: Die Dreiecke müssen also exakt an derselben Stelle in der Ebene liegen.

2. **Gleichheit bis auf Verschiebung.**

   Zwei Dreiecke T und T' heißen äquivalent, wenn man eines durch Verschieben in das andere überführen kann:

   $$T \sim_2 T' \quad :\Longleftrightarrow \quad \exists v \in \mathbb{R}^2 \,:\, T' = T + v.$$

   Dabei bedeutet

   $$T + v := \{x + v \mid x \in T\}.$$

   Hier ist die genaue Position egal, die Richtung im Raum bleibt aber wichtig: Ein nach oben zeigendes Dreieck ist also nicht äquivalent zu einem gedrehten Dreieck, wenn nur Verschiebungen erlaubt sind.

3. **Gleichheit bis auf Verschiebung und Rotation.**

   Zwei Dreiecke T und T' heißen äquivalent, wenn man eines durch Verschieben und Rotieren in das andere überführen kann:

   $$T \sim_3 T' \quad :\Longleftrightarrow \quad \exists R \in \mathrm{SO}(2) \,:\, \exists v \in \mathbb{R}^2 \,:\, T' = R(T) + v.$$

   Dabei ist $\mathrm{SO}(2)$ die Menge der Rotationen der Ebene um den Ursprung.

   Hier sind Position und Ausrichtung egal, die Größe bleibt aber wichtig: Zwei Dreiecke mit denselben Seitenlängen sind in diesem Sinne äquivalent, sofern keine Spiegelung nötig ist.

4. **Gleichheit bis auf Verschiebung, Rotation und Skalierung.**

   Zwei Dreiecke T und T' heißen äquivalent, wenn man eines durch Verschieben, Rotieren und gleichmäßiges Skalieren in das andere überführen kann:

   $$T \sim_4 T' \quad :\Longleftrightarrow \quad \exists \lambda \in \mathbb{R}_{>0} \,:\, \exists R \in \mathrm{SO}(2) \,:\, \exists v \in \mathbb{R}^2 \,:\, T' = \lambda R(T) + v.$$

   Hier sind Position, Ausrichtung und Größe egal, es bleibt nur noch die abstrakte Form des Dreiecks und die Orientierung als Charakteristik übrig. Dies entspricht dem Begriff ähnlicher Dreiecke, sofern Spiegelungen nicht erlaubt werden.

5. **Gleichheit der abstrakten Dreiecksform.**

   Wenn wir zusätzlich Spiegelungen erlauben, erhalten wir einen noch gröberen Begriff:

   $$T \sim_5 T' \quad :\Longleftrightarrow \quad \exists \lambda \in \mathbb{R}_{>0} \,:\, \exists Q \in \mathrm{O}(2) \,:\, \exists v \in \mathbb{R}^2 \,:\, T' = \lambda Q(T) + v.$$

   Dabei ist $\mathrm{O}(2)$ die Menge aller Drehungen und Spiegelungen der Ebene.

   In diesem Sinn sind zwei Dreiecke äquivalent, wenn sie dieselbe abstrakte Dreiecksform besitzen: Ein Dreieck und sein skaliertes, rotiertes und verschobenes Spiegelbild gelten dann als gleich.

Alle fünf Relationen sind Äquivalenzrelationen. Für $\sim_3$, $\sim_4$ und $\sim_5$ können wir das mit unseren Mitteln noch nicht sauber beweisen — die Transitivität braucht, dass sich Verschiebungen, Drehungen und Streckungen verketten und umkehren lassen. Präzise wird das, sobald wir Gruppen kennen; hier genügt das Bild.

Bemerkung 1.5.82. Das Dreiecksbeispiel zeigt einen wichtigen Gedanken: Es gibt nicht nur eine einzige sinnvolle Bedeutung von „gleich“.

Manchmal meinen wir exakt dasselbe Objekt. Manchmal meinen wir dasselbe Objekt bis auf Verschiebung. Manchmal meinen wir dieselbe geometrische Form. Manchmal meinen wir sogar dieselbe Form bis auf Skalierung und Spiegelung.

Die Sprache der Äquivalenzrelationen erlaubt es uns genau zu bestimmen welchen Gleichheitsbegriff wir verwenden.

Beispiel 1.5.83 (Äquivalenzrelationen im Alltag)**.** Äquivalenzrelationen kommen auch außerhalb der Mathematik sehr natürlich vor.

1. Auf der Menge aller Menschen können wir definieren:

$$x \sim y \quad :\Longleftrightarrow \quad x \text{ und } y \text{ haben dasselbe Geburtsjahr.}$$

   Diese Relation ist reflexiv, symmetrisch und transitiv.

2. Auf der Menge aller Personen in Deutschland können wir definieren:

$$x \sim y \quad :\Longleftrightarrow \quad x \text{ und } y \text{ wohnen in derselben Stadt.}$$

   Auch das ist eine Äquivalenzrelation.

3. Auf der Menge aller Bücher können wir definieren:

$$x \sim y \quad :\Longleftrightarrow \quad x \text{ und } y \text{ haben dieselbe ISBN.}$$

   Dann betrachten wir verschiedene physische Exemplare desselben Buches als äquivalent.

4. Auf der Menge der Bücher können wir auch definieren

$$x \sim y \quad :\Longleftrightarrow \quad x \text{ und } y \text{ haben denselben Inhalt.}$$

   Hier können wir wieder wie beim Dreieck sehr viele Zwischenstufen meinen: Exakte Gleichheit des Textes? Was ist mit Übersetzungen? Verschiedene Ausgaben?

5. Auf der Menge aller Dateien auf einem Computer können wir definieren:

$$x \sim y \quad :\Longleftrightarrow \quad x \text{ und } y \text{ haben denselben Inhalt.}$$

   Dabei können die Dateien verschiedene Namen haben und an verschiedenen Orten gespeichert sein.

Beispiel 1.5.84 (Äquivalenzrelationen aus der Physik)**.** Auch in der Physik betrachtet man Objekte oft als gleich, wenn sie in einem bestimmten Sinn dieselben messbaren oder relevanten Eigenschaften haben.

1. Auf der Menge aller Körper kann man definieren:

$$x \sim y \quad :\Longleftrightarrow \quad x \text{ und } y \text{ haben dieselbe Masse.}$$

   Diese Relation ist eine Äquivalenzrelation.

2. Auf der Menge aller geladenen Teilchen kann man definieren:

$$x \sim y \quad :\Longleftrightarrow \quad x \text{ und } y \text{ haben dieselbe elektrische Ladung.}$$

   Dann sind zum Beispiel alle Elektronen in Bezug auf ihre elektrische Ladung äquivalent.

3. Auf der Menge aller Zustände eines physikalischen Systems kann man definieren:

$$x \sim y \quad :\Longleftrightarrow \quad x \text{ und } y \text{ unterscheiden sich nur durch eine Wahl der Koordinaten.}$$

   Die konkrete Beschreibung kann also verschieden sein, obwohl der physikalische Zustand derselbe ist.

4. Auf der Menge aller gleichförmig bewegten Bezugssysteme kann man definieren:

$$S \sim S' \quad :\Longleftrightarrow \quad S \text{ und } S' \text{ unterscheiden sich nur durch eine Galilei-Transformation.}$$

In der klassischen Mechanik beschreibt das die Idee, dass alle Inertialsysteme physikalisch gleichberechtigt sind.

Bemerkung 1.5.85. Bei physikalischen Beispielen muss man immer genau sagen, welche Eigenschaften man als relevant betrachtet.

Zwei Objekte können dieselbe Masse haben, aber unterschiedliche Form.

Sie können dieselbe Ladung haben, aber unterschiedliche Geschwindigkeit.

Sie können durch verschiedene Koordinaten beschrieben werden, aber denselben physikalischen Zustand darstellen.

Äquivalenzrelationen sind also ein Werkzeug, um bewusst festzulegen, welche Unterschiede wir ignorieren wollen.

Beispiel 1.5.86 (Die gewöhnliche Ordnung auf Zahlen)**.** Auf $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ oder $\mathbb{R}$ ist die Relation

$$a \leq b$$

eine Ordnungsrelation.

Sie ist reflexiv, denn

$$a \leq a.$$

Sie ist antisymmetrisch, denn aus

$$a \leq b \quad \text{und} \quad b \leq a$$

folgt

$$a = b.$$

Sie ist transitiv, denn aus

$$a \leq b \quad \text{und} \quad b \leq c$$

folgt

$$a \leq c.$$

Beispiel 1.5.87 (Teilmengenordnung)**.** Sei X eine Menge.

Auf der Potenzmenge $\mathfrak{P}(X)$ definieren wir eine Relation durch

$$A \leq B \quad :\Longleftrightarrow \quad A \subseteq B.$$

Diese Relation ist eine Ordnungsrelation.

Sie ist reflexiv, denn für alle $A \subseteq X$ gilt

$$A \subseteq A.$$

Sie ist antisymmetrisch, denn aus

$$A \subseteq B \quad \text{und} \quad B \subseteq A$$

folgt

$$A = B.$$

Sie ist transitiv, denn aus

$$A \subseteq B \quad \text{und} \quad B \subseteq C$$

folgt

$$A \subseteq C.$$

Diese Ordnung ist im Allgemeinen keine totale Ordnung.
Zum Beispiel sind in $\mathfrak{P}(\{1,2\})$ die Mengen

$$\{1\} \quad \text{und} \quad \{2\}$$

nicht miteinander vergleichbar.

Definition 1.5.88 (Totale Ordnung)**.** Eine Ordnungsrelation $\leq$ auf einer Menge A heißt *totale Ordnung*, wenn zusätzlich für alle $a, b \in A$ gilt:

$$a \leq b \quad \text{oder} \quad b \leq a.$$

In einer totalen Ordnung sind also je zwei Elemente vergleichbar.

Beispiel 1.5.89 (Partielle Ordnung versus totale Ordnung)**.** Die Ordnung

$$\leq$$

auf $\mathbb{R}$ ist eine totale Ordnung.
Für zwei reelle Zahlen $x, y \in \mathbb{R}$ gilt immer

$$x \leq y \quad \text{oder} \quad y \leq x.$$

Die Teilmengenordnung

$$\subseteq$$

auf $\mathfrak{P}(X)$ ist im Allgemeinen nur eine partielle Ordnung.
Nicht alle Teilmengen von X müssen miteinander vergleichbar sein.

Beispiel 1.5.90 (Teilbarkeit als Ordnung)**.** Auf $\mathbb{N}$ definieren wir eine Relation durch

$$a \leq_| b \quad :\Longleftrightarrow \quad a \text{ teilt } b.$$

Also gilt zum Beispiel

$$2 \leq_| 6,$$

denn 2 teilt 6.
Ebenso gilt

$$3 \leq_| 12.$$

Die Relation $\leq_|$ ist eine Ordnungsrelation.
Sie ist reflexiv, denn jede natürliche Zahl $a \geq 1$ teilt sich selbst.
Sie ist antisymmetrisch, denn wenn a die Zahl b teilt und b die Zahl a teilt, dann gilt für positive natürliche Zahlen

$$a = b.$$

Sie ist transitiv, denn wenn a die Zahl b teilt und b die Zahl c teilt, dann teilt a auch c.
Diese Ordnung ist keine totale Ordnung.
Zum Beispiel sind

$$2 \quad \text{und} \quad 3$$

nicht vergleichbar.
Weder teilt 2 die Zahl 3, noch teilt 3 die Zahl 2.

Beispiel 1.5.91 (Produktordnung)**.** Auf $\mathbb{R}^2$ definieren wir eine Relation durch

$$(x_1, x_2) \leq (y_1, y_2) \quad :\Longleftrightarrow \quad x_1 \leq y_1 \text{ und } x_2 \leq y_2.$$

Diese Relation heißt *Produktordnung*.
Sie ist eine Ordnungsrelation.
Zum Beispiel gilt

$$(1, 2) \leq (3, 5).$$

Aber die Punkte

$$(1, 5) \quad \text{und} \quad (3, 2)$$

sind nicht vergleichbar.
Denn zwar gilt

$$1 \leq 3,$$

aber nicht

$$5 \leq 2.$$

Also ist die Produktordnung auf $\mathbb{R}^2$ keine totale Ordnung.

Beispiel 1.5.92 (Ordnungen im Alltag)**.** Auch im Alltag gibt es viele Ordnungsrelationen.

1. Auf der Menge aller Kalenderdaten ist die Relation

   $$d \leq e \quad :\Longleftrightarrow \quad d \text{ liegt nicht später als } e$$

   eine totale Ordnung.

2. Auf der Menge aller Aufgaben in einem Projekt kann man definieren:

   $$A \leq B \quad :\Longleftrightarrow \quad A \text{ muss erledigt sein, bevor } B \text{ erledigt werden kann; oder } A = B.$$

   Das ist typischerweise eine partielle Ordnung. Wenn sie wollen, können sie sich überlegen, was es für die Lösbarkeit einzelner Aufgaben bedeutet, wenn $\leq$ keine Ordnungsrelation ist.

3. Auf der Menge aller Ordner in einem Dateisystem kann man definieren:

   $$A \leq B \quad :\Longleftrightarrow \quad A \text{ liegt innerhalb von } B.$$

   Je nach Konvention kann man auch die umgekehrte Relation verwenden.

   Wichtig ist nicht die Richtung des Symbols, sondern die Eigenschaften der Relation.

4. Auf der Menge aller Aussagen kann man definieren:

   $$P \leq Q \quad :\Longleftrightarrow \quad Q \implies P.$$

   Diese Relation beschreibt, dass Q mindestens so stark ist wie P.

   Auf Aussagen selbst ist das nur dann antisymmetrisch, wenn wir Aussagen mit gleichem Wahrheitsgehalt identifizieren. Das Beispiel zeigt daher auch, dass man bei Ordnungen genau festlegen muss, was die Objekte sind. Manchmal ist eine Relation erst eine Ordnungsrelation wenn man eine Äquivalenzrelation „ausfaktorisiert“. Was das heißen soll und worauf dabei zu achten ist (Stichwort „Wohldefiniertheit“) sehen wir erst später bei Äquivalenzrelationen.

Bemerkung 1.5.93. Äquivalenzrelationen und Ordnungsrelationen haben fast dieselben Bausteine. Beide verlangen Reflexivität. Beide verlangen Transitivität.

Der entscheidende Unterschied liegt in der mittleren Eigenschaft: Äquivalenzrelationen verlangen Symmetrie. Ordnungsrelationen verlangen Antisymmetrie.

Kurz gesagt: Äquivalenzrelationen sortieren Objekte in Gruppen von gleichartigen Objekten. Ordnungsrelationen vergleichen Objekte in einer Richtung.

Leitbeispiel 1.5.94 (Die Geburtstagsfunktion: Äquivalenz oder Ordnung?)**.** Die Relation $R =$ „hat am selben Kalendertag Geburtstag wie“ aus Leitbeispiel 1.5.25 ist eine Äquivalenzrelation auf J: Sie ist reflexiv (jede Person hat am selben Tag Geburtstag wie sie selbst), symmetrisch (teilt p den Tag mit q, dann auch q mit p) und transitiv (hat p denselben Tag wie q und q denselben wie r, dann hat p denselben Tag wie r).

Versuchen wir dagegen zu *ordnen*:

$$p \preccurlyeq q \quad :\Longleftrightarrow \quad \text{der Geburtstag von } p \text{ liegt im Kalender nicht später als der von } q.$$

Diese Relation ist reflexiv und transitiv, und je zwei Personen sind vergleichbar. Aber sie ist *nicht antisymmetrisch*: Haben $p \neq q$ am selben Tag Geburtstag, dann gilt $p \preccurlyeq q$ und $q \preccurlyeq p$, ohne dass $p = q$ wäre. Nach unserer Definition ist $\preccurlyeq$ also *keine* Ordnungsrelation — es scheitert exakt an der mittleren Eigenschaft aus der letzten Bemerkung.

Der Ausweg wurde eben schon angedeutet: Man muss zuerst die Äquivalenzrelation R „ausfaktorisieren“, also nicht mehr Personen vergleichen, sondern ganze Geburtstags-Schubladen. Auf den Kalendertagen selbst ist die Reihenfolge nämlich eine totale Ordnung. Wie das Sortieren in Schubladen formal funktioniert, klären die nächsten Definitionen.

Definition 1.5.95 (Äquivalenzklasse)**.** Sei A eine Menge und sei $\sim$ eine Äquivalenzrelation auf A.

Für ein Element $a \in A$ definieren wir die *Äquivalenzklasse von a* durch

$$[a]_\sim := \{x \in A \mid x \sim a\}.$$

Wenn klar ist, welche Äquivalenzrelation gemeint ist, schreiben wir auch einfach

$$[a]$$

statt

$$[a]_\sim.$$

Bemerkung 1.5.96. Die Äquivalenzklasse $[a]$ besteht aus allen Elementen, die zu a äquivalent sind.

Man kann also sagen: $[a]$ ist die Menge aller Objekte, die im gewählten Sinn dieselben sind wie a.

Bei Brüchen enthält die Äquivalenzklasse von $(1, 2)$ zum Beispiel alle Paare, die denselben Bruchwert wie $\frac{1}{2}$ beschreiben.

Beispiel 1.5.97 (Energieniveaus als Äquivalenzklassen)**.** Auch die Physik sortiert unablässig in Äquivalenzklassen.

Der Zustand eines (reibungsfreien) Federpendels ist durch Auslenkung x und Geschwindigkeit v festgelegt, also durch ein Paar $(x, v) \in \mathbb{R} \times \mathbb{R}$. Die Gesamtenergie definiert eine Funktion

$$E\colon \mathbb{R}^2 \to \mathbb{R}, \qquad E(x, v) = \tfrac{1}{2}mv^2 + \tfrac{1}{2}kx^2,$$

mit Masse $m > 0$ und Federkonstante $k > 0$. Wir erklären zwei Zustände für äquivalent, wenn sie dieselbe Energie haben:

$$(x_1, v_1) \sim (x_2, v_2) \quad :\Longleftrightarrow \quad E(x_1, v_1) = E(x_2, v_2).$$

Das ist eine Äquivalenzrelation: Sie erbt Reflexivität, Symmetrie und Transitivität direkt von der Gleichheit der Energiewerte.

Die Äquivalenzklasse $[(x, v)]$ ist die Menge aller Zustände derselben Energie. Geometrisch ist das eine Ellipse in der (x, v)-Ebene, denn $\frac{1}{2}mv^2 + \frac{1}{2}kx^2 = E_0$ beschreibt für $E_0 > 0$ genau eine Ellipse (eine in beiden Achsenrichtungen verschieden gestreckte Kreisgleichung — man vergleiche $x^2 + v^2 = 1$). Die Ebene aller Zustände zerfällt also in ineinanderliegende Ellipsen (plus den einzelnen Punkt $(0, 0)$ zur Energie $E_0 = 0$). Und das Pendel bewegt sich, ohne seine Klasse je zu verlassen: Energieerhaltung sagt gerade, dass die gesamte Bewegung innerhalb einer einzigen Äquivalenzklasse abläuft.

In der Physik heißen diese Klassen *Energieschalen* (nicht zu verwechseln mit den diskreten *Energieniveaus* der Atomphysik — hier ist für jeden Wert $E_0 > 0$ eine Schale da). Strukturell ist das exakt die Situation aus Leitbeispiel 1.5.41: Eine Funktion (E statt geb) sortiert ihren Definitionsbereich in Fasern. Die Energie ist sozusagen die Geburtstagsfunktion der Mechanik.

Proposition 1.5.98 (Grundlegende Eigenschaften von Äquivalenzklassen)**.** *Sei A eine Menge und sei $\sim$ eine Äquivalenzrelation auf A.*

Dann gelten folgende Aussagen.

1. *Für jedes $a \in A$ gilt*
$$a \in [a].$$
2. *Für alle $a, b \in A$ gilt*
$$a \sim b \quad \Longleftrightarrow \quad [a] = [b].$$
3. *Für alle $a, b \in A$ gilt*
$$[a] \cap [b] \neq \emptyset \quad \Longleftrightarrow \quad [a] = [b].$$
4. *Zwei Äquivalenzklassen sind also entweder gleich oder disjunkt.*
   Genauer: Für alle $a, b \in A$ gilt
$$[a] = [b] \quad \textit{oder} \quad [a] \cap [b] = \emptyset.$$
5. *Die Vereinigung aller Äquivalenzklassen ist ganz A:*
$$A = \bigcup_{a \in A} [a].$$

Beweis. Wir beweisen die Aussagen nacheinander.

1. Sei $a \in A$.
   Da $\sim$ reflexiv ist, gilt
$$a \sim a.$$
   Nach Definition der Äquivalenzklasse folgt
$$a \in [a].$$

2. Seien $a, b \in A$.

   Zuerst nehmen wir an, dass

   $$a \sim b$$

   gilt.

   Wir zeigen

   $$[a] = [b].$$

   Dazu zeigen wir beide Inklusionen.

   Sei zunächst

   $$x \in [a].$$

   Dann gilt nach Definition

   $$x \sim a.$$

   Außerdem gilt nach Annahme

   $$a \sim b.$$

   Mit Transitivität folgt

   $$x \sim b.$$

   Also gilt

   $$x \in [b].$$

   Damit haben wir

   $$[a] \subseteq [b].$$

   Sei nun

   $$x \in [b].$$

   Dann gilt

   $$x \sim b.$$

   Aus $a \sim b$ folgt wegen Symmetrie

   $$b \sim a.$$

   Mit Transitivität folgt

   $$x \sim a.$$

   Also gilt

   $$x \in [a].$$

   Damit haben wir

   $$[b] \subseteq [a].$$

   Insgesamt folgt

   $$[a] = [b].$$

   Umgekehrt nehmen wir nun an, dass

   $$[a] = [b]$$

   gilt.

   Nach Teil 1 gilt

   $$a \in [a].$$

Wegen $[a] = [b]$ folgt

$$a \in [b].$$

Nach Definition von $[b]$ bedeutet das

$$a \sim b.$$

Damit ist gezeigt:

$$a \sim b \quad \Longleftrightarrow \quad [a] = [b].$$

3. Seien $a, b \in A$.

   Wenn

   $$[a] = [b]$$

   gilt, dann ist

   $$[a] \cap [b] = [a].$$

   Nach Teil 1 gilt $a \in [a]$.

   Also ist $[a]$ nicht leer.

   Daher gilt

   $$[a] \cap [b] \neq \emptyset.$$

   Umgekehrt nehmen wir an, dass

   $$[a] \cap [b] \neq \emptyset$$

   gilt.

   Dann gibt es ein Element

   $$x \in [a] \cap [b].$$

   Also gilt

   $$x \in [a] \quad \text{und} \quad x \in [b].$$

   Nach Definition der Äquivalenzklasse bedeutet das

   $$x \sim a \quad \text{und} \quad x \sim b.$$

   Aus $x \sim a$ folgt wegen Symmetrie

   $$a \sim x.$$

   Zusammen mit $x \sim b$ folgt durch Transitivität

   $$a \sim b.$$

   Nach Teil 2 folgt

   $$[a] = [b].$$

4. Seien $a, b \in A$.

   Entweder gilt

   $$[a] \cap [b] = \emptyset.$$

   Dann sind wir fertig.

   Oder es gilt

   $$[a] \cap [b] \neq \emptyset.$$

   Dann folgt aus Teil 3

   $$[a] = [b].$$

   Also sind zwei Äquivalenzklassen entweder gleich oder disjunkt.

5. Wir zeigen
$$A = \bigcup_{a \in A} [a].$$
Zuerst gilt für jedes $a \in A$
$$[a] \subseteq A,$$
denn Äquivalenzklassen sind Teilmengen von A.
Also gilt
$$\bigcup_{a \in A} [a] \subseteq A.$$
Umgekehrt sei
$$x \in A.$$
Nach Teil 1 gilt
$$x \in [x].$$
Da $[x]$ eine der Mengen in der Vereinigung ist, folgt
$$x \in \bigcup_{a \in A} [a].$$
Also gilt
$$A \subseteq \bigcup_{a \in A} [a].$$
Damit folgt die Gleichheit. □

Bemerkung 1.5.99. Die letzte Proposition sagt anschaulich: Eine Äquivalenzrelation zerlegt die Menge A in Blöcke.

Jedes Element liegt in genau einem Block. Zwei verschiedene Blöcke überlappen sich nicht. Und alle Blöcke zusammen ergeben wieder die ganze Menge A.

Diese Blöcke sind genau die Äquivalenzklassen.

Definition 1.5.100 (Partition)**.** Sei A eine Menge. Eine Menge $\mathscr{P}$von Teilmengen von A heißt *Partition* von A, wenn folgende Bedingungen gelten:

1. Jedes $P \in \mathscr{P}$ist nicht leer.
2. Für alle $P, Q \in \mathscr{P}$gilt:
$$P = Q \quad \text{oder} \quad P \cap Q = \emptyset.$$
3. Die Vereinigung aller Mengen in $\mathscr{P}$ist ganz A:
$$A = \bigcup_{P \in \mathscr{P}} P.$$

Korollar 1.5.101 (Äquivalenzklassen bilden eine Partition)**.** *Sei A eine Menge und sei $\sim$ eine Äquivalenzrelation auf A. Dann bildet die Menge aller Äquivalenzklassen*
$$\{[a] \mid a \in A\}$$
eine Partition von A.

Beweis. Jede Äquivalenzklasse ist nicht leer, denn nach Proposition 1.5.98 gilt

$$a \in [a]$$

für jedes $a \in A$.

Zwei Äquivalenzklassen sind nach Proposition 1.5.98 entweder gleich oder disjunkt. Außerdem ist die Vereinigung aller Äquivalenzklassen nach der Proposition ganz A. Damit erfüllen die Äquivalenzklassen genau die Bedingungen einer Partition. □

Bemerkung 1.5.102. Man kann sich eine Äquivalenzrelation also als eine präzise mathematische Art vorstellen, eine Menge in Schubladen zu sortieren.

Die Äquivalenzklasse $[a]$ ist die Schublade, in der a liegt. Alle Elemente in derselben Schublade sind zueinander äquivalent. Elemente aus verschiedenen Schubladen sind nicht zueinander äquivalent.

Leitbeispiel 1.5.103 (Die Geburtstagsfunktion: alle Fäden zusammen)**.** Jetzt zahlt sich das Leitbeispiel aus: Alle Begriffe dieses Abschnitts treffen sich in einem Bild.

Die Äquivalenzklassen der Relation R = „hat am selben Kalendertag Geburtstag wie“ sind genau die nichtleeren Fasern der Geburtstagsfunktion:

$$[p]_R = \{q \in J \mid \text{geb}(q) = \text{geb}(p)\} = F_{\text{geb}(p)}.$$

Nach dem Korollar bilden diese Klassen eine Partition von J: Der Jahrgang zerfällt vollständig in disjunkte Geburtstags-Schubladen. Die Schubladen aus Leitbeispiel 1.5.41 *sind* also die Äquivalenzklassen — und das dort versprochene offizielle Wort lautet Partition. Ein Detail verdient dabei Aufmerksamkeit: Zur Partition gehören nur die *nichtleeren* Schubladen — eine pro Tag im Bild geb(J), bei 200 Personen also höchstens 200 Stück. Die mindestens 166 leeren Schubladen sind keine Äquivalenzklassen, denn eine Partition enthält keine leeren Mengen — und es gibt ja auch keine Person, deren Klasse sie sein könnten.

Drei Intuitionen, ein Objekt:

1. *Funktionen erzeugen Äquivalenzrelationen:* „gleicher Wert unter f“ ist für jede Funktion f eine Äquivalenzrelation, und ihre Klassen sind die Fasern von f. Unsere Relation R war nie etwas anderes als „gleicher Wert unter geb“.

2. *Äquivalenz ist gewolltes Vergessen:* Wer von einer Person nur den Geburtstag behalten will, ersetzt die Person durch ihre Schublade. Die Menge der Schubladen entspricht dabei genau dem Bild geb(J): eine Klasse pro tatsächlich vorkommendem Geburtstag.

3. *Partitionen können grob oder fein sein:* „gleiches Geburtsdatum (mit Jahr)“ zerlegt J in feinere Schubladen als R. „gleiches Geburtsjahr“ zerlegt J dagegen in andere, mit R unvergleichbare Schubladen: Zwei Personen können denselben Kalendertag in verschiedenen Jahren treffen — oder dasselbe Jahr an verschiedenen Tagen. Welche Äquivalenzrelation die richtige ist, hängt davon ab, welche Information man vergessen möchte.

Diese Sichtweise trägt weit über den Jahrgang hinaus: Brüche entstanden oben als Klassen von Zahlenpaaren, Energieschalen als Klassen von Pendelzuständen. Immer ist es dasselbe Muster — eine Menge, eine Äquivalenzrelation, eine Partition in Schubladen.

Kapitel 2

Abstrakte Algebra

2.1 Gruppen

2.1.1 Allgemeines

Bemerkung 2.1.1 (Motivation: Symmetrien und abstrakte Algebra)**.** Der Gruppenbegriff ist einer der ersten großen Schritte in die abstrakte Algebra.

Die Grundidee ist zunächst sehr konkret: Man betrachtet Symmetrien eines Objekts. Zum Beispiel kann man ein gleichseitiges Dreieck drehen oder spiegeln, ohne dass es sich als geometrische Form verändert.

Wichtig ist dabei nicht nur jede einzelne Symmetrie für sich, sondern auch, wie Symmetrien miteinander verknüpft werden können. Wenn man zuerst eine Symmetrie ausführt und danach eine zweite, erhält man wieder eine Symmetrie.

Der Gruppenbegriff abstrahiert genau diese Situation. Wir studieren also nicht mehr nur einzelne Symmetrien. Wir studieren auch nicht nur konkrete Mengen von Symmetrien eines bestimmten Objekts. Stattdessen untersuchen wir abstrakt, welche Eigenschaften eine Menge mit einer Verknüpfung haben muss, damit sie sich wie eine Menge von Symmetrien verhält. Und was für Eigenschaften Mengen von Symmetrien allgemein haben können und wie man diese verstehen kann.

Deshalb sprechen wir im Folgenden einfach von einer Menge G mit einer Verknüpfung $*$. Die Elemente von G müssen nicht unbedingt Zahlen, Funktionen oder geometrische Bewegungen sein. Entscheidend ist nur, dass man sie miteinander verknüpfen kann und dass diese Verknüpfung bestimmte Regeln erfüllt.

Definition 2.1.2 (Gruppe)**.** Eine *Gruppe* ist ein Tripel

$$(G, *, e),$$

bestehend aus einer Menge G, einer Abbildung

$$* : G \times G \to G$$

und einem Element

$$e \in G,$$

sodass die folgenden Eigenschaften gelten.

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

2. **Neutrales Element.**

   Für alle $x \in G$ gilt

   $$e * x = x \quad \text{und} \quad x * e = x.$$

3. **Inverse Elemente.**

   Für jedes $x \in G$ gibt es ein Element $x' \in G$, sodass

   $$x * x' = e \quad \text{und} \quad x' * x = e.$$

Die Menge G heißt die *Trägermenge* der Gruppe.
Die Abbildung $*$ heißt die *Verknüpfung* oder *Gruppenoperation*.
Das Element e heißt das *neutrale Element* der Gruppe.

Bemerkung 2.1.3 (Warum steht das neutrale Element in der Definition?)**.** Wir haben eine Gruppe hier formal als Tripel

$$(G, *, e)$$

definiert.

Das ist didaktisch etwas expliziter als die häufige Schreibweise

$$(G, *).$$

Der Grund ist folgender: Bei der Definition der inversen Elemente müssen wir bereits wissen, welches Element das neutrale Element ist.

Die Bedingung für Inverse lautet nämlich:

$$x * x' = e \quad \text{und} \quad x' * x = e.$$

In dieser Formel kommt e schon vor.

Formal ist es deshalb sauber, e als Teil der Struktur mitzuführen.

In vielen Büchern definiert man eine Gruppe aber nur als Paar $(G, *)$ und verlangt dann zuerst: Es gibt ein neutrales Element $e \in G$.

Danach fordert man: Zu jedem $x \in G$ gibt es ein inverses Element bezüglich dieses neutralen Elements.

Beide Sichtweisen beschreiben dieselbe mathematische Idee.

In der Praxis geht man meist so vor:

Man hat zuerst eine Menge G und eine Verknüpfung $*$ gegeben.

Dann prüft man die Assoziativität.

Danach sucht man ein neutrales Element.

Erst wenn man dieses neutrale Element gefunden hat, kann man sinnvoll nach inversen Elementen fragen.

Bemerkung 2.1.4 (Historischer Hintergrund)**.** Der Gruppenbegriff entstand nicht plötzlich als fertige abstrakte Definition.

Er entwickelte sich im 19. Jahrhundert aus mehreren konkreten mathematischen Problemen.

Eine wichtige Quelle war die Untersuchung von Permutationen.

Permutationen sind Umordnungen einer endlichen Menge.

Wenn man zwei Permutationen hintereinander ausführt, erhält man wieder eine Permutation.

Diese Operation ist assoziativ, es gibt eine Permutation, die nichts verändert, und jede Permutation kann rückgängig gemacht werden.

Genau hier sieht man bereits die Gruppenaxiome.

Besonders wichtig war die Arbeit von Évariste Galois.

Er untersuchte Gleichungen und die Permutationen ihrer Lösungen.

Dabei erkannte er, dass bestimmte algebraische Eigenschaften einer Gleichung durch die Struktur dieser Permutationen verstanden werden können.

Später wurden Gruppen immer stärker unabhängig von konkreten Gleichungen oder geometrischen Figuren betrachtet.

Man erkannte: Sehr verschiedene mathematische Objekte besitzen dieselbe abstrakte Struktur.

Der moderne Gruppenbegriff beschreibt genau diese gemeinsame Struktur.

Bemerkung 2.1.5 (Was hier abstrakt passiert)**.** Beim Übergang zu Gruppen wechseln wir die Perspektive.

Früher haben wir oft konkrete Objekte betrachtet: Zahlen, Mengen, Funktionen oder geometrische Figuren.

Jetzt betrachten wir eine Struktur, die auf sehr verschiedenen Arten realisiert werden kann.

Eine Gruppe kann aus Zahlen bestehen.

Eine Gruppe kann aus Symmetrien bestehen.

Eine Gruppe kann aus Matrizen bestehen.

Eine Gruppe kann aus Funktionen bestehen.

Aber in allen Fällen interessieren uns zunächst nur die Regeln der Verknüpfung.

Das ist ein typischer Gedanke der abstrakten Algebra:

Wir vergessen absichtlich viele konkrete Eigenschaften der Objekte und behalten nur die Struktur, die für die jeweilige Theorie wesentlich ist.

Das ist nicht weniger präzise, sondern präziser.

Wir sagen genau, welche Eigenschaften wir verwenden dürfen und welche nicht.

Definition 2.1.6 (Abelsche Gruppe)**.** Eine Gruppe $(G, *, e)$ heißt *abelsch* oder *kommutativ*, wenn für alle $x, y \in G$ gilt:

$$x * y = y * x.$$

Das bedeutet: Die Reihenfolge der Verknüpfung spielt keine Rolle.

Definition 2.1.7 (Ordnung einer endlichen Gruppe)**.** Sei $(G, *, e)$ eine Gruppe.

Die Anzahl der Elemente von G heißt die *Ordnung* von G.

Man schreibt dafür

$$|G|.$$

Wenn G endlich viele Elemente besitzt, heißt G eine *endliche Gruppe*.

Proposition 2.1.8 (Eindeutigkeit des neutralen Elements)**.** *Sei $(G, *, e)$ eine Gruppe.*
Dann ist das neutrale Element eindeutig.

Genauer gilt: Wenn $e' \in G$ ebenfalls ein neutrales Element ist, dann gilt

$$e = e'.$$

Beweis. Sei $e' \in G$ ein weiteres neutrales Element.

Da e neutral ist, gilt insbesondere

$$e * e' = e'.$$

Da e' neutral ist, gilt aber auch

$$e * e' = e.$$

Also folgt

$$e = e * e' = e'.$$

Damit ist das neutrale Element eindeutig. □

Bemerkung 2.1.9. Der Beweis ist kurz, aber sehr wichtig.

Er zeigt: Wenn eine Verknüpfung überhaupt ein neutrales Element besitzt, dann kann es nur eines geben.

Deshalb ist es später unproblematisch, von *dem* neutralen Element zu sprechen.

Das erklärt auch, warum man eine Gruppe oft nur als Paar $(G, *)$ definiert.

Das neutrale Element ist dann zwar nicht explizit Teil der Daten, aber durch die Gruppenstruktur eindeutig bestimmt.

Beispiel 2.1.10 (Die ganzen Zahlen mit Addition)**.** Die Menge $\mathbb{Z}$ bildet mit der Addition eine Gruppe.

Wir betrachten also

$$(\mathbb{Z}, +, 0).$$

Die Verknüpfung ist

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}.$$

Die Assoziativität der Addition besagt: Für alle $a, b, c \in \mathbb{Z}$ gilt

$$a + (b + c) = (a + b) + c.$$

Das neutrale Element ist 0, denn für alle $a \in \mathbb{Z}$ gilt

$$0 + a = a \quad \text{und} \quad a + 0 = a.$$

Das inverse Element zu a ist $-a$, denn

$$a + (-a) = 0 \quad \text{und} \quad (-a) + a = 0.$$

Diese Gruppe ist abelsch, denn für alle $a, b \in \mathbb{Z}$ gilt

$$a + b = b + a.$$

Beispiel 2.1.11 (Weitere additive Zahlengruppen)**.** Analog sind auch

$$(\mathbb{Q}, +, 0) \quad \text{und} \quad (\mathbb{R}, +, 0)$$

Gruppen.

In beiden Fällen ist das neutrale Element 0.

Das inverse Element zu x ist jeweils $-x$.

Auch diese Gruppen sind abelsch.

Beispiel 2.1.12 (Warum $(\mathbb{N}, +, 0)$ keine Gruppe ist)**.** Die Menge $\mathbb{N}$ bildet mit der Addition im Allgemeinen keine Gruppe.

Die Addition ist zwar assoziativ.

Falls $0 \in \mathbb{N}$ gilt, besitzt $\mathbb{N}$ mit der Addition auch ein neutrales Element.

Aber nicht jedes Element besitzt ein additives Inverses in $\mathbb{N}$.

Zum Beispiel müsste das inverse Element zu 1 ein Element $x \in \mathbb{N}$ sein mit

$$1 + x = 0.$$

Ein solches natürliches x gibt es nicht.

Also ist $(\mathbb{N}, +, 0)$ keine Gruppe.

Beispiel 2.1.13 (Von Null verschiedene reelle Zahlen mit Multiplikation)**.** Die Menge

$$\mathbb{R}^\times := \mathbb{R} \setminus \{0\}$$

bildet mit der Multiplikation eine Gruppe.

Wir betrachten also

$$(\mathbb{R}^\times, \cdot, 1).$$

Die Assoziativität folgt aus der Assoziativität der Multiplikation reeller Zahlen.

Das neutrale Element ist 1, denn für alle $x \in \mathbb{R}^\times$ gilt

$$1 \cdot x = x \quad \text{und} \quad x \cdot 1 = x.$$

Das inverse Element zu x ist

$$x^{-1} = \frac{1}{x}.$$

Denn

$$x \cdot x^{-1} = 1 \quad \text{und} \quad x^{-1} \cdot x = 1.$$

Diese Gruppe ist abelsch.

Beispiel 2.1.14 (Warum $(\mathbb{R}, \cdot, 1)$ keine Gruppe ist)**.** Die Menge $\mathbb{R}$ bildet mit der Multiplikation keine Gruppe.

Das Problem ist die Zahl 0.

Sie besitzt kein multiplikatives Inverses.

Es gibt nämlich kein $x \in \mathbb{R}$ mit

$$0 \cdot x = 1.$$

Also ist $(\mathbb{R}, \cdot, 1)$ keine Gruppe.

Beispiel 2.1.15 (Die triviale Gruppe)**.** Sei

$$G = \{e\}.$$

Wir definieren

$$e * e = e.$$

Dann ist

$$(G, *, e)$$

eine Gruppe.

Sie heißt die *triviale Gruppe*.

Sie hat genau ein Element.

Das neutrale Element ist e.

Das inverse Element von e ist wieder e.

Beispiel 2.1.16 (Eine Gruppe mit zwei Elementen)**.** Die Menge

$$G = \{1, -1\}$$

bildet mit der gewöhnlichen Multiplikation eine Gruppe.

Das neutrale Element ist 1.

Es gilt

$$1^{-1} = 1 \quad \text{und} \quad (-1)^{-1} = -1.$$

Die Verknüpfungstafel lautet

$\cdot$	1	-1
1	1	-1
-1	-1	1

Diese Gruppe ist endlich und abelsch.
Ihre Ordnung ist

$$|G| = 2.$$

Beispiel 2.1.17 (Restklassen modulo n mit Addition)**.** Sei $n \in \mathbb{N}$.
Wir betrachten die Menge

$$\mathbb{Z}/n\mathbb{Z}$$

der *Restklassen* modulo n. Das ist nichts Neues: $\mathbb{Z}/n\mathbb{Z}$ ist die Menge der Äquivalenzklassen der Kongruenzrelation $\equiv_n$ aus Beispiel 1.5.80. Die Klasse $[a]$ enthält alle ganzen Zahlen, die bei Division durch n denselben Rest lassen wie a — daher der Name *Restklasse*. (Die Schreibweise $\mathbb{Z}/n\mathbb{Z}$ liest man als „$\mathbb{Z}$ modulo n“.)

Jede Restklasse enthält genau einen der Reste $0, 1, \dots, n-1$, also besteht die Menge aus

$$[0], [1], \dots, [n-1].$$

Wir definieren Addition durch

$$[a] + [b] := [a + b].$$

Dann bildet

$$(\mathbb{Z}/n\mathbb{Z}, +, [0])$$

eine Gruppe. Das neutrale Element ist $[0]$. Das inverse Element zu $[a]$ ist $[-a]$. Auf den ersten Blick fehlt $[-a]$ in der Liste $[0], \dots, [n-1]$ — aber dieselbe Restklasse trägt viele Namen: Wegen $-a \equiv_n n - a$ ist $[-a] = [n-a]$. In $\mathbb{Z}/5\mathbb{Z}$ ist zum Beispiel $[-1] = [4]$ (in Beispiel 1.5.80 hatten wir schon $-1 \equiv_5 4$ nachgerechnet), und tatsächlich gilt $[1] + [4] = [5] = [0]$.

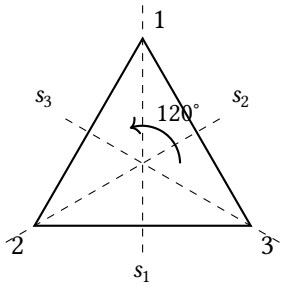
Diese Gruppe ist endlich und abelsch. Sie hat Ordnung n.

Warum diese Definition *wohldefiniert* ist — das Ergebnis darf nicht davon abhängen, welchen Vertreter der Restklasse man zum Rechnen benutzt — untersuchen wir im Leitbeispiel Leitbeispiel 2.2.7 genauer.

Leitbeispiel 2.1.18 (Die Symmetrien des Dreiecks)**.** Als Leitbeispiel für die Gruppentheorie begleitet uns ein besonders anschauliches Objekt: ein gleichseitiges Dreieck. Dieses taucht auch in der Natur auf — man denke etwa an das Molekül Bortrifluorid BF_3, dessen drei Fluoratome ein gleichseitiges Dreieck um das zentrale Boratom bilden.

Eine *Symmetrie* ist eine Bewegung der Ebene, die das Dreieck als Ganzes auf sich abbildet. Mit *Bewegung* ist dabei eine abstandserhaltende Abbildung der Ebene gemeint — eine Kongruenzabbildung, wie man sie aus der Schule kennt. (Ohne diese Einschränkung gäbe es unendlich viele Abbildungen, die das Dreieck auf sich werfen.)

Damit wir alle vom selben Dreieck reden, legen wir Konventionen fest: Wir nummerieren die Ecken *gegen* den Uhrzeigersinn mit 1, 2, 3, gedreht wird ebenfalls gegen den Uhrzeigersinn, und s_i bezeichnet die Spiegelachse durch die Ecke i und die Mitte der gegenüberliegenden Seite.



Von diesen Symmetrien gibt es genau sechs:

- drei *Drehungen* um den Mittelpunkt, um 0°, 120° und 240°;
- drei *Spiegelungen* an den Achsen s_1, s_2 und s_3.

Führt man zwei Symmetrien nacheinander aus, so entsteht wieder eine Symmetrie. Die 0°-Drehung lässt alles an seinem Platz — das ist das neutrale Element. Und jede Symmetrie lässt sich rückgängig machen. Also bilden die sechs Symmetrien unter der Verkettung eine Gruppe, die *Diedergruppe* D_3 der Ordnung 6.

Diese Gruppe ist *nicht abelsch*: Erst spiegeln und dann drehen ergibt im Allgemeinen etwas anderes, als erst drehen und dann spiegeln. Das kann man am Bild nachspielen: Spiegelt man erst an s_1 und dreht dann um 120°, so landet die Ecke 1 auf dem Platz von Ecke 2; dreht man dagegen erst und spiegelt dann an s_1, so landet die Ecke 1 auf dem Platz von Ecke 3. Sie ist unser erstes Beispiel, in dem die Reihenfolge zählt — und sie trägt uns durch das ganze Kapitel.

Wir werden die Symmetrien als Permutationen der drei Ecken wiedererkennen — und überhaupt verstehen was es für zwei Gruppen heißt „*strukturgleich*“ zu sein.

Beispiel 2.1.19 (Funktionen mit punktweiser Addition)**.** Sei X eine Menge. Wir betrachten die Menge aller Funktionen

$$f : X \to \mathbb{R}.$$

Diese Menge bezeichnen wir mit

$$\mathbb{R}^X.$$

Wir definieren eine Verknüpfung punktweise durch

$$(f + g)(x) := f(x) + g(x)$$

für alle $x \in X$. Dann ist

$$(\mathbb{R}^X, +, n)$$

eine abelsche Gruppe.

Dabei ist n die Nullfunktion

$$n : X \to \mathbb{R}, \quad n(x) = 0.$$

Das inverse Element zu einer Funktion f ist die Funktion $-f$, definiert durch

$$(-f)(x) := -f(x).$$

Dieses Beispiel zeigt: Auch Mengen von Funktionen können Gruppen bilden.

Beispiel 2.1.20 (Vektoren mit Addition)**.** Die Menge

$$\mathbb{R}^n$$

bildet mit der Vektoraddition eine abelsche Gruppe. Das neutrale Element ist der Nullvektor

$$0 = (0, \dots, 0).$$

Das inverse Element zu

$$x = (x_1, \dots, x_n)$$

ist

$$-x = (-x_1, \dots, -x_n).$$

Dieses Beispiel wird später besonders wichtig. Vektorräume sind nämlich Mengen, auf denen insbesondere eine additive Gruppenstruktur gegeben ist. Dazu kommt dann noch die Skalarmultiplikation.

Bemerkung 2.1.21. Die Beispiele zeigen ein wiederkehrendes Muster. Eine Gruppe entsteht oft, wenn man Transformationen hat, die man hintereinander ausführen kann und wieder rückgängig machen kann.

Bei Zahlen ist die Verknüpfung Addition oder Multiplikation. Bei Symmetrien und Permutationen ist die Verknüpfung das Hintereinanderausführen. Bei Matrizen ist die Verknüpfung die Matrixmultiplikation. Bei Funktionen mit Werten in $\mathbb{R}$ ist die Verknüpfung punktweise Addition.

Die abstrakte Definition erlaubt es uns, all diese Situationen mit einer einzigen Sprache zu behandeln.

Lemma 2.1.22 (Grundregeln in Gruppen)**.** *Sei G eine Gruppe mit Verknüpfung $*$. Dann gelten die folgenden Aussagen.*

1. *Das neutrale Element von G ist eindeutig bestimmt.*
2. *Für jedes $x \in G$ ist das inverse Element von x eindeutig bestimmt. Wir bezeichnen es mit x^{-1}.*
3. *Für $a, b \in G$ besitzt die Gleichung*
$$a * x = b$$
genau eine Lösung $x \in G$. Ebenso besitzt die Gleichung
$$y * a = b$$
genau eine Lösung $y \in G$.
4. *Für alle $x, y \in G$ gilt*
$$(x * y)^{-1} = y^{-1} * x^{-1}.$$
5. *Für jedes $x \in G$ gilt*
$$(x^{-1})^{-1} = x.$$
6. *Für das neutrale Element e gilt*
$$e^{-1} = e.$$

Beweis. Wir zeigen die Aussagen der Reihe nach.

1. Die Behauptung ist exakt Proposition 2.1.8.

2. Sei $x \in G$. Seien $u, v \in G$ inverse Elemente zu x. Dann gilt

$$u * x = e, \qquad x * v = e.$$

Daher folgt mit Assoziativität

$$u = u * e = u * (x * v) = (u * x) * v = e * v = v.$$

Also besitzt x höchstens ein inverses Element. Da jedes Element einer Gruppe ein inverses Element besitzt, ist dieses eindeutig.

3. Sei $a, b \in G$. Wir behaupten, dass

$$x = a^{-1} * b$$

die eindeutige Lösung von $a * x = b$ ist. Tatsächlich gilt

$$a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b.$$

Also ist $a^{-1} * b$ eine Lösung. Ist umgekehrt $x \in G$ eine beliebige Lösung von $a * x = b$, so folgt

$$x = e * x = (a^{-1} * a) * x = a^{-1} * (a * x) = a^{-1} * b.$$

Also ist die Lösung eindeutig.

Analog ist

$$y = b * a^{-1}$$

die eindeutige Lösung von $y * a = b$. Denn

$$(b * a^{-1}) * a = b * (a^{-1} * a) = b * e = b,$$

und aus $y * a = b$ folgt

$$y = y * e = y * (a * a^{-1}) = (y * a) * a^{-1} = b * a^{-1}.$$

4. Seien $x, y \in G$. Wir prüfen, dass $y^{-1} * x^{-1}$ invers zu $x * y$ ist. Es gilt

$$(x * y) * (y^{-1} * x^{-1}) = x * (y * y^{-1}) * x^{-1} = x * e * x^{-1} = e.$$

Ebenso gilt

$$(y^{-1} * x^{-1}) * (x * y) = y^{-1} * (x^{-1} * x) * y = y^{-1} * e * y = e.$$

Wegen der Eindeutigkeit des inversen Elements folgt

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

5. Sei $x \in G$. Das Element x^{-1} ist dadurch charakterisiert, dass

$$x * x^{-1} = e = x^{-1} * x.$$

Also ist x ein inverses Element zu x^{-1}. Wegen der Eindeutigkeit des inversen Elements folgt

$$(x^{-1})^{-1} = x.$$

6. Für das neutrale Element e gilt

$$e * e = e.$$

Also ist e ein inverses Element zu e. Wegen der Eindeutigkeit des inversen Elements folgt

$$e^{-1} = e.$$

□

2.1.2 Permutationsgruppen

Definition 2.1.23 (Permutationsgruppen)**.** Sei X eine Menge. Eine *Permutation* von X ist eine bijektive Abbildung

$$\sigma : X \to X.$$

Die Menge aller Permutationen von X bezeichnen wir mit

$$\mathrm{Sym}(X).$$

Lemma 2.1.24 (Die symmetrische Gruppe)**.** *Sei*

$$\circ : \mathrm{Sym}(X) \times \mathrm{Sym}(X) \longrightarrow \mathrm{Sym}(X), (f, g) \longmapsto f \circ g$$

die gewöhnliche Komposition von Abbildungen (eingeschränkt auf $\mathrm{Sym}(X)$*). Dann bildet*

$$(\mathrm{Sym}(X), \circ, \mathrm{Id}_X)$$

eine Gruppe.

Beweis. Die Assoziativität folgt aus der allgemeineren Assoziativität der Komposition.
Die Identität

$$\mathrm{Id}_X : X \to X.$$

ist tatsächlich ein neutrales Element, denn für $a \in \mathrm{Sym}(X)$ und $x \in X$ gilt

$$(a \circ \mathrm{Id}_X)(x) = a(\mathrm{Id}_X(x)) = a(x) \quad \text{und} \quad (\mathrm{Id}_X \circ a)(x) = \mathrm{Id}_X(a(x)) = a(x)\,.$$

Da Permutationen bijektiv sind, besitzt jede Permutation eine Umkehrabbildung. Diese Umkehrabbildung ist genau das inverse Element in der Gruppe. □

Definition 2.1.25 (Symmetrische Gruppe)**.** Falls

$$X = \{1, \dots, n\}$$

ist, schreibt man häufig

$$S_n := \mathrm{Sym}(X)$$

für die Permutationsgruppe.
Wir nennen sie dann die *symmetrische Gruppe* auf n Elementen.

Sei $n \in \mathbb{N}$. Wir setzen $X_n := \{1, \dots, n\}$. Es sei S_n die symmetrische Gruppe auf n Elementen, also $S_n = \mathrm{Sym}(X_n)$.

Definition 2.1.26 (Zykel)**.** Sei $k \geqslant 2$, dann heißt eine Permutation $\sigma \in S_n$ ein *k-Zykel*, wenn es paarweise verschiedene Elemente $x_1, \dots, x_k \in X_n$ gibt, sodass

$$\sigma(x_i) = x_{i+1} \text{ falls } 1 \leqslant i < k, \quad \sigma(x_k) = x_1, \quad \sigma(x) = x \text{ sonst.}$$

Wir schreiben dann $\begin{pmatrix} x_1 & x_2 & \dots & x_k \end{pmatrix}$.
Ein 2-Zykel heißt Transposition.

Bemerkung 2.1.27. *Jedes Element wird auf seinen rechten Nachbarn geschickt, das letzte auf das erste — und was nicht in der Klammer steht, bleibt fest.*
Achtung: In der Klammer steht also *nicht* die Bilderzeile $\tau(x_1), \tau(x_2), \ldots$, sondern es stehen die Elemente selbst darin; wohin sie wandern, sagt die Nachbar-Regel.

Eine Folge der Nachbar-Regel: Man darf die Klammer zyklisch rotieren,

$$(x_1 \quad x_2 \quad \ldots \quad x_k) = (x_2 \quad \ldots \quad x_k \quad x_1),$$

denn beide Schreibweisen schicken jedes Element auf denselben Nachbarn. Ein und derselbe Zykel hat also mehrere Namen.

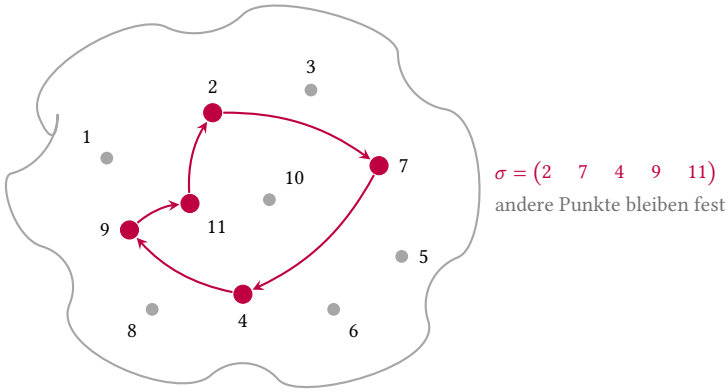
Bemerkung 2.1.28. Alternativ kann man auch über die Notation den Zykel definieren:
Sei M eine Menge und sei σ eine Permutation von M. Sind $a_1, \ldots, a_k \in M$ paarweise verschieden, so bezeichnet

$$(a_1\ a_2\ \ldots\ a_k)$$

diejenige Permutation, welche

$$a_1 \mapsto a_2, \quad a_2 \mapsto a_3, \quad \ldots, \quad a_{k-1} \mapsto a_k, \quad a_k \mapsto a_1$$

abbildet und alle anderen Elemente von M festlässt. Eine solche Permutation heißt ein *Zykel* der Länge k. Ein Zykel der Länge 2 heißt auch eine *Transposition*.



Beispiel 2.1.29 (Erste Beispiele)**.** Der Zyklus

$$(1 \quad 3 \quad 5 \quad 2)$$

sendet

$$1 \mapsto 3, \quad 3 \mapsto 5, \quad 5 \mapsto 2, \quad 2 \mapsto 1$$

und lässt alle übrigen Zahlen fest. Insbesondere gilt also zum Beispiel

$$(1 \quad 3 \quad 5 \quad 2) : 4 \longmapsto 4.$$

Der Zyklus

$$(2 \quad 7)$$

vertauscht 2 und 7 und lässt alle anderen Elemente fest. Es gilt also

$$(2 \quad 7) : 2 \longmapsto 7, \quad (2 \quad 7) : 7 \longmapsto 2.$$

Die Schreibweise eines Zyklus ist nicht eindeutig. Zum Beispiel beschreiben

$$(1\ \ 3\ \ 5\ \ 2),\quad (3\ \ 5\ \ 2\ \ 1),\quad (5\ \ 2\ \ 1\ \ 3),\quad (2\ \ 1\ \ 3\ \ 5)$$

alle denselben Zyklus. Die Reihenfolge darf aber nicht beliebig vertauscht werden. Zum Beispiel ist

$$(1\ \ 3\ \ 5\ \ 2) \neq (1\ \ 5\ \ 3\ \ 2).$$

Bemerkung 2.1.30. Gegeben ein Zykel $\tau = (1\ \ 7\ \ 5\ \ 8)$ schreiben wir $\tau(1)$ für das Bild von 1 (also 7). In Zykelschreibweise wäre das $(1\ \ 7\ \ 5\ \ 8)(1)$. Dabei ist schwer zu erkennen, ob das „(1)“ am Ende ein 1-Zykel oder das Argument ist. Daher habe ich oben andere Notation verwendet. Wir werden bald aber sehen, dass man 1-Zykel sowieso weglassen kann, daher können wir in Zukunft auch sicher $(1\ \ 7\ \ 5\ \ 8)(1)$ schreiben.

Definition 2.1.31 (Multiplikation von Zyklen)**.** Wir multiplizieren Zykel wie allgemeine Permutationen. Und die Multiplikation auf den Permutationen war die Komposition von Funktionen. Das heißt: In einem Produkt

$$\sigma\tau = \sigma \circ \tau$$

wird zuerst τ angewendet und danach σ. Äquivalent gilt

$$(\sigma\tau)(x) = \sigma(\tau(x)).$$

Man liest Produkte von Permutationen also von rechts nach links.

Will man das Bild von x also ausrechnen, schaut man zunächst darauf, was das Bild von x unter τ ist. Ist τ ein Zykel und als Zykel geschrieben so ist $\tau(x)$ der Wert direkt rechts neben x, falls x am rechten Rand liegt, ist $\tau(x)$ Wert ganz links im Zykel und falls x im Zykel gar nicht auftaucht, dann ist $\tau(x) = x$. Nun geht man weiter und betrachtet was das Bild von $\tau(x)$ unter σ ist. So arbeitet man sich von rechts nach links durch.

Beispiel 2.1.32 (Multiplikation von Zyklen)**.** Wir berechnen

$$(1\ \ 2\ \ 4)(2\ \ 3).$$

Nach unserer Konvention wird zuerst $(2\ \ 3)$ angewendet und danach $(1\ \ 2\ \ 4)$. Wir verfolgen die Bilder der einzelnen Elemente:

x	$(2\ \ 3)(x)$	$(1\ \ 2\ \ 4)((2\ \ 3)(x))$
1	1	2
2	3	3
3	2	4
4	4	1

Also gilt

$$(1\ \ 2\ \ 4)(2\ \ 3) = (1\ \ 2\ \ 3\ \ 4).$$

Vertauscht man die Reihenfolge, erhält man im Allgemeinen ein anderes Ergebnis. Tatsächlich ist

$$(2\ \ 3)(1\ \ 2\ \ 4) = (1\ \ 3\ \ 2\ \ 4).$$

Daher gilt

$$(1\ \ 2\ \ 4)(2\ \ 3) \neq (2\ \ 3)(1\ \ 2\ \ 4).$$

Die Multiplikation von Permutationen ist also im Allgemeinen nicht kommutativ.

Theorem 2.1.33 (Zerlegung in disjunkte Zykel)**.** *Sei $n \in \mathbb{N}$ beliebig. Jede Permutation $\sigma \in S_n$ lässt sich als Produkt von disjunkten Zykeln schreiben.*

Wenn man die Reihenfolge der Faktoren ignoriert ist die Zerlegung eindeutig.

Beweis. Sei $\sigma \in S_n$ eine beliebige Permutation. Betrachte die Menge

$$A_1 = \left\{ \sigma^k(1) \;\middle|\; k \in \mathbb{N} \right\}.$$

Hier ist

$$\sigma^k = \underbrace{\sigma \circ \ldots \circ \sigma}_{k\text{-mal}}.$$

Da $A_1 \subseteq \{1, \ldots, n\} =: X_n$ gilt und X_n endlich ist, müssen in der Folge

$$1, \sigma^1(1), \sigma^2(1) \ldots$$

Einträge doppelt vorkommen. Also sei r die kleinste Zahl mit $\sigma^r(1) = \sigma^s(1)$ für ein $s < r$. Per Definition ist $\sigma^{r-s}(1) = \sigma^{-s}(\sigma^r(1))$. Da aber $\sigma^s(1) = \sigma^r(1)$ ist, ist

$$\sigma^{r-s}(1) = \sigma^{-s}(\sigma^r(1)) = 1 = \sigma^0(1).$$

Also gilt auch $\sigma^{r-s}(1) = \sigma^0(1)$. Da r aber als kleinste Zahl mit dieser Eigenschaft gewählt wurde muss $s = 0$ sein. Also ist $\sigma^r(1) = 1$. Also verhält sich σ auf der Menge A_1 wie ein Zykel.

Falls $A_1 = X_n$ ist sind wir fertig. Ansonsten nehme die kleinste Zahl $x_2 \in X_n \setminus A_1$. Dann argumentieren wir genauso und sehen dass σ sich auf

$$A_2 := \left\{ \sigma^k(x_2) \;\middle|\; k \in \mathbb{N} \right\}.$$

auch wie ein Zykel verhält. Tatsächlich sind A_1 und A_2 disjunkt. (Aufgabe: Warum?)

Falls nun $X_n = A_1 \cup A_2$ so sind wir fertig. Falls nicht können wir fortfahren. Für ein $N \leqslant n$ gilt sicher

$$X_n = A_1 \cup A_2 \cup \ldots \cup A_N$$

denn jede der Mengen enthält mindestens ein Element.

Zur Eindeutigkeit: Wir zeigen dass wir bei der obigen Methode keine Wahl hatten wenn wir disjunkte Zykel haben wollen! Sei also $\sigma = \tau_1 \ldots \tau_K$ eine Zerlegung in disjunkte Zykel.

Sei $b \in X_n$ beliebig. Es muss einen Zykel τ_j geben der b enthält (wenn er nur b enthält lassen wir ihn weg). Ohne Beschränkung der Allgemeinheit können wir annehmen, dass b ganz links in τ_j steht. Da die Zykel τ_i disjunkt sind bestimmt lediglich τ_j das Bild von b unter σ. Also muss $\sigma(b)$ direkt neben b stehen. Sei nun k die kleinste Zahl mit $\sigma^k(b) = b$. Der Zykel der b enthält muss genau die Form

$$\begin{pmatrix} b & \sigma(b) & \ldots & \sigma^{k-1}(b) \end{pmatrix}$$

haben. Denn jede Abweichung davon würde sich auf diesem Orbit anders verhalten als σ. Und da die Zykel disjunkt sind kann dies auch kein anderer Zykel reparieren.

Das zeigt die Eindeutigkeit. □

Bemerkung 2.1.34 (Fixpunkte und Einszyklen)**.** Ein Element, welches von einer Permutation auf sich selbst abgebildet wird, nennt man einen *Fixpunkt*.

Fixpunkte werden in der Zykelnotation meistens weggelassen. So schreibt man zum Beispiel statt

$$\begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 \end{pmatrix} \begin{pmatrix} 4 \end{pmatrix} \begin{pmatrix} 5 \end{pmatrix}$$

meist einfach

$$\begin{pmatrix} 1 & 3 \end{pmatrix}.$$

Das liegt daran, dass der Zykel (2) sagt, 2 wird auf 2 geschickt und der Rest auf sich selber. Damit ist $(2) = \mathrm{Id}$. (Streng nach unserer Definition ist (2) übrigens gar kein Zykel — dort war $k \geqslant 2$ verlangt. Für $k = 1$ liefert dieselbe Schreibvorschrift aber einfach die Identität, deshalb lassen wir die Schreibweise trotzdem zu.) Das selbige gilt selbstverständlich für alle 1-Zykel. Da man die Identitätsfunktion in Komposition (da sie das neutrale Element ist) weglassen kann, kann man auch 1-Zykel weglassen.

Beispiel 2.1.35 (Disjunkte Zyklen)**.** Die Zyklen

$$(1 \quad 4 \quad 2) \quad \text{und} \quad (3 \quad 5)$$

sind disjunkt, weil kein Element in beiden Zyklen vorkommt. Ihr Produkt wirkt daher unabhängig auf den beiden Mengen

$$\{1, 2, 4\} \quad \text{und} \quad \{3, 5\}.$$

Zum Beispiel gilt

$$(1 \quad 4 \quad 2)(3 \quad 5) = (3 \quad 5)(1 \quad 4 \quad 2).$$

Lemma 2.1.36 (Disjunkte Zyklen kommutieren)**.** *Seien*

$$\alpha = (a_1 \quad a_2 \quad \dots \quad a_k) \quad \textit{und} \quad \beta = (b_1 \quad b_2 \quad \dots \quad b_\ell)$$

zwei disjunkte Zyklen. Dann gilt

$$\alpha\beta = \beta\alpha.$$

Beweis. Da α und β disjunkt sind, gilt

$$\{a_1, \dots, a_k\} \cap \{b_1, \dots, b_\ell\} = \emptyset.$$

Wir zeigen, dass $\alpha\beta$ und $\beta\alpha$ jedes Element gleich abbilden. Sei also $x \in M$ beliebig.

Zuerst sei

$$x \in \{a_1, \dots, a_k\}.$$

Dann lässt β das Element x fest. Außerdem liegt auch $\alpha(x)$ wieder in $\{a_1, \dots, a_k\}$, also lässt β auch $\alpha(x)$ fest. Daher gilt

$$(\alpha\beta)(x) = \alpha(\beta(x)) = \alpha(x)$$

und

$$(\beta\alpha)(x) = \beta(\alpha(x)) = \alpha(x).$$

Also stimmen $\alpha\beta$ und $\beta\alpha$ auf allen Elementen von $\{a_1, \dots, a_k\}$ überein.

Nun sei

$$x \in \{b_1, \dots, b_\ell\}.$$

Analog lässt α sowohl x als auch $\beta(x)$ fest. Daher gilt

$$(\alpha\beta)(x) = \alpha(\beta(x)) = \beta(x)$$

und

$$(\beta\alpha)(x) = \beta(\alpha(x)) = \beta(x).$$

Also stimmen $\alpha\beta$ und $\beta\alpha$ auch auf allen Elementen von $\{b_1, \dots, b_\ell\}$ überein.

Schließlich sei

$$x \notin \{a_1, \dots, a_k\} \cup \{b_1, \dots, b_\ell\}.$$

Dann lassen sowohl α als auch β das Element x fest. Also gilt

$$(\alpha\beta)(x) = x = (\beta\alpha)(x).$$

Damit stimmen $\alpha\beta$ und $\beta\alpha$ auf jedem Element von M überein. Folglich gilt

$$\alpha\beta = \beta\alpha.$$

□

Leitbeispiel 2.1.37 (Die Symmetrien des Dreiecks als Permutationen)**.** Jede Symmetrie unseres Dreiecks Leitbeispiel 2.1.18 verschiebt die (gegen den Uhrzeigersinn nummerierten) Ecken 1, 2, 3 — sie entspricht also auch einer Permutation von $\{1, 2, 3\}$. Die Symmetrie selbst ist dabei weiterhin eine Abbildung der *Ebene*; wir notieren nur, welche Ecke auf welchen Eckplatz wandert.

- Die Drehung um 120° schickt $1 \mapsto 2 \mapsto 3 \mapsto 1$, ist also der 3-Zykel $\begin{pmatrix}1 & 2 & 3\end{pmatrix}$; die Drehung um 240° ist $\begin{pmatrix}1 & 3 & 2\end{pmatrix}$.
- Die Spiegelung, die die Ecke 1 festhält und 2, 3 vertauscht, ist die Transposition $\begin{pmatrix}2 & 3\end{pmatrix}$; ebenso gehören $\begin{pmatrix}1 & 3\end{pmatrix}$ und $\begin{pmatrix}1 & 2\end{pmatrix}$ zu den Spiegelungen.
- Die Ruhelage ist die Identität.

Das sind genau die sechs Elemente von S_3. Die Symmetriegruppe des Dreiecks *ist* also in einem gewissen Sinne S_3. Der Begriff des Isomorphismus wird diese Erkenntnis präzisieren.

Diese Strukturgleichheit zu den Permutationen gilt nur im Fall $n = 3$. Das Dreieck ist unter den regelmäßigen Vielecken der einzige, in dem *jede* Permutation der Ecken durch eine geometrische Symmetrie realisiert wird. Ein Quadrat ($n = 4$) hat $4! = 24$ Eckpermutationen, aber nur 8 Symmetrien; die übrigen Vertauschungen würden es zerreißen. (Allgemein hat das regelmäßige n-Eck genau $2n$ Symmetrien: n Drehungen und n Spiegelungen.) Beim Dreieck geht alles, denn $2 \cdot 3 = 3!$.

Nebenbei wird die Nicht-Kommutativität aus Leitbeispiel 2.1.18 in Zykelsprache handgreiflich, denn es gilt

$$\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\end{pmatrix}, \qquad \text{aber} \qquad \begin{pmatrix}2 & 3\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix} = \begin{pmatrix}1 & 3 & 2\end{pmatrix}.$$

2.1.3 Gruppenhomomorphismen

Seien $(G, *, e)$ und $(H, \odot, i)$ zwei Gruppen. Da wir bereits gesehen haben, dass die neutralen Elemente eindeutig aus der Verknüpfung herleitbar sind schreiben wir ab jetzt nur $(G, *)$ und $(H, \odot)$ für die beiden Gruppen.

Definition 2.1.38 (Gruppenhomomorphismen)**.** Eine Abbildung $f : G \to H$ heißt *(Gruppen-)Homomorphismus* genau dann wenn

$$f(x * y) = f(x) \odot f(y)$$

für alle $x, y \in G$. Man sagt auch „f ist ein Homomorphismus zwischen den Gruppen $(G, *)$ und $(H, \odot)$“.

Bemerkung 2.1.39. Ein Gruppenhomomorphismus ist eine Abbildung die mit den Verknüpfungen verträglich ist. Bei einem Gruppenhomomorphismus ist es egal ob man vor oder nach der Anwendung der Funktion die Gruppenelemente verknüpft.

Beispiel 2.1.40 (Bereits bekannte Gruppenhomomorphismen)**.** Einige Ihnen bereits aus der Schule bekannte Abbildungen sind Gruppenhomomorphismen, wenn man die Gruppen richtig wählt.

1. Die Abbildung
$$f : \mathbb{Z} \longrightarrow \mathbb{Z},\ n \longmapsto 2 \cdot n$$
ist ein Gruppenhomomorphismus zwischen der Gruppe $(\mathbb{Z}, +)$ mit sich selber.

2. Allgemeiner ist für jedes $k \in \mathbb{Z}$ die Abbildung
$$f_k : \mathbb{Z} \longrightarrow \mathbb{Z},\ n \longmapsto k \cdot n$$
ein Gruppenhomomorphismus zwischen der Gruppe $(\mathbb{Z}, +)$ mit sich selber. (Der Grund ist das Distributivgesetz, also dass $k \cdot (n_1 + n_2) = k \cdot n_1 + k \cdot n_2$ für alle $k, n_1, n_2 \in \mathbb{Z}$).

3. Das obige Beispiel lässt sich auch auf $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$ verallgemeinern (wie?).

4. Wir schreiben $\mathbb{Q}^\times := \mathbb{Q} \setminus \{0\}$. Zumindest in $\mathbb{Z}$ ist Multiplikation einfach mehrfaches Addieren. Mehrfaches Multiplizieren ist dann Potenzieren und in $\mathbb{Q}^\times$ ist Multiplikation auch eine Gruppenverküpfung. Tatsächlich bekommt man so auch einen Gruppenhomomorphismus von $(\mathbb{Q}^\times, \cdot)$ in sich selber und zwar
$$g : \mathbb{Q}^\times \longrightarrow \mathbb{Q}^\times,\ q \longmapsto q^2\,.$$
Die Rechnung dahinter ist eine Zeile: $(pq)^2 = pqpq = p^2q^2$, wobei wir die Faktoren dank Kommutativität umsortieren durften.

5. Allgemeiner ist wieder für jedes $k \in \mathbb{Z}$ die Abbildung
$$g : \mathbb{Q}^\times \longrightarrow \mathbb{Q}^\times,\ q \longmapsto q^k$$
ein Gruppenhomomorphismus. Grund ist die Tatsache, dass $(pq)^k = (p^k)(q^k)$ gilt.

6. Auch die Exponentialfunktion
$$\exp : \mathbb{R} \longrightarrow \mathbb{R}^\times,\ x \longmapsto e^x$$
ist eine Gruppenhomomorphismus zwischen $(\mathbb{R}, +)$ und $(\mathbb{R}^\times, \cdot)$. Hierbei ist $\mathbb{R}^\times := \mathbb{R} \setminus \{0\}$.

Wir werden im Laufe der Vorlesung noch einige neue Gruppenhomomorphismen kennenlernen.

Nun noch ein Beispiel für etwas das *kein* Gruppenhomomorphismus ist:
$$p : \mathbb{R} \longrightarrow \mathbb{R},\ x \longmapsto x^2 + 3x$$
ist kein Gruppenhomomorphismus (zumindest nicht zwischen zwei der Standardgruppen $(\mathbb{R}, +), (\mathbb{R}^\times, \cdot)$). Für $(\mathbb{R}, +)$ zeigt das das Einsetzen von konkreten Zahlen:
$$p(1 + 1) = p(2) = 4 + 6 = 10, \qquad p(1) + p(1) = 4 + 4 = 8 \neq 10.$$

In unserer Definition von Gruppen haben wir die neutralen Elemente zusätzlich benannt. Später haben wir gesehen, dass diese eindeutig sind. Daher lassen sich die neutralen Elemente aus der Verknüpfung, solange diese ein neutrales Element hat, herleiten. Bei der Definition eines Homomorphismus haben wir gar nichts über das Verhalten auf den neutralen Elementen gesagt. Eine natürliche Forderung wäre, dass auch diese aufeinander abgebildet werden. Tatsächlich folgt diese Forderung aber bereits aus der Verträglichkeit mit der Verknüpfung. Dies ist ein weiteres Zeichen dafür, dass sich die neutralen Elemente bereits aus der Verknüpfung ergeben.

Lemma 2.1.41 (Homomorphismen erhalten die neutralen Elemente)**.** *Seien $(G, *)$ und $(H, \odot)$ Gruppen mit neutralen Elementen $e \in G$ und $i \in H$. Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt $f(e) = i$.*

Beweis. Es gilt

$$f(e) = f(e * e) = f(e) \odot f(e).$$

Wir wissen aber, dass die Gleichung $f(e) = x \odot f(e)$ eindeutig lösbar ist (nach Lemma 2.1.22, 3)). Aber offenkundig löst auch i diese Gleichung, also gilt $f(e) = i$. □

Eine weitere Struktur ist die Bildung von Inversen. Auch diese sind eindeutig durch die Verknüpfung festgelegt. Wieder sehen wir, dass wir in der Definition von Homomorphismen nichts über das Verhalten auf Inversen sagen mussten, weil sich die natürliche Forderung dass $f(x^{-1}) = f(x)^{-1}$ von selber ergibt.

Lemma 2.1.42 (Homomorphismen erhalten Inverse)**.** *Seien G und H Gruppen. Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann gilt für jedes $g \in G$:*

$$\varphi\left(g^{-1}\right) = \varphi(g)^{-1}.$$

Beweis. Sei $g \in G$. Dann gilt

$$\varphi(g) \cdot \varphi\left(g^{-1}\right) = \varphi\left(g \cdot g^{-1}\right) = \varphi(e_G) = e_H.$$

Ebenso gilt

$$\varphi\left(g^{-1}\right) \cdot \varphi(g) = \varphi\left(g^{-1} \cdot g\right) = \varphi(e_G) = e_H.$$

Also ist $\varphi\left(g^{-1}\right)$ ein Inverses von $\varphi(g)$. Wegen der Eindeutigkeit des Inversen folgt

$$\varphi\left(g^{-1}\right) = \varphi(g)^{-1}.$$ □

Lemma 2.1.43 (Komposition von Gruppenhomomorphismen)**.** *Seien $(G_1, *_1), (G_2, *_2)$ und $(G_3, *_3)$ Gruppen. Seien $f : G_1 \to G_2$ und $g : G_2 \to G_3$ Gruppenhomomorphismen, dann ist auch $g \circ f$ ein Gruppenhomomorphismus.*

Beweis. Das ist eine Übungsaufgabe. □

Definition 2.1.44 (Isomorphismen von Gruppen)**.** Seien $(G, *)$ und $(H, \odot)$ Gruppen.
Ein Gruppenhomomorphismus

$$f : G \to H$$

heißt ein *Isomorphismus*, wenn f bijektiv ist und sowohl f als auch

$$f^{-1} : H \to G$$

Gruppenhomomorphismen sind.

Wenn es einen Isomorphismus $f : G \to H$ gibt, heißen die Gruppen $(G, *)$ und $(H, \odot)$ *isomorph*. Man schreibt dann

$$(G, *) \cong (H, \odot).$$

Lemma 2.1.45 (Bijektive Homomorphismen sind Isomorphismen)**.** *Seien $(G, *)$ und $(H, \odot)$ Gruppen.*

Ist

$$f : G \to H$$

ein bijektiver Gruppenhomomorphismus, dann ist f ein Isomorphismus.

Beweis. Nach Voraussetzung ist f bijektiv und ein Gruppenhomomorphismus. Es bleibt also nur zu zeigen, dass

$$f^{-1} : H \to G$$

ein Gruppenhomomorphismus ist.

Seien $u, v \in H$ beliebig. Da f bijektiv ist, gibt es eindeutig bestimmte Elemente $x, y \in G$ mit

$$f(x) = u \quad \text{und} \quad f(y) = v.$$

Also gilt

$$x = f^{-1}(u) \quad \text{und} \quad y = f^{-1}(v).$$

Da f ein Gruppenhomomorphismus ist, gilt

$$f(x * y) = f(x) \odot f(y) = u \odot v.$$

Wir wenden nun f^{-1} auf beide Seiten an und erhalten

$$x * y = f^{-1}(u \odot v).$$

Mit $x = f^{-1}(u)$ und $y = f^{-1}(v)$ folgt

$$f^{-1}(u \odot v) = f^{-1}(u) * f^{-1}(v).$$

Also ist f^{-1} ein Gruppenhomomorphismus.

Damit ist f ein Isomorphismus. □

Beispiel 2.1.46 (Die Exponentialfunktion als Isomorphismus)**.** Wir betrachten die Gruppen

$$(\mathbb{R}, +) \quad \text{und} \quad (\mathbb{R}_{>0}, \cdot).$$

Die Exponentialfunktion

$$\exp : \mathbb{R} \to \mathbb{R}_{>0}, \quad x \mapsto e^x$$

ist ein Gruppenhomomorphismus.

Denn für alle $x, y \in \mathbb{R}$ gilt

$$\exp(x + y) = e^{x+y} = e^x e^y = \exp(x) \cdot \exp(y).$$

Außerdem ist $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ bijektiv.

Ihre Umkehrabbildung ist der natürliche Logarithmus

$$\ln : \mathbb{R}_{>0} \to \mathbb{R}.$$

Nach dem vorherigen Lemma ist die Exponentialfunktion also ein Isomorphismus

$$(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot).$$

Die Gruppen sehen zunächst sehr verschieden aus: In der einen Gruppe verknüpfen wir reelle Zahlen durch Addition. In der anderen Gruppe verknüpfen wir positive reelle Zahlen durch Multiplikation. Algebraisch besitzen sie aber dieselbe Gruppenstruktur.

Bemerkung 2.1.47 (Was bedeutet Isomorphie?)**.** Ein Isomorphismus bedeutet, dass zwei mathematische Objekte bezüglich der gerade betrachteten Struktur gleich sind. Das heißt nicht, dass die Objekte in jeder Hinsicht identisch aussehen müssen. Es heißt aber: Alles, was nur von der relevanten Struktur abhängt, kann von einem Objekt in das andere übersetzt werden.

Ein anschauliches Beispiel ist Schach. Für das Spiel selbst ist es nicht wesentlich, ob die Figuren aus vergoldetem Elfenbein, aus Plastik oder aus Papierstücken mit aufgeschriebenen Figurennamen bestehen. Manche Ausführungen sehen schöner aus, andere sind leichter zu transportieren oder sind angenehmer zu greifen. Aber solange Brett, Figuren, erlaubte Züge und Gewinnbedingungen dieselbe Struktur haben, ist das Spiel dasselbe.

Ein weiteres Beispiel ist das Game of Fifteen. Bei diesem Spiel wählen zwei Spieler abwechselnd Zahlen aus $\{1, \dots, 9\}$. Wer zuerst drei eigene Zahlen besitzt, deren Summe 15 ist, gewinnt. Dieses Spiel ist Tic-Tac-Toe in anderer Darstellung. Man benutzt dazu die folgende Beschriftung des Tic-Tac-Toe-Brettes:

$$\begin{matrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{matrix}$$

Die Zeilen, Spalten und Diagonalen dieses Quadrats sind genau die Dreiermengen, deren Summe 15 ist. Ein Spielzustand im Game of Fifteen besteht darin, welche Zahlen Spieler 1 und welche Zahlen Spieler 2 bereits gewählt hat. Diesen Zustand übersetzt man in einen Tic-Tac-Toe-Zustand, indem man jede gewählte Zahl durch das entsprechende Feld im oben beschrifteten Brett ersetzt. Die erlaubten Züge in beiden Spielen entsprechen einander. Auch die Gewinnzustände entsprechen einander, denn in der obigen Darstellung braucht man im Game of Fifteen genau eine volle Zeile, Spalte oder Diagonale um zu gewinnen.

In der Algebra bedeutet ein Isomorphismus zwischen Gruppen entsprechend: Mit Blick auf die Gruppeneigenschaften sind die beiden Gruppen gleich. Die Gruppen $(\mathbb{R}, +)$ und $(\mathbb{R}_{>0}, \cdot)$ sind als Mengen und als konkrete Rechenbereiche verschieden. Aber als Gruppen sind sie nicht verschieden. Der Isomorphismus exp übersetzt Addition in Multiplikation und ln übersetzt Multiplikation zurück in Addition.

Wir haben abstrakt gesagt, dass zwei isomorphe Gruppen in allen gruppentheoretischen Eigenschaften identisch sind. Entweder man definiert das Wort „gruppentheoretische Eigenschaften“ als genau diese die unter Isomorphie erhalten bleiben. Das wäre eine gute Definition, würde aber die obige Behauptung zu einer Tautologie machen. Wir motivieren diese Behauptung einfach indem wir anhand eines Beispiels zeigen wie sich Eigenschaften mittels Isomorphismen von einer Gruppe auf eine andere übertragen. Natürlich übertragen sich nicht die Eigenschaften selber, denn die Gruppen haben diese Eigenschaften ja auch ohne den Isomorphismus. Aber es lassen sich *Beweise* von Eigenschaften von einer Gruppe zu *Beweisen* von Eigenschaften isomorpher Gruppen, mittels des Isomorphismus, übertragen. Wenn man das formalisiert sieht man, dass genau die Eigenschaften, die nur die Grundmenge, die Verknüpfung und das neutrale Element einer Gruppe verwenden erhalten bleiben. Eigenschaften über den Namen von Elementen oder nicht-algebraische Informationen wie „Abstand“ übertragen sich bei Gruppen selbstverständlich nicht.

Beispiel 2.1.48 (Eigenschaften entlang eines Isomorphismus übersetzen)**.** Seien $(G, *)$ und $(H, \odot)$ Gruppen und sei

$$f : G \to H$$

ein Isomorphismus.

Wenn jedes Element von G sein eigenes Inverses ist, dann ist auch jedes Element von H sein eigenes Inverses.

Genauer: Gilt

$$g * g = e_G \quad \text{für alle } g \in G,$$

dann gilt

$$h \odot h = e_H \quad \text{für alle } h \in H.$$

Beweis. Sei $h \in H$ beliebig.

Da f bijektiv ist, gibt es ein $g \in G$ mit

$$f(g) = h.$$

Da jedes Element von G sein eigenes Inverses ist, gilt

$$g * g = e_G.$$

Also folgt

$$h \odot h = f(g) \odot f(g) = f(g * g) = f(e_G) = e_H.$$

Damit ist jedes Element von H sein eigenes Inverses. □

Bemerkung 2.1.49 (Beweise übersetzen)**.** Das vorherige Argument ist ein Beispiel für ein allgemeines Prinzip.

Ein Isomorphismus erlaubt es, Aussagen und Beweise von einer Gruppe in eine andere Gruppe zu übersetzen.

Wenn man eine Aussage über $(G, *)$ beweist, die nur die Gruppenstruktur verwendet, dann kann man dieselbe Aussage über jede zu G isomorphe Gruppe formulieren und beweisen.

Der Isomorphismus ist dabei das Wörterbuch: Er übersetzt Elemente von G in Elemente von H und die Verknüpfung $*$ in die Verknüpfung $\odot$.

Leitbeispiel 2.1.50 (Die Symmetrien des Dreiecks: dasselbe in zwei Sprachen)**.** Die Zuordnung aus dem letzten Abschnitt — jeder Dreieckssymmetrie ihre Eckpermutation — ist genau ein solches Wörterbuch. Sie ist eine Abbildung

$$\varphi : D_3 \longrightarrow S_3$$

und sie ist ein *Homomorphismus*: Die Eckpermutation einer Verkettung ist die Verkettung der Eckpermutationen,

$$\varphi(g \circ h) = \varphi(g) \circ \varphi(h).$$

Das lässt sich am Bild aus Leitbeispiel 2.1.18 konkret nachprüfen. Für die Drehung d um 120° und die Spiegelung s an der Achse s_1 ist $\varphi(d) = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ und $\varphi(s) = \begin{pmatrix} 2 & 3 \end{pmatrix}$. Die Verkettung $d \circ s$ — erst spiegeln, dann drehen — ist am Bild die Spiegelung an der Achse s_3, ihre Eckpermutation vertauscht also die Ecken 1 und 2. Und tatsächlich:

$$\varphi(d) \circ \varphi(s) = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 \end{pmatrix}.$$

Aus Leitbeispiel 2.1.37 wissen wir, dass φ bijektiv ist: sechs Symmetrien, sechs Permutationen, jede genau einmal getroffen. Nach Lemma 2.1.45 ist φ daher ein *Isomorphismus*,

$$D_3 \cong S_3.$$

Die geometrische Gruppe der Bewegungen und die kombinatorische Gruppe der Permutationen sind dieselbe Gruppe, nur in zwei Sprachen erzählt. Was immer wir über S_3 mit Zykeln ausrechnen, gilt damit für das Dreieck — und umgekehrt.

Lemma 2.1.51. *Seien $(G_1, *_1), (G_2, *_2)$ und $(G_3, *_3)$ Gruppen. Seien $f : G_1 \to G_2$ und $g : G_2 \to G_3$ Gruppenisomorphismen, dann ist auch $g \circ f$ ein Gruppenisomorphismus.*

Beweis. Nach Lemma 2.1.43 ist $g \circ f$ wieder ein Gruppenhomomorphismus. Da g und f bijektiv sind ist auch $g \circ f$ bijektiv. Nach Lemma 2.1.45 ist also $g \circ f$ ein Isomorphismus. □

Oben habe ich behauptet, dass man isomorphe Gruppen als „gleich im Sinne der Gruppentheorie" betrachten kann. Für solche Abschwächungen von Gleichheit haben wir bereits Äquivalenzrelationen kennengelernt. Tatsächlich ist Isomorphie eine Äquivalenzrelation.

Proposition 2.1.52 (Isomorphie ist eine Äquivalenzrelation)**.** *Sei $\mathscr{K}$ eine Menge von Gruppen. Wir definieren auf $\mathscr{K}$ eine Relation $\sim$ durch*

$$G \sim H \quad :\Longleftrightarrow \quad G \text{ ist isomorph zu } H.$$

Dann ist $\sim$ eine Äquivalenzrelation.

Beweis. Wir zeigen Reflexivität, Symmetrie und Transitivität.

Reflexivität Sei $(G, *) \in \mathscr{K}$. Die Identitätsabbildung

$$\mathrm{Id}_G : G \to G, \quad g \mapsto g$$

ist bijektiv. Außerdem gilt für alle $x, y \in G$

$$\mathrm{Id}_G(x * y) = x * y = \mathrm{Id}_G(x) * \mathrm{Id}_G(y).$$

Also ist Id_G ein Gruppenhomomorphismus. Nach Lemma 2.1.45 ist Id_G ein Isomorphismus.[1] Also gilt $G \sim G$.

Symmetrie Seien $(G, *), (H, \odot) \in \mathscr{K}$ mit $G \sim H$. Dann gibt es einen Isomorphismus

$$f : G \to H.$$

Nach Definition eines Isomorphismus ist $f^{-1} : H \to G$ ebenfalls ein Gruppenhomomorphismus. Außerdem ist f^{-1} bijektiv. Also ist f^{-1} nach Lemma 2.1.45 ein Isomorphismus.[2] Daher gilt $H \sim G$.

[1] Statt dem Lemma kann man auch verwenden, dass $(\mathrm{Id}_G)^{-1} = \mathrm{Id}_G$ gilt. Damit ist auch das Inverse ein Homomorphismus.

[2] Statt dem Lemma kann man auch verwenden, dass $(f^{-1})^{-1} = f$ gilt. Damit ist auch das Inverse von f^{-1} ein Homomorphismus.

Transitivität Seien $(G,*),(H,\odot),(K,\otimes) \in \mathscr{K}$ mit

$$G \sim H \quad \text{und} \quad H \sim K.$$

Dann gibt es Isomorphismen

$$f : G \to H \quad \text{und} \quad g : H \to K.$$

Die Komposition

$$g \circ f : G \to K$$

ist nach Lemma 2.1.51 wieder ein Isomorphismus. Also gilt $G \sim K$.

Damit ist $\sim$ reflexiv, symmetrisch und transitiv. Also ist $\sim$ eine Äquivalenzrelation. □

Isomorphismen übersetzen zwischen zwei Gruppen. Eine besonders wichtige Übersetzung findet innerhalb einer einzigen Gruppe statt. Sie bekommt einen eigenen Namen und wird uns in Kapitel 5 als Hauptdarsteller wiederbegegnen.

Definition 2.1.53 (Konjugation)**.** Sei $(G,*)$ eine Gruppe und sei $g \in G$. Die Abbildung

$$c_g : G \to G, \quad h \mapsto g * h * g^{-1}$$

heißt die *Konjugation* mit g. Das Element $g*h*g^{-1}$ heißt das *Konjugat* von h mit g. Zwei Elemente $h, h' \in G$ heißen *konjugiert*, wenn es ein $g \in G$ gibt mit

$$h' = g * h * g^{-1}.$$

Bemerkung 2.1.54 (Wie man ein Konjugat liest)**.** Besteht die Gruppe aus Abbildungen mit der Komposition als Verknüpfung — wie $\mathrm{Sym}(X)$ oder die Symmetrien des Dreiecks —, dann liest man das Konjugat $g \circ h \circ g^{-1}$ von rechts nach links:

Erst mit g^{-1} zurückholen, dann h ausführen, dann mit g wieder hinschicken.

Das Konjugat ist also die Handlung h, verpflanzt dorthin, wo g hinführt. Es verhält sich „am neuen Ort“ genauso, wie sich h „am alten Ort“ verhält. Das folgende Beispiel im Dreieck macht das konkret.

Lemma 2.1.55 (Konjugation ist ein Isomorphismus)**.** *Sei $(G,*)$ eine Gruppe und sei $g \in G$. Dann ist die Konjugation*

$$c_g : G \to G, \quad h \mapsto g * h * g^{-1}$$

ein Isomorphismus von G nach G.

Beweis. Zuerst zeigen wir, dass c_g ein Gruppenhomomorphismus ist. Seien $h, h' \in G$. Dann gilt

$$c_g(h) * c_g(h') = g * h * \underbrace{g^{-1} * g}_{=e} * h' * g^{-1} = g * h * h' * g^{-1} = c_g(h * h').$$

In der Mitte heben sich g^{-1} und g auf.

Außerdem ist c_g bijektiv, denn $c_{g^{-1}}$ ist die Umkehrabbildung:

$$c_{g^{-1}}(c_g(h)) = g^{-1} * (g * h * g^{-1}) * g = h.$$

Genauso gilt $c_g(c_{g^{-1}}(h)) = h$. Nach Lemma 2.1.45 ist c_g ein Isomorphismus. □

Lemma 2.1.56 (Konjugieren und Kommutieren)**.** *Sei $(G, *)$ eine Gruppe und seien $g, h \in G$. Dann gilt:*

$$g * h * g^{-1} = h \quad \Longleftrightarrow \quad g * h = h * g.$$

Das Konjugat von h ist also genau dann wieder h selbst, wenn g und h kommutieren. Insbesondere ändert Konjugation in einer abelschen Gruppe gar nichts.

Beweis. Multipliziert man die linke Gleichung von rechts mit g, erhält man die rechte. Multipliziert man die rechte Gleichung von rechts mit g^{-1}, erhält man die linke. □

Beispiel 2.1.57 (Konjugation im Dreieck: die Achse dreht mit)**.** Wir konjugieren in S_3 und lesen das Ergebnis über den Isomorphismus aus Leitbeispiel 2.1.50 geometrisch am Dreieck ab.

Sei $h = \begin{pmatrix} 2 & 3 \end{pmatrix}$, also die Spiegelung an der Achse durch die Ecke 1. Sei $g = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$, also die Drehung, die Ecke 1 auf Ecke 2 schiebt. Wir berechnen das Konjugat $g \circ h \circ g^{-1}$ elementweise (von rechts nach links, mit $g^{-1} = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$):

$$1 \overset{g^{-1}}{\longmapsto} 3 \overset{h}{\longmapsto} 2 \overset{g}{\longmapsto} 3, \qquad 2 \overset{g^{-1}}{\longmapsto} 1 \overset{h}{\longmapsto} 1 \overset{g}{\longmapsto} 2, \qquad 3 \overset{g^{-1}}{\longmapsto} 2 \overset{h}{\longmapsto} 3 \overset{g}{\longmapsto} 1.$$

Also ist

$$g \circ h \circ g^{-1} = \begin{pmatrix} 1 & 3 \end{pmatrix}.$$

Das ist die Spiegelung an der Achse durch die Ecke 2 — also an derjenigen Achse, auf die g die alte Achse gedreht hat. Das Konjugat der Spiegelung ist die Spiegelung an der mitgedrehten Achse: Die Handlung ist dieselbe geblieben, nur ihr Schauplatz ist mit g mitgewandert.

Dahinter steckt eine allgemeine Merkregel für Zykel: Konjugieren mit g benennt einfach die Einträge des Zykels um,

$$g \circ \begin{pmatrix} x & y \end{pmatrix} \circ g^{-1} = \begin{pmatrix} g(x) & g(y) \end{pmatrix}.$$

Man prüft das genau wie oben, indem man die drei Abbildungen nacheinander auf ein Element anwendet.

2.1.4 Das Vorzeichen einer Permutation

Wir werden am Ende dieses Abschnitts sehen (Korollar 2.1.63), dass sich jede Permutation als Produkt von (nicht notwendig disjunkten) 2-Zykeln schreiben lässt. Bezeichnen wir 2-Zykeln als *Transpositionen* so wollen wir sagen:

Eine Permutation σ heißt gerade *falls die Anzahl von Transpositionen in dieser Schreibweise gerade ist und* ungerade *sonst.*

Wir würden dann das Vorzeichen definieren als

$$\operatorname{signum} \sigma := \begin{cases} 1 & \sigma \text{ ist gerade} \\ -1 & \sigma \text{ ist ungerade} \end{cases}.$$

Das Problem an dieser Definition ist, dass wir gar nicht wissen, ob sich eine Permutation nicht sowohl als Produkt von einer geraden als auch als Produkt einer ungeraden Anzahl von Transpositionen schreiben lässt.

Die Anzahl der Transpositionen ist nicht eindeutig. Offenbar ist

$$\begin{pmatrix} 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 2 & 4 \end{pmatrix}\begin{pmatrix} 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 2 & 4 \end{pmatrix}\begin{pmatrix} 2 & 4 \end{pmatrix}\begin{pmatrix} 2 & 4 \end{pmatrix}\begin{pmatrix} 2 & 4 \end{pmatrix} = \dots,$$

denn $\begin{pmatrix} 2 & 4 \end{pmatrix}\begin{pmatrix} 2 & 4 \end{pmatrix} = \mathrm{Id}$. Dieser Trick erlaubt aber natürlich nur die Anzahl der Transpositionen um 2 zu verändern.

Tatsächlich stimmt es, dass wenn eine Permutation als Produkt einer geraden Anzahl von Transpositionen geschrieben werden kann, dass es dann nicht als Produkt einer ungeraden Anzahl geschrieben werden kann (und umgekehrt). Wenn wir das beweisen können funktioniert also die obige Definition. Aber es ist tatsächlich einfacher, das Vorzeichen anders zu definieren, dann die obige Definition als Resultat herzuleiten und daraus abzuleiten, dass die Aussage über gerade und ungerade Produkte von Transpositionen stimmt. Das Problem dabei ist, dass diese Definition keinerlei Anschauung zulässt.

Definition 2.1.58 (Das Vorzeichen einer Permutation)**.** Das Vorzeichen signum σ einer Permutation $\sigma \in S_n$ ist definiert als

$$\operatorname{signum} \sigma := \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Bemerkung 2.1.59. Eigentlich scheint dieser Definitionsversuch völlig waghalsig zu sein. Zunächst nimmt man die Zahlen $\{1, \dots, n\}$, die ja zunächst einfach nur für beliebige Elemente die eben vertauscht werden stehen, wortwörtlich und verwendet ihren konkreten Zahlenwert. Dann bildet man Brüche aus Differenzen und bildet das Produkt. Das wird eine rationale Zahl ergeben. Aller Wahrscheinlichkeit nach aber keine ganze Zahl. Aber das Vorzeichen soll ja sogar entweder $+1$ oder -1 sein. Wir werden nun sehen, dass sich das Produkt sehr viel besser verhält als wir auf den ersten Blick erwarten würden.

Bemerkung 2.1.60 (Ein Unbehagen bleibt: die Zahlenwerte)**.** Das folgende Lemma wird zeigen, dass die Brüche sich wegkürzen und tatsächlich immer ± 1 herauskommt. Ein zweites Unbehagen können wir an dieser Stelle noch nicht auflösen: Permutationen kann man von *jeder* n-elementigen Menge bilden — die Ecken eines Dreiecks, die Gäste an einem Tisch. Die Formel behandelt die Elemente $1, \dots, n$ aber nicht als bloße Namen, sondern rechnet mit ihren Zahlenwerten: Sie bildet Differenzen wie $\sigma(j) - \sigma(i)$. Nummeriert man dieselben Objekte anders durch, ist zunächst überhaupt nicht klar, dass am Ende dasselbe Vorzeichen herauskommt. Es kommt dasselbe heraus — und der Grund ist ein schönes allgemeines Prinzip über Gruppenhomomorphismen in abelsche Gruppen, das wir in Kapitel 5 beweisen. Bis dahin merken wir uns: Die Zahlenwerte sind ein Gerüst für die *Formel*, nicht für den *Begriff*.

Beispiel 2.1.61 (Die Formel einmal ausgerechnet)**.** Für die Transposition $\sigma = \begin{pmatrix} 1 & 2 \end{pmatrix}$ in S_3 durchläuft das Produkt die Paare $(1,2)$, $(1,3)$ und $(2,3)$:

$$\operatorname{signum} \sigma = \frac{\sigma(2) - \sigma(1)}{2-1} \cdot \frac{\sigma(3) - \sigma(1)}{3-1} \cdot \frac{\sigma(3) - \sigma(2)}{3-2} = \frac{1-2}{1} \cdot \frac{3-2}{2} \cdot \frac{3-1}{1} = (-1) \cdot \tfrac{1}{2} \cdot 2 = -1.$$

Unterwegs tauchen tatsächlich Brüche auf (das $\frac{1}{2}$), aber am Ende kürzt sich alles zu -1 — genau das Verhalten, das das folgende Lemma erklärt.

Lemma 2.1.62 (Eigenschaften des Vorzeichens)**.** *Sei $n \in \mathbb{N}$. Dann gilt:*

1. *Sei $\sigma \in S_n$. Dann gilt* $\operatorname{signum} \sigma \in \{-1, +1\}$ *und sogar*

$$\operatorname{signum} \sigma = (-1)^N,$$

   wobei N die Anzahl der Paare (i,j) mit $i < j$ und $\sigma(i) > \sigma(j)$ ist.

2. *Das Vorzeichen ist ein Gruppenhomomorphismus*

$$\operatorname{signum} : (S_n, \circ) \longrightarrow (\{-1, +1\}, \cdot).$$

   Das heißt, für alle $\sigma, \tau \in S_n$ gilt

$$\operatorname{signum}(\sigma \circ \tau) = \operatorname{signum}(\sigma) \cdot \operatorname{signum}(\tau).$$

3. *Ist $\sigma \in S_n$ eine Transposition, also ein 2-Zykel, dann gilt*

$$\operatorname{signum} \sigma = -1.$$

4. *Ist $\sigma \in S_n$ ein r-Zykel, dann gilt*

$$\operatorname{signum} \sigma = (-1)^{r-1}.$$

Beweis. Wir schreiben

$$X_n := \{1, \dots, n\}.$$

Zu (a): Für jedes Paar $i < j$ ist der Nenner $j - i$ positiv. Im Zähler steht der Faktor $\sigma(j) - \sigma(i)$. Da σ bijektiv ist, läuft das ungeordnete Paar $\{\sigma(i), \sigma(j)\}$ beim Durchlaufen aller Paare $i < j$ genau einmal durch alle zweielementigen Teilmengen von X_n. Daher kommen im Zähler dieselben absoluten Werte vor wie im Nenner: Zu jedem Paar $a < b$ kommt genau einmal der Faktor $\pm(b - a)$ vor. Also kürzen sich alle absoluten Werte weg und es bleibt nur ein Vorzeichen übrig. Folglich gilt $\operatorname{signum} \sigma \in \{-1, +1\}$.

Ein Faktor $\sigma(j) - \sigma(i)$ ist genau dann negativ, wenn $\sigma(i) > \sigma(j)$ gilt. Die negativen Faktoren werden also genau durch die Paare (i, j) mit $i < j$ und $\sigma(i) > \sigma(j)$ gezählt. Ist N die Anzahl dieser Paare, so folgt

$$\operatorname{signum} \sigma = (-1)^N.$$

Zu (b): Wir betrachten zunächst einen kleinen Notationstrick. Für eine zweielementige Teilmenge $P = \{i, j\} \subseteq X_n$ setzen wir

$$D_\rho(P) := \frac{\rho(j) - \rho(i)}{j - i}$$

für $\rho \in S_n$. Diese Zahl hängt nicht davon ab, in welcher Reihenfolge wir die beiden Elemente von P als i und j schreiben, denn beim Vertauschen von i und j ändern sowohl Zähler als auch Nenner ihr Vorzeichen. Damit können wir schreiben

$$\operatorname{signum} \rho = \prod_{\substack{P \subseteq X_n \\ |P|=2}} D_\rho(P).$$

Seien nun $\sigma, \tau \in S_n$. Für $P = \{i, j\}$ gilt

$$\begin{aligned} D_{\sigma\circ\tau}(P) &= \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j - i} \\ &= \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \cdot \frac{\tau(j) - \tau(i)}{j - i} \\ &= D_\sigma(\{\tau(i), \tau(j)\}) \cdot D_\tau(P). \end{aligned}$$

Dabei ist $\tau(i) \neq \tau(j)$, weil τ injektiv ist. Außerdem permutiert τ die zweielementigen Teilmengen von X_n. Also gilt

$$\begin{aligned} \operatorname{signum}(\sigma \circ \tau) &= \prod_{\substack{P \subseteq X_n \\ |P|=2}} D_{\sigma\circ\tau}(P) \\ &= \prod_{\substack{P \subseteq X_n \\ |P|=2}} D_\sigma(\tau(P)) \cdot \prod_{\substack{P \subseteq X_n \\ |P|=2}} D_\tau(P) \\ &= \prod_{\substack{Q \subseteq X_n \\ |Q|=2}} D_\sigma(Q) \cdot \prod_{\substack{P \subseteq X_n \\ |P|=2}} D_\tau(P) \\ &= \operatorname{signum} \sigma \cdot \operatorname{signum} \tau. \end{aligned}$$

Damit ist signum ein Gruppenhomomorphismus.

Zu (c): Sei σ eine Transposition. Dann gibt es $a < b$ mit

$$\sigma(a) = b, \quad \sigma(b) = a, \quad \sigma(\ell) = \ell \text{ für } \ell \notin \{a, b\}.$$

Nach (a) genügt es, die Anzahl der Inversionen von σ modulo 2 zu bestimmen. Eine Inversion ist zunächst das Paar (a, b). Außerdem gibt es für jedes ℓ mit $a < \ell < b$ genau zwei weitere Inversionen, nämlich (a, ℓ) und (ℓ, b). Alle anderen Paare liefern keine Inversion. Die Anzahl der Inversionen ist also

$$1 + 2(b - a - 1),$$

und diese Zahl ist ungerade. Mit (a) folgt daher $\operatorname{signum} \sigma = -1$.

Zu (d): Wir beweisen die Aussage per Induktion über r. Der Fall $r = 2$ ist genau (c). Sei nun $r \geqslant 3$ und sei

$$\sigma = \begin{pmatrix} x_1 & x_2 & \dots & x_r \end{pmatrix}$$

ein r-Zykel. Dann gilt

$$\begin{pmatrix} x_1 & x_2 & \dots & x_r \end{pmatrix} = \begin{pmatrix} x_1 & x_r \end{pmatrix} \circ \begin{pmatrix} x_1 & x_2 & \dots & x_{r-1} \end{pmatrix}.$$

Nach (b), (c) und der Induktionsannahme folgt

$$\operatorname{signum} \sigma = \operatorname{signum} \begin{pmatrix} x_1 & x_r \end{pmatrix} \cdot \operatorname{signum} \begin{pmatrix} x_1 & x_2 & \dots & x_{r-1} \end{pmatrix} = (-1) \cdot (-1)^{r-2} = (-1)^{r-1}.$$

□

Korollar 2.1.63 (Jede Permutation ist ein Produkt von Transpositionen)**.** *Jede Permutation $\sigma \in S_n$ lässt sich als Produkt von Transpositionen schreiben. (Die Identität schreibt man dabei etwa als $\begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix}$.)*

Beweis. Nach Theorem 2.1.33 ist σ ein Produkt von Zykeln. Es genügt also, jeden einzelnen Zykel als Produkt von Transpositionen zu schreiben. Das leistet dieselbe Abspaltungsformel, die schon im Beweis von Teil (d) benutzt wurde, durch wiederholtes Anwenden:

$$\begin{pmatrix} x_1 & x_2 & \dots & x_r \end{pmatrix} = \begin{pmatrix} x_1 & x_r \end{pmatrix} \circ \begin{pmatrix} x_1 & x_{r-1} \end{pmatrix} \circ \cdots \circ \begin{pmatrix} x_1 & x_2 \end{pmatrix}.$$

Ein r-Zykel ist also ein Produkt von $r - 1$ Transpositionen. □

Korollar 2.1.64 (Die Parität ist wohldefiniert)**.** *Ist $\sigma = \tau_1 \circ \cdots \circ \tau_m$ ein Produkt von Transpositionen, dann gilt*

$$\operatorname{signum} \sigma = (-1)^m.$$

Insbesondere ist die Parität von m durch σ festgelegt: Keine Permutation lässt sich sowohl als Produkt einer geraden *als auch einer* ungeraden *Anzahl von Transpositionen schreiben.*

Beweis. Da signum nach Teil (b) ein Homomorphismus ist und jede Transposition nach Teil (c) das Vorzeichen -1 hat, gilt

$$\operatorname{signum} \sigma = \operatorname{signum} \tau_1 \cdots \operatorname{signum} \tau_m = (-1)^m.$$

Wäre σ zugleich ein Produkt von m und von m' Transpositionen mit verschiedener Parität, dann wäre $(-1)^m = \operatorname{signum} \sigma = (-1)^{m'}$ — ein Widerspruch. □

Bemerkung 2.1.65 (Das Eingangsproblem ist gelöst)**.** Damit ist die Sorge vom Anfang des Abschnitts ausgeräumt: Die Begriffe *gerade* und *ungerade* sind wohldefiniert, und sie stimmen mit dem Vorzeichen überein — $\operatorname{signum}\sigma = +1$ heißt *gerade*, $\operatorname{signum}\sigma = -1$ heißt *ungerade*. Die waghalsige Bruchformel war also nur ein Gerüst; stehen bleibt die anschauliche Definition, mit der wir angefangen haben.

Leitbeispiel 2.1.66 (Die Symmetrien des Dreiecks: das Vorzeichen ist das Umklappen)**.** Über den Isomorphismus $D_3 \cong S_3$ aus Leitbeispiel 2.1.50 bekommt das Vorzeichen eine rein geometrische Bedeutung. Die Drehungen sind die Identität und die beiden 3-Zykel; nach Teil (d) des Lemmas hat ein 3-Zykel das Vorzeichen $(-1)^{3-1} = +1$. Die Spiegelungen sind Transpositionen, haben also Vorzeichen -1. Damit beantwortet

$$\operatorname{signum} : S_3 \longrightarrow \{+1, -1\},$$

über den Isomorphismus als Abbildung auf den Dreieckssymmetrien gelesen, eine anschauliche Frage: *Bleibt das Dreieck in der Ebene liegen, oder wird es umgeklappt?* Drehungen bewegen es innerhalb der Ebene und erhalten die Orientierung ($\operatorname{signum} = +1$); Spiegelungen klappen es um und kehren die Orientierung um ($\operatorname{signum} = -1$).

Beim „Umklappen“ lohnt ein zweiter Blick. *Innerhalb* der Ebene ist eine Spiegelung durch keine noch so geschickte Kombination aus Drehen und Verschieben zu erreichen — ein Wesen, das in der Ebene lebt, kann das Dreieck nicht umklappen. Wir können es nur, weil wir das Papierdreieck durch die *dritte* Dimension wenden.

Die Symmetrien mit $\operatorname{signum} = +1$ — die drei Drehungen — bilden für sich genommen wieder eine Gruppe: die Gruppe der *eigentlichen*, orientierungserhaltenden Symmetrien. (Eine Teilmenge einer Gruppe, die selbst eine Gruppe bildet, nennt man eine *Untergruppe*; diese spezielle Untergruppe heißt der *Kern* von signum — beide Begriffe werden uns später systematisch wiederbegegnen.) Und dass signum ein Homomorphismus ist, hat eine handfeste Lesart: Zwei Umklappungen heben sich zu einer Drehung auf, so wie sich beim Multiplizieren zwei Minuszeichen aufheben.

Für die physikalische Interpretation ist die Frage der Orientierungserhaltung auch wichtig: Ein linker Handschuh kann nicht durch geschickte Bewegung in einen rechten Handschuh verwandelt werden (innerhalb des $\mathbb{R}^3$). Das ist dieselbe Situation wie beim Dreieck, nur eine Dimension höher — so wie das flache Dreieck sich nur durch die dritte Dimension umklappen ließ, bräuchte der räumliche Handschuh eine vierte Dimension, um sich zu wenden. Ob ein solches Umklappen also als Symmetrie akzeptiert wird, hängt davon ab, welche Bewegungen man zulässt. Die Händigkeit von Molekülen ist beispielsweise höchst relevant. Manche Moleküle sind in der einen Händigkeit gesund und in der spiegelbildlichen Form giftig (mehr dazu findet man unter dem Stichwort *Chiralität*). Hier kann das Vorzeichen also eine wichtige Unterscheidung sein. (Unser flaches BF_3 ist dagegen selbst *nicht* händig: Sein Spiegelbild lässt sich im Raum durch das Umklappen wieder mit dem Original zur Deckung bringen — genau wie beim Papierdreieck.)

2.2 Ringe

Bemerkung 2.2.1 (Von Gruppen zu Ringen)**.** Bisher haben wir Strukturen betrachtet, bei denen es nur eine Verknüpfung gibt. Jetzt lernen wir Ringe kennen.

In diesen gibt es die sogenannte „Addition“ und die „Multiplikation“. Die Addition soll sich wie die Addition von Zahlen verhalten. Die Multiplikation soll zumindest assoziativ sein und ein neutrales Element besitzen.

Außerdem müssen Addition und Multiplikation miteinander verträglich sein. Diese Verträglichkeit wird durch die Distributivgesetze ausgedrückt.

Bemerkung 2.2.2 (Name der Verknüpfungen)**.** Bei Gruppen gibt es eine Menge und eine Verknüpfung, die wir zum Beispiel als Addition oder Multiplikation oder eine beliebige andere Operation interpretieren können. Daher konnten wir die Verknüpfung recht beliebig als „Addition", „Multiplikation" oder ganz anders bezeichnen.

Bei Ringen treten nun zwei Verknüpfungen gleichzeitig auf, diese wechselwirken miteinander und spielen unterschiedliche Rollen. Das Wechselspiel der Verknüpfungen ist – wie wir in den Beispielen sehen werden – sehr analog zu dem der Addition und Multiplikation auf $\mathbb{Z}$, daher werden wir die eine fest als „Addition" und die andere fest als „Multiplikation" bezeichnen. Auch in unserer Notation werden wir diese Analogie hervorheben.

Definition 2.2.3 (Ring)**.** Ein *Ring* ist ein Tupel $(R, +, 0, \cdot, 1)$, bestehend aus einer Menge R, einer Addition

$$+ : R \times R \to R,$$

einem Element $0 \in R$, einer Multiplikation

$$\cdot : R \times R \to R,$$

und einem Element $1 \in R$, sodass die folgenden Eigenschaften gelten.

(R1) **Additive Struktur.**

Das Tripel $(R, +, 0)$ ist eine abelsche Gruppe.

Das bedeutet: Für alle $x, y, z \in R$ gilt

$$x + (y + z) = (x + y) + z,$$

für alle $x \in R$ gilt

$$0 + x = x \quad \textit{und} \quad x + 0 = x,$$

zu jedem $x \in R$ gibt es ein additives Inverses $-x \in R$, und für alle $x, y \in R$ gilt

$$x + y = y + x.$$

(R2) **Assoziativität der Multiplikation.**

Für alle $x, y, z \in R$ gilt

$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

(R3) **Einselement.**

Für alle $x \in R$ gilt

$$1 \cdot x = x \quad \text{und} \quad x \cdot 1 = x.$$

(R4) **Distributivgesetze.**

Für alle $x, y, z \in R$ gilt

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

und

$$(x + y) \cdot z = x \cdot z + y \cdot z.$$

Wir schreiben meistens kurz xy statt $x \cdot y$.
Der Ring heißt *kommutativ*, wenn zusätzlich für alle $x, y \in R$ gilt

$$xy = yx.$$

Bemerkung 2.2.4 (Konvention)**.** In diesem Skript besitzt ein Ring immer ein Einselement.
Manche Bücher verwenden das Wort „Ring“ allgemeiner und verlangen kein Einselement.
Dann sagt man für unsere Definition manchmal „Ring mit Eins“ oder „unitärer Ring“.
Wir wählen hier die Version mit Einselement, weil sie besonders gut zu Körpern und Vektorräumen passt.

Bemerkung 2.2.5 (Kommutativität von Ringen)**.** Die Addition eines Ringes ist immer kommutativ. Ob ein Ring als „kommutativ“ gilt hängt also ausschließlich daran, ob die Multiplikation kommutativ ist.

Beispiel 2.2.6 (Erste Beispiele)**.**

1. Die ganzen Zahlen bilden mit der üblichen Addition und Multiplikation einen Ring
$$(\mathbb{Z}, +, 0, \cdot, 1).$$
2. Auch
$$(\mathbb{Q}, +, 0, \cdot, 1) \quad \text{und} \quad (\mathbb{R}, +, 0, \cdot, 1)$$
sind Ringe.
3. Die Menge $\mathbb{R}[X]$ aller Polynome mit reellen Koeffizienten ist ein Ring.
Addition und Multiplikation sind dabei die übliche Addition und Multiplikation von Polynomen.
4. Der Nullring besteht nur aus einem Element:
$$R = \{0\}.$$
In diesem Ring gilt notwendigerweise
$$0 = 1.$$
Der Nullring ist nach unserer Definition also erlaubt.

Leitbeispiel 2.2.7 (Die Uhr: Restklassenringe)**.** Als zweites Leitbeispiel — für Ringe und Körper — nehmen wir die *Uhr*. Auf einer 12-Stunden-Uhr ist $10 + 5 = 3$ und nicht 15: Man rechnet *modulo* 12. Allgemein bilden für $n \in \mathbb{N}$ die Restklassen
$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \dots, [n-1]\}$$
mit
$$[a] + [b] := [a + b] \qquad \text{und} \qquad [a] \cdot [b] := [a \cdot b]$$
einen kommutativen Ring. Die additive Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$ kennen wir schon aus dem Gruppenkapitel. Neu ist die Multiplikation — und mit ihr lösen wir das Versprechen aus dem Gruppenkapitel ein und schauen der *Wohldefiniertheit* einmal wirklich ins Auge.

Das Problem: Die Vorschrift $[a] \cdot [b] := [a \cdot b]$ rechnet mit den *Vertretern* a und b — aber dieselbe Restklasse trägt viele Namen. Auf der Uhr ist $[10] = [22]$, denn 22 Uhr ist 10 Uhr. Rechnen wir also beide Wege:
$$[10] \cdot [5] = [50] = [2] \qquad \text{und} \qquad [22] \cdot [5] = [110] = [2].$$

Dasselbe Ergebnis — und das ist kein Zufall. Sind $[a] = [a']$ und $[b] = [b']$, dann teilt n sowohl $a - a'$ als auch $b - b'$, und wegen

$$ab - a'b' = a(b - b') + (a - a')b'$$

teilt n auch $ab - a'b'$, also ist $[ab] = [a'b']$. Die Vorschrift ist *wohldefiniert*: Das Ergebnis hängt nicht davon ab, welche Vertreter man wählt.

Dass das keine Selbstverständlichkeit ist, zeigt ein Gegenbeispiel. Die Vorschrift $Q([a]) :=$ [Quersumme von a] definiert auf $\mathbb{Z}/12\mathbb{Z}$ *gar nichts*: Es ist $[10] = [22]$, aber Q würde einmal $[1]$ und einmal $[4]$ liefern. Wer auf Restklassen etwas definieren will, muss die Wohldefiniertheit also stets prüfen.

An unserem Ring zeigt sich außerdem ein Phänomen, das es in $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ nicht gibt. In $\mathbb{Z}/6\mathbb{Z}$ gilt

$$[2] \cdot [3] = [6] = [0] \ :$$

Ein Produkt zweier von null verschiedener Elemente kann null sein. Solche Elemente bekommen gleich einen eigenen Namen. Ob ein Restklassenring sie enthält, entscheidet im nächsten Abschnitt darüber, ob aus ihm sogar ein Körper wird.

Definition 2.2.8 (Nullteiler)**.** Sei R ein kommutativer Ring. Ein Element $x \in R$ mit $x \neq 0$ heißt *Nullteiler*, wenn es ein $y \in R$ mit $y \neq 0$ und

$$x \cdot y = 0$$

gibt. Im Leitbeispiel sind also $[2]$ und $[3]$ Nullteiler von $\mathbb{Z}/6\mathbb{Z}$.

Proposition 2.2.9 (Eindeutigkeit der neutralen Elemente in Ringen)**.** *Sei $(R, +, 0, \cdot, 1)$ ein Ring.*
Dann sind 0 und 1 eindeutig bestimmt.
Genauer gilt:

1. *Es gibt in $(R, +)$ genau ein neutrales Element.*
2. *Es gibt bezüglich der Multiplikation genau ein beidseitig neutrales Element.*

Beweis. Die Eindeutigkeit von 0 folgt sofort daraus, dass $(R, +, 0)$ eine Gruppe ist.
Wir haben bereits gesehen, dass das neutrale Element einer Gruppe eindeutig ist.
Nun zeigen wir die Eindeutigkeit von 1.
Seien 1_R und $1'_R$ zwei beidseitig neutrale Elemente bezüglich der Multiplikation.
Da 1_R neutral ist, gilt

$$1_R \cdot 1'_R = 1'_R.$$

Da $1'_R$ neutral ist, gilt aber auch

$$1_R \cdot 1'_R = 1_R.$$

Also folgt

$$1_R = 1_R \cdot 1'_R = 1'_R.$$

Damit ist auch das Einselement eindeutig. □

Bemerkung 2.2.10 (Wie allgemein sollte man Aussagen formulieren?)**.** Der Beweis für die Eindeutigkeit des neutralen Elements in Gruppen (in Proposition 2.1.8) hat gar nicht benutzt, dass es Inverse gibt. Daher konnten wir *den Beweis* im Wortlaut (nicht aber die bewiesene *Aussage* Proposition 2.1.8) oben wiederverwenden.

Der Beweis hat auch nicht benutzt, dass die Multiplikation assoziativ ist. Er hat nur benutzt, dass zwei Elemente beide beidseitig neutral für dieselbe Verknüpfung sind.

Also gilt allgemeiner: Wenn eine Menge mit einer beliebigen zweistelligen Verknüpfung überhaupt ein beidseitig neutrales Element besitzt, dann ist dieses eindeutig.

Man könnte diesen allgemeineren Satz sofort formulieren und beweisen. Das hätte den Vorteil, dass wir ihn später in vielen Situationen direkt wiederverwenden könnten. Oben könnten wir also in beiden Fällen einfach den allgemeinen Satz zitieren ohne den Beweis zu wiederholen.

Der Nachteil wäre aber, dass wir dafür mehr Begriffe auf einmal einführen müssten. In der Darstellung von Mathematik muss man deshalb immer entscheiden, wie viel Allgemeinheit man gerade tragen möchte.

Mehr Allgemeinheit macht Aussagen oft wiederverwendbarer. Zu viel Allgemeinheit kann aber am Anfang verdecken, worum es in der konkreten Situation eigentlich geht.

Wir beweisen manche Aussagen deshalb zunächst dort, wo wir sie brauchen, und weisen danach darauf hin, dass der Beweis eigentlich allgemeiner funktioniert.

Lemma 2.2.11 (Multiplikation mit Null)**.** *Sei* $(R, +, 0, \cdot, 1)$ *ein Ring.*
Dann gilt für jedes $x \in R$

$$0 \cdot x = 0 \quad \textit{und} \quad x \cdot 0 = 0.$$

Beweis. Wir zeigen zuerst $0 \cdot x = 0$.

Da 0 das neutrale Element der Addition ist, gilt

$$0 + 0 = 0.$$

Also gilt

$$0 \cdot x = (0 + 0) \cdot x.$$

Mit dem Distributivgesetz folgt

$$(0 + 0) \cdot x = 0 \cdot x + 0 \cdot x.$$

Zusammen erhalten wir

$$0 \cdot x = 0 \cdot x + 0 \cdot x.$$

Wir addieren auf beiden Seiten das additive Inverse von $0 \cdot x$.
Dann folgt

$$0 = 0 \cdot x.$$

Also gilt

$$0 \cdot x = 0.$$

Der Beweis von $x \cdot 0 = 0$ ist analog.
Man benutzt

$$x \cdot 0 = x \cdot (0 + 0)$$

und danach das andere Distributivgesetz. □

Alternativer Beweis. Wir geben noch einen zweiten Beweis, weil er die Struktur hinter der Rechnung sichtbar macht.

Fixiere ein Element $x \in R$.
Wir betrachten die Abbildung

$$R_x : R \to R, \quad y \mapsto yx.$$

Diese Abbildung ist ein Gruppenhomomorphismus

$$R_x : (R, +, 0) \to (R, +, 0).$$

Denn für alle $y, z \in R$ gilt

$$R_x(y + z) = (y + z)x = yx + zx = R_x(y) + R_x(z).$$

Gruppenhomomorphismen erhalten neutrale Elemente.
Also gilt

$$R_x(0) = 0.$$

Das bedeutet genau

$$0x = 0.$$

Genauso betrachten wir die Abbildung

$$L_x : R \to R, \quad y \mapsto xy.$$

Auch sie ist ein Gruppenhomomorphismus

$$L_x : (R, +, 0) \to (R, +, 0),$$

denn für alle $y, z \in R$ gilt

$$L_x(y + z) = x(y + z) = xy + xz = L_x(y) + L_x(z).$$

Also gilt

$$L_x(0) = 0.$$

Das bedeutet genau

$$x0 = 0.$$

□

Definition 2.2.12 (Minuszeichen in Ringen)**.** In Ringen haben wir zwei Verknüpfungen, also im allgemeinen unterschiedliche Inverse, je nach dem ob wir bezüglich der Addition und der Multiplikation das Inverse bestimmen. Bezüglich der Multiplikation muss es in Ringen natürlich gar keine Inversen Elemente geben.

Wir schreiben $-x$ für das *additive Inverse* von x. Damit meinen wir das eindeutige Element (siehe Lemma 2.1.22 2)) $y \in R$ mit

$$y + x = 0 = x + y.$$

Lemma 2.2.13 (Rechenregeln des Minuszeichens in Ringen)**.** *Sei* $(R, +, 0, \cdot, 1)$ *ein Ring.*
Dann gelten:

1. *Für alle* $x, y \in R$ *gilt*
$$x \cdot (-y) = (-x) \cdot y = -(xy).$$
2. *Es gilt*
$$(-1)^2 = 1.$$

Beweis. Wir benutzen jetzt systematisch folgenden Gedanken: In der additiven Gruppe $(R, +, 0)$ sind additive inverse Elemente eindeutig. Um also zu zeigen, dass ein Element a gleich $-b$ ist, genügt es zu zeigen, dass

$$b + a = 0.$$

Seien nun $x, y \in R$. Wir zeigen zuerst

$$x \cdot (-y) = -(xy).$$

Dazu reicht es also wegen der Eindeutigkeit additiver Inverser zu zeigen, dass $x \cdot (-y)$ ein additives Inverses von xy ist. Es gilt

$$xy + x \cdot (-y) = x \cdot y + x \cdot (-y) = x \cdot (y + (-y)) = x \cdot 0 = 0.$$

Also ist $x \cdot (-y)$ das additive Inverse von xy. Daher gilt

$$x \cdot (-y) = -(xy).$$

Analog zeigen wir

$$(-x) \cdot y = -(xy).$$

Es gilt nämlich

$$xy + (-x) \cdot y = x \cdot y + (-x) \cdot y = (x + (-x)) \cdot y = 0 \cdot y = 0.$$

Also ist auch $(-x) \cdot y$ das additive Inverse von xy. Damit gilt

$$x \cdot (-y) = (-x) \cdot y = -(xy).$$

Es bleibt zu zeigen, dass $(-1)^2 = 1$ gilt. Wir zeigen wieder, dass zwei Elemente dasselbe additive Inverse sind. Zunächst ist 1 ein additives Inverses von -1, denn

$$(-1) + 1 = 0.$$

Andererseits gilt

$$(-1)^2 + (-1) = (-1) \cdot (-1) + 1 \cdot (-1).$$

Mit dem Distributivgesetz erhalten wir

$$(-1) \cdot (-1) + 1 \cdot (-1) = ((-1) + 1) \cdot (-1).$$

Also folgt

$$(-1)^2 + (-1) = 0 \cdot (-1) = 0.$$

Damit ist $(-1)^2$ ebenfalls ein additives Inverses von -1. Wegen der Eindeutigkeit additiver Inverser folgt

$$(-1)^2 = 1.$$

□

2.3 Körper

Bemerkung 2.3.1 (Von Ringen zu Körpern)**.** Ringe erlauben Addition, Subtraktion und Multiplikation.

Was in einem allgemeinen Ring aber fehlen kann, ist Division.

Zum Beispiel ist $\mathbb{Z}$ ein Ring. In $\mathbb{Z}$ können wir zwar addieren, subtrahieren und multiplizieren. Aber wir können nicht immer dividieren: Die Gleichung

$$2x = 1$$

hat keine Lösung in $\mathbb{Z}$.

Körper sind Ringe, in denen diese Schwierigkeit für alle Elemente ungleich 0 verschwindet.

Definition 2.3.2 (Körper)**.** Ein *Körper* ist ein kommutativer Ring

$$(k, +, 0, \cdot, 1),$$

der zusätzlich die folgenden beiden Eigenschaften erfüllt.

(K1) Es gilt

$$1 \neq 0.$$

(K2) Jedes Element ungleich 0 besitzt ein multiplikatives Inverses.

Das heißt: Für jedes $x \in k$ mit $x \neq 0$ gibt es ein $y \in k$ mit

$$xy = 1.$$

Bemerkung 2.3.3 (Körper als gute Skalarenbereiche)**.** Ein Körper fasst die algebraischen Eigenschaften zusammen, die wir von „Zahlen, mit denen man gut skalieren und rechnen kann“ erwarten.

Man kann addieren, subtrahieren, multiplizieren und durch jedes Element ungleich 0 dividieren.

Genau deshalb werden Körper später in der Theorie der Vektorräume als Skalarenbereiche verwendet.

Bemerkung 2.3.4 (Alternative Formulierung)**.** Sei k ein kommutativer Ring mit $1 \neq 0$. Wir setzen

$$k^\times := k \setminus \{0\}.$$

Dann ist k genau dann ein Körper, wenn $k^\times$ bezüglich der Multiplikation eine Gruppe ist.

Das neutrale Element dieser Gruppe ist 1.

Die Inversen in dieser Gruppe sind genau die multiplikativen Inversen der Elemente ungleich 0.

Beispiel 2.3.5 (Erste Beispiele und Nichtbeispiele)**.**

1. Die rationalen Zahlen bilden einen Körper

$$(\mathbb{Q}, +, 0, \cdot, 1).$$

Ist $x \in \mathbb{Q}$ und $x \neq 0$, dann ist auch $\frac{1}{x} \in \mathbb{Q}$.

2. Die reellen Zahlen bilden einen Körper

$$(\mathbb{R}, +, 0, \cdot, 1).$$

3. Die komplexen Zahlen bilden einen Körper

$$(\mathbb{C}, +, 0, \cdot, 1).$$

   Man kann $\mathbb{C}$ als $\mathbb{R}^2$ auffassen.

   Die Addition ist komponentenweise gegeben durch

$$(a, b) + (c, d) := (a + c, b + d).$$

   Die Multiplikation ist gegeben durch

$$(a, b) \cdot (c, d) := (ac - bd, ad + bc).$$

   Schreibt man

$$i := (0, 1),$$

   und identifiziert man $a \in \mathbb{R}$ mit $(a, 0) \in \mathbb{C}$, dann gilt

$$(a, b) = a + bi$$

   und insbesondere

$$i^2 = -1.$$

4. Die ganzen Zahlen bilden keinen Körper.

   Der Grund ist: Es gilt $2 \in \mathbb{Z}$ und $2 \neq 0$. Aber es gibt kein $x \in \mathbb{Z}$ mit

$$2x = 1.$$

   Also besitzt 2 in $\mathbb{Z}$ kein multiplikatives Inverses.

5. Die Restklassen modulo 2 bilden einen Körper

$$\mathbb{Z}/2\mathbb{Z}.$$

   Dieser Körper hat genau zwei Elemente:

$$\mathbb{Z}/2\mathbb{Z} = \{0, 1\}.$$

   Hier lassen wir — wie allgemein üblich, wenn keine Verwechslungsgefahr besteht — die Klammern weg und schreiben a statt $[a]$; gemeint ist immer die Restklasse.

   Addition und Multiplikation werden modulo 2 gerechnet. Also gilt insbesondere

$$1 + 1 = 0, \quad 1 \cdot 1 = 1.$$

   Die Gleichung $1 + 1 = 0$ ist dabei keine falsche Zahlengleichung, sondern eine wahre Aussage über Restklassen: $[1] + [1] = [2] = [0]$.

   Für diesen Körper schreiben wir auch

$$\mathbb{F}_2 := \mathbb{Z}/2\mathbb{Z}.$$

   Der Buchstabe $\mathbb{F}$ steht dabei für „field“, also das englische Wort für Körper.

Leitbeispiel 2.3.6 (Die Uhr: wann $\mathbb{Z}/n\mathbb{Z}$ ein Körper ist)**.** Wir kehren zur Uhr Leitbeispiel 2.2.7 zurück. Wann ist $\mathbb{Z}/n\mathbb{Z}$ ein Körper, wann kann man also durch jedes Element $\neq [0]$ teilen? Die Nullteiler geben die Antwort.

Ist n zusammengesetzt, etwa $n = 6 = 2 \cdot 3$, so gilt $[2] \cdot [3] = [0]$. Hätte $[2]$ ein multiplikatives Inverses $[x]$, also $[x] \cdot [2] = [1]$, so folgte

$$[3] = [1] \cdot [3] = [x] \cdot [2] \cdot [3] = [x] \cdot [0] = [0],$$

ein Widerspruch. Also besitzt $[2]$ kein Inverses, und $\mathbb{Z}/6\mathbb{Z}$ ist *kein* Körper.

Ist dagegen $n = p$ eine *Primzahl*, so gibt es keine Nullteiler. (Das liegt an einer Grundtatsache über Primzahlen: Teilt p ein Produkt ab, dann teilt p schon a oder b — aus $[a] \cdot [b] = [0]$ folgt also $[a] = [0]$ oder $[b] = [0]$.) Und ohne Nullteiler besitzt tatsächlich jedes $[a] \neq [0]$ ein Inverses. Das ist ein hübsches Endlichkeits-Argument: Die Abbildung $[x] \mapsto [a] \cdot [x]$ von $\mathbb{Z}/p\mathbb{Z}$ in sich ist *injektiv*, denn aus $[a][x] = [a][y]$ folgt $[a]([x] - [y]) = [0]$, und da $[a] \neq [0]$ kein Nullteiler ist, muss $[x] = [y]$ sein. Eine injektive Abbildung einer *endlichen* Menge in sich ist aber surjektiv — insbesondere wird $[1]$ getroffen, es gibt also ein $[x]$ mit $[a] \cdot [x] = [1]$. Man sieht das auch konkret, etwa in $\mathbb{Z}/5\mathbb{Z}$:

$$[2] \cdot [3] = [6] = [1], \qquad [4] \cdot [4] = [16] = [1],$$

jedes Element $\neq [0]$ findet seinen Partner. Kurz:

$$\mathbb{Z}/n\mathbb{Z} \text{ ist ein Körper} \quad \Longleftrightarrow \quad n \text{ ist eine Primzahl.}$$

Der kleinste Fall $n = 2$ ist der oben eingeführte Körper $\mathbb{F}_2$. So entstehen die *endlichen* Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$: Zahlbereiche mit nur endlich vielen Elementen, in denen man dennoch uneingeschränkt addieren, multiplizieren und teilen kann. Neben den endlichen Körpern der Form $\mathbb{Z}/p\mathbb{Z}$ gibt es noch Körper mit komplexerer interner Struktur. Tatsächlich sind endliche Körper das Rückgrat der modernen Kryptographie und Codierungstheorie.

Definition 2.3.7 (Multiplikative Inverse)**.** Sei k ein Körper und sei $x \in k$ mit $x \neq 0$.

Nach Definition eines Körpers gibt es ein $y \in k$ mit

$$xy = 1.$$

Da k kommutativ ist, gilt dann auch

$$yx = xy = 1.$$

Also ist y ein Inverses von x in der Gruppe $k^\times$.

Aus der Gruppentheorie wissen wir: Inversen in Gruppen sind eindeutig.

Deshalb ist auch das multiplikative Inverse von x eindeutig.

Wir schreiben

$$x^{-1}$$

für dieses eindeutige Element.

Es gilt also

$$xx^{-1} = 1 = x^{-1}x.$$

Bemerkung 2.3.8 (Minuszeichen und Inversenzeichen)**.** Das Zeichen $-x$ bezeichnet das additive Inverse von x.

Es ist für jedes $x \in k$ definiert, denn $(k, +, 0)$ ist eine abelsche Gruppe.

Das Zeichen x^{-1} bezeichnet dagegen das multiplikative Inverse von x.

Es ist in einem Körper genau dann definiert, wenn $x \neq 0$ gilt.
Insbesondere ist

$$0^{-1}$$

nicht definiert.
Man darf also nicht durch 0 teilen.

Lemma 2.3.9 (Nullproduktregel in Körpern)**.** *Sei k ein Körper und seien $x, y \in k$.*
Dann gilt

$$xy = 0 \quad \Longleftrightarrow \quad x = 0 \text{ oder } y = 0.$$

Beweis. Wir zeigen zuerst die Implikation von rechts nach links. Wenn $x = 0$ gilt, dann ist

$$xy = 0y = 0.$$

Wenn $y = 0$ gilt, dann ist

$$xy = x0 = 0.$$

Dabei benutzen wir die Rechenregel $0z = 0 = z0$ aus dem Abschnitt über Ringe (Lemma 2.2.11).
Nun zeigen wir die Richtung von links nach rechts. Sei also

$$xy = 0.$$

Wir müssen zeigen, dass $x = 0$ oder $y = 0$ gilt. Angenommen, es gilt $x \neq 0$. Dann besitzt x ein multiplikatives Inverses x^{-1}. Wir multiplizieren die Gleichung $xy = 0$ von links mit x^{-1} und erhalten

$$x^{-1}(xy) = x^{-1}0.$$

Die rechte Seite ist gleich 0. Auf der linken Seite benutzen wir die Assoziativität der Multiplikation:

$$x^{-1}(xy) = (x^{-1}x)y = 1y = y.$$

Also folgt

$$y = 0.$$

Damit haben wir gezeigt: Wenn $xy = 0$ gilt und $x \neq 0$ ist, dann muss $y = 0$ gelten.
Wir haben beide Richtungen der Äquivalenz bewiesen. □

Bemerkung 2.3.10 (Warum Linearfaktoren Nullstellen finden)**.** Die Nullproduktregel ist eine der wichtigsten Rechenregeln in Körpern. Sie erklärt, warum das Zerlegen eines Polynoms in Faktoren so nützlich ist.
Nehmen wir zum Beispiel an, ein Polynom $p(X)$ über einem Körper k habe die Form

$$p(X) = (X - a_1)(X - a_2) \cdots (X - a_n)$$

mit $a_1, \ldots, a_n \in k$. Dann ist für $x \in k$

$$p(x) = 0$$

genau dann, wenn

$$(x - a_1)(x - a_2) \cdots (x - a_n) = 0.$$

Wegen der Nullproduktregel kann ein Produkt in einem Körper nur dann 0 sein, wenn mindestens ein Faktor 0 ist. Also gilt

$$p(x) = 0$$

genau dann, wenn es ein $i \in \{1, \dots, n\}$ gibt mit

$$x - a_i = 0.$$

Das ist genau dann der Fall, wenn

$$x = a_i$$

für ein $i \in \{1, \dots, n\}$ gilt.

Die Zerlegung in Linearfaktoren liefert also nicht nur einige Nullstellen. Wenn ein Polynom vollständig in Linearfaktoren zerlegt ist, liefert diese Zerlegung alle Nullstellen.

Kapitel 3

Vektorräume

3.1 Definition

Bemerkung 3.1.1 (Warum Vektorräume?)**.** Die Vektorrechnung entsteht zunächst aus sehr anschaulichen geometrischen Situationen. Man möchte Verschiebungen, Geschwindigkeiten, Kräfte oder Richtungen addieren können. Man möchte sie auch verlängern, verkürzen oder umdrehen können. Der abstrakte Vektorraumbegriff geht aber weit über diese geometrische Anschauung hinaus. Eine wichtige historische Figur auf diesem Weg ist Hermann Graßmann. In seiner *Ausdehnungslehre* entwickelte er im 19. Jahrhundert eine sehr allgemeine und koordinatenarme Sprache für lineare Größen. Darin treten bereits viele Grundbegriffe der linearen Algebra auf: Erzeuger, lineare Kombinationen, lineare Unabhängigkeit, Basis und Dimension. Der moderne axiomatische Begriff eines Vektorraums wurde erst später vollständig herausgearbeitet. Trotzdem ist Graßmanns Idee für uns zentral: Man soll nicht nur im $\mathbb{R}^2$ oder im $\mathbb{R}^3$ rechnen. Man soll die gemeinsamen Rechenregeln erkennen, die hinter vielen verschiedenen Beispielen stehen. Genau deshalb wählen wir eine abstrakte Definition. Sie ist am Anfang etwas ungewohnt. Dafür gilt danach alles, was wir beweisen, gleichzeitig für geometrische Vektoren, Zahlenräume, Matrizenräume, Funktionenräume, Lösungsräume linearer Gleichungssysteme und viele weitere Beispiele.

Definition 3.1.2 (Vektorraum)**.** Sei k ein Körper. Ein *k-Vektorraum* ist ein Tupel

$$(V, +, 0, \cdot),$$

bestehend aus einer Menge V, einer Vektoraddition

$$+ : V \times V \to V,$$

einem Element $0 \in V$, das wir den *Nullvektor* nennen, und einer Skalarmultiplikation

$$\cdot : k \times V \to V, \quad (\lambda, v) \mapsto \lambda v,$$

sodass die folgenden Eigenschaften gelten.

(V1) **Additive Struktur.** Das Tripel $(V, +, 0)$ ist eine abelsche Gruppe. *Das bedeutet: Für alle $u, v, w \in V$ gilt*

$$u + (v + w) = (u + v) + w,$$

für alle $v \in V$ gilt

$$0 + v = v \quad \textit{und} \quad v + 0 = v,$$

zu jedem $v \in V$ gibt es ein additives Inverses $-v \in V$, und für alle $v, w \in V$ gilt

$$v + w = w + v.$$

(V2) **Assoziativität der Skalarmultiplikation.** Für alle $\lambda, \mu \in k$ und alle $v \in V$ gilt

$$(\lambda\mu)v = \lambda(\mu v).$$

(V3) **Distributivität in den Vektoren.** Für alle $\lambda \in k$ und alle $v, w \in V$ gilt

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

(V4) **Distributivität in den Skalaren.** Für alle $\lambda, \mu \in k$ und alle $v \in V$ gilt

$$(\lambda + \mu)v = \lambda v + \mu v.$$

(V5) **Normierung.** Für alle $v \in V$ gilt

$$1v = v.$$

Die Elemente von V heißen *Vektoren*. Die Elemente von k heißen *Skalare*.

Bemerkung 3.1.3 (Zur Notation)**.** Wir benutzen für die Skalarmultiplikation meistens kein eigenes Symbol. Wir schreiben also

$$\lambda v$$

statt

$$\lambda \cdot v.$$

Dabei ist wichtig: Der Ausdruck λv enthält zwei verschiedene Arten von Objekten. Der Skalar λ liegt im Körper k. Der Vektor v liegt im Vektorraum V. Das Ergebnis λv ist wieder ein Vektor in V.

Beispiel 3.1.4 (Geometrische Vektoren im Anschauungsraum)**.** Der wichtigste anschauliche Ursprung des Vektorraumbegriffs sind geometrische Vektoren. Man kann sich einen geometrischen Vektor als eine Verschiebung vorstellen: Er hat eine Richtung, eine Orientierung und eine Länge. Wo genau man den Pfeil hinzeichnet, ist dabei nicht entscheidend. Zwei Pfeile beschreiben denselben Vektor, wenn sie gleich lang sind und in dieselbe Richtung zeigen. Die Addition von geometrischen Vektoren wird durch die Parallelogrammregel beschrieben. Sind v und w zwei Vektoren, dann zeichnet man beide Pfeile mit gemeinsamem Anfangspunkt. Dann spannt man ein Parallelogramm auf. Die Diagonale dieses Parallelogramms ist der Vektor

$$v + w.$$

Anschaulich heißt das: Erst um v verschieben und danach um w verschieben hat denselben Gesamteffekt wie die Verschiebung um $v + w$. Die Skalarmultiplikation ist hier wortwörtlich eine Skalierung. Für $\lambda \in \mathbb{R}$ und einen geometrischen Vektor v ist λv der Vektor, der aus v entsteht, indem man seine Länge mit dem Faktor $|\lambda|$ skaliert. Ist $\lambda > 0$, bleibt die Orientierung gleich. Ist $\lambda < 0$, wird zusätzlich die Richtung umgedreht. Ist $\lambda = 0$, erhält man den Nullvektor. Auf dieser Anschauungsebene kann man alle Vektorraumaxiome anschaulich begründen. Die Addition ist assoziativ, denn drei nacheinander ausgeführte Verschiebungen haben denselben Gesamteffekt unabhängig davon, ob man zuerst die ersten beiden oder zuerst die letzten beiden zusammenfasst. Sie ist kommutativ, denn das Parallelogramm hat dieselbe Diagonale, egal in welcher Reihenfolge man die beiden Seiten einzeichnet. Der Nullvektor ist die Verschiebung um nichts. Das additive Inverse $-v$ ist die Verschiebung mit gleicher Länge in entgegengesetzter Richtung. Die Distributivgesetze drücken aus, dass Skalierung und Addition zusammenpassen: Wenn man die Summe zweier Verschiebungen skaliert, erhält man dasselbe wie die Summe der skalierten Verschiebungen. Und

wenn man denselben Vektor erst mit λ und mit μ skaliert und dann addiert, erhält man dasselbe wie die Skalierung mit $\lambda + \mu$.

Diese *Idee* ist so einfach, wie sie aussieht, und genau dieses Bild sollte man im Kopf behalten. Ehrlicherweise ist „anschaulich begründen“ aber noch kein Beweis — und was hier ein Beweis *ist*, hängt davon ab, was man über die Geometrie schon zu wissen glaubt. Je nach Ausgangspunkt braucht man verschiedene Argumente:

- Fasst man Verschiebungen als *Abbildungen* der Ebene auf und die Addition als Hintereinanderausführung, dann ist die Assoziativität geschenkt — Komposition von Abbildungen ist immer assoziativ. Die Kommutativität ist dann aber ein echter geometrischer Satz, und genau ihn spricht die Parallelogrammregel aus.

- Nimmt man die Schulgeometrie mit ihren Kongruenz- und Ähnlichkeitssätzen als gegeben, dann werden die Axiome zu kleinen Sätzen über Parallelogramme. Das Distributivgesetz $\lambda(v + w) = \lambda v + \lambda w$ etwa ist der Strahlensatz in Verkleidung: Die zentrische Streckung um λ bildet das Parallelogramm von v und w auf das Parallelogramm von λv und λw ab und nimmt dabei die Diagonale mit.

- Übersetzt man die Ebene zuerst in Koordinaten, dann rechnen sich alle Axiome komponentenweise nach — die geometrische Frage ist damit aber nur verschoben, nämlich dorthin, warum Koordinaten die Geometrie treu beschreiben.

Historisch ist das keine Fußnote. Graßmanns *Ausdehnungslehre* (1844) ist im Kern genau dieses Programm: den Kalkül der Größen koordinatenfrei (und in einem speziellen Sinne auch geometriefrei[1]) aufzubauen und seine Rechengesetze aus der „Erzeugung ausgedehnter Größen“ *herzuleiten*. Was wir heute als Axiome an den Anfang stellen, war dort das Resultat einer Untersuchung.

Die moderne Definition dreht den Spieß um: Sie schreibt die Gesetze als Forderungen hin und lässt offen, woher sie kommen. Jede Auffassung von Geometrie, die sie begründet, bekommt dafür alle Sätze der linearen Algebra geschenkt.

Leitbeispiel 3.1.5 (Der Signalraum)**.** Als Leitbeispiel für dieses Kapitel begleiten uns *reine Sinuswellen* und ihre Überlagerungen. Für eine feste Zahl $c > 0$ betrachten wir die Funktion

$$s_c : \mathbb{R} \to \mathbb{R}, \qquad s_c(x) = \sin(cx),$$

eine Welle, die mit der *Frequenz c* schwingt. Man darf dabei an Radiowellen denken: Jeder Sender strahlt — idealisiert — eine solche reine Welle aus, und was eine Antenne erreicht, ist die Überlagerung aller Sender. Unser Vektorraum ist der *Signalraum S*, die Menge aller endlichen Überlagerungen

$$\lambda_1 s_{c_1} + \lambda_2 s_{c_2} + \cdots + \lambda_n s_{c_n} \qquad (\lambda_i \in \mathbb{R},\ c_i > 0),$$

aufgefasst als Funktionen $\mathbb{R} \to \mathbb{R}$. Dabei dürfen die Anzahl n und die Frequenzen $c_1, \ldots, c_n$ von Signal zu Signal verschieden sein — zum Beispiel liegen $3s_1 + 2s_5$ und $s_\pi - 7s_2$ beide in S.

Wichtig ist, was hier *ein* Vektor ist: nicht ein einzelner Messwert der Welle, sondern die *ganze Funktion* — der komplette Kurvenzug ist ein einziges Element von S. Die Operationen sind dann handgreiflich:

- **Überlagern.** Zwei Wellen, die gleichzeitig durch die Luft laufen, addieren sich Punkt für Punkt zu einem neuen Signal. Das ist unsere *Addition* $u + v$.

[1] Es ging Graßmann um die Theorie der *Erzeugung* ausgedehnter Größen. Dieser Ansatz war sowohl seinen Zeitgenossen als auch uns heute recht fremd. Deshalb kam die verdiente Würdigung auch erst spät.

- **Verstärken und Abschwächen.** Dreht man die Sendeleistung um einen Faktor λ hoch oder herunter, wird die Welle um diesen Faktor gestreckt. Das ist unsere *Skalarmultiplikation* λv.

Der Nullvektor ist die *Stille*: das Signal, das überall den Wert 0 hat. Die Vektorraumaxiome muss man kaum nachrechnen, denn addiert und skaliert wird Punkt für Punkt in $\mathbb{R}$; die Axiome erben ihre Gültigkeit also direkt von den Rechenregeln der reellen Zahlen. Erfreulich ist, dass hier auch negative Vorfaktoren nichts Exotisches sind: $-s_c$ ist die auf den Kopf gestellte Sinuswelle — eine genauso echte Welle wie s_c selbst.

Idealisiert ist an dem Modell etwas anderes: Wir tun so, als bestünde jedes Signal aus endlich vielen *scharfen* Frequenzen, und wir unterschlagen, dass reale Wellen gegeneinander *verschoben* sein können. Beides ist unphysikalisch, aber es hält das Beispiel einfach; am Ende des Kapitels kommen wir darauf zurück. Der Signalraum wird uns eine praktische Frage beantworten: Was *sieht* eine Messstation, die nur auf wenige Frequenzen lauscht? Die Antwort führt geradewegs zu den Begriffen *Basis* und *Dimension*.

Beispiel 3.1.6 (Der Raum $\mathbb{R}^n$)**.** Für jedes $n \in \mathbb{N}$ ist

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

ein $\mathbb{R}$-Vektorraum. Die Addition ist komponentenweise definiert:

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

Die Skalarmultiplikation ist ebenfalls komponentenweise definiert:

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

Der Nullvektor ist

$$0 = (0, \dots, 0).$$

Für $n = 2$ und $n = 3$ kann man diese Vektorräume geometrisch zeichnen. Für größeres n ist das nicht mehr direkt möglich. Die abstrakte Definition erlaubt uns aber trotzdem, mit $\mathbb{R}^n$ genauso systematisch zu rechnen.

Beispiel 3.1.7 (Funktionenräume)**.** Sei

$$C^0(\mathbb{R})$$

die Menge aller stetigen Abbildungen

$$f : \mathbb{R} \to \mathbb{R}.$$

Diese Menge ist ein $\mathbb{R}$-Vektorraum. Die Addition ist punktweise definiert:

$$(f + g)(x) := f(x) + g(x).$$

Die Skalarmultiplikation ist ebenfalls punktweise definiert:

$$(\lambda f)(x) := \lambda f(x).$$

Der Nullvektor ist hier nicht eine Zahl und auch kein Pfeil. Der Nullvektor ist die Nullfunktion

$$0 : \mathbb{R} \to \mathbb{R}, \quad x \mapsto 0.$$

Das ist ein wichtiger Moment: In einem abstrakten Vektorraum müssen die Vektoren nicht wie Pfeile aussehen. Sie können auch Funktionen oder noch abstraktere Objekte sein.

Beispiel 3.1.8 (Folgen)**.** Die Menge aller reellen Folgen

$$(a_n)_{n\in\mathbb{N}}$$

ist ein $\mathbb{R}$-Vektorraum. Addition und Skalarmultiplikation werden gliedweise definiert:

$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} := (a_n + b_n)_{n\in\mathbb{N}}$$

und

$$\lambda(a_n)_{n\in\mathbb{N}} := (\lambda a_n)_{n\in\mathbb{N}}.$$

Auch die Menge aller konvergenten reellen Folgen ist ein $\mathbb{R}$-Vektorraum. Der Grund ist: Summen konvergenter Folgen sind wieder konvergent. Skalare Vielfache konvergenter Folgen sind wieder konvergent. Diese Aussage beruht auf den Grenzwertsätzen aus der Analysis.

Beispiel 3.1.9 ($\mathbb{C}$ als reeller Vektorraum)**.** Die komplexen Zahlen bilden einen $\mathbb{R}$-Vektorraum. Die Vektoraddition ist die gewöhnliche Addition komplexer Zahlen. Die Skalarmultiplikation ist die Multiplikation einer komplexen Zahl mit einer reellen Zahl. Schreibt man eine komplexe Zahl als

$$z = a + bi,$$

dann gilt für $\lambda \in \mathbb{R}$

$$\lambda z = \lambda(a + bi) = \lambda a + (\lambda b)i.$$

Als $\mathbb{R}$-Vektorraum verhält sich $\mathbb{C}$ also wie $\mathbb{R}^2$. Die reelle und die imaginäre Richtung sind die beiden grundlegenden Richtungen.

Beispiel 3.1.10 (Polynome)**.** Die Menge aller Polynome mit reellen Koeffizienten ist ein $\mathbb{R}$-Vektorraum. Die Addition ist die gewöhnliche Addition von Polynomen. Die Skalarmultiplikation ist die Multiplikation aller Koeffizienten mit derselben reellen Zahl. Auch die Menge aller Polynome vom Grad höchstens n ist ein $\mathbb{R}$-Vektorraum. Man muss hier nur beachten: Wenn zwei Polynome jeweils Grad höchstens n haben, dann hat auch ihre Summe Grad höchstens n. Und wenn man ein Polynom vom Grad höchstens n mit einem Skalar multipliziert, dann hat das Ergebnis wieder Grad höchstens n.

Bemerkung 3.1.11 (Warum andere Körper interessant sind)**.** Bisher haben wir vor allem $\mathbb{R}$-Vektorräume betrachtet. Das ist für Geometrie, Analysis und viele Anwendungen in der Physik sehr natürlich. Die abstrakte Definition erlaubt aber auch Vektorräume über anderen Körpern. Das ist nicht nur eine technische Spielerei. Der Körper bestimmt, welche Skalare erlaubt sind. Dadurch ändert sich auch, welche Linearkombinationen möglich sind und welche lineare Struktur ein Raum hat.

Beispiel 3.1.12 (Vektorräume über beliebigen Körpern)**.** Sei k ein beliebiger Körper. Dann ist

$$k^n$$

ein k-Vektorraum. Die Addition und Skalarmultiplikation sind wieder komponentenweise definiert.

Beispiel 3.1.13 (Komplexe Funktionen als komplexer Vektorraum)**.** Die Menge aller analytischen Funktionen

$$f : \mathbb{C} \to \mathbb{C}$$

bildet einen $\mathbb{C}$-Vektorraum. Addiert man zwei analytische Funktionen, so erhält man wieder eine analytische Funktion. Multipliziert man eine analytische Funktion mit einem komplexen Skalar, so erhält man wieder eine analytische Funktion. Hier sind also nicht nur die Vektoren komplexwertige Funktionen. Auch die Skalare kommen aus $\mathbb{C}$.

Solche Räume spielen in der Quantenmechanik eine wichtige Rolle.

Beispiel 3.1.14 (Bytes als Vektoren über $\mathbb{F}_2$)**.** Der Körper

$$\mathbb{F}_2 = \{0, 1\}$$

hat nur zwei Elemente. In ihm gilt

$$1 + 1 = 0.$$

Ein Byte in einem Computer ist eine Folge von acht Bits:

$$(b_1, \dots, b_8) \in \mathbb{F}_2^8.$$

Damit ist die Menge aller Bytes ein $\mathbb{F}_2$-Vektorraum. Die Addition ist komponentenweise Addition modulo 2. In der Informatik entspricht das der Operation XOR. Zum Beispiel gilt

$$(1, 0, 1, 1) + (0, 1, 1, 0) = (1, 1, 0, 1).$$

Die Skalarmultiplikation ist besonders einfach:

$$1v = v \quad \text{und} \quad 0v = 0.$$

Beispiel 3.1.15 (Potenzmengen als Vektorräume über $\mathbb{F}_2$)**.** Sei M eine Menge. Dann kann man die Potenzmenge

$$\mathfrak{P}(M)$$

als $\mathbb{F}_2$-Vektorraum auffassen. Die Addition ist die symmetrische Differenz:

$$A \triangle B := (A \cup B) \setminus (A \cap B).$$

Das sind genau die Elemente, die in genau einer der beiden Mengen A und B liegen. Der Nullvektor ist die leere Menge:

$$0 = \emptyset.$$

Außerdem gilt für jede Teilmenge $A \subseteq M$

$$A \triangle A = \emptyset.$$

Das bedeutet: Jeder Vektor ist sein eigenes additives Inverses. Die Skalarmultiplikation ist gegeben durch

$$1A = A \quad \text{und} \quad 0A = \emptyset.$$

Dieses Beispiel zeigt besonders deutlich, dass Vektoren nicht unbedingt Pfeile oder Zahlentupel sein müssen. Sie können sogar Mengen sein.

Beispiel 3.1.16 ($\mathbb{R}$ als $\mathbb{Q}$-Vektorraum)**.** Die reellen Zahlen bilden nicht nur einen $\mathbb{R}$-Vektorraum. Sie bilden auch einen $\mathbb{Q}$-Vektorraum. Als Menge betrachten wir weiterhin $\mathbb{R}$. Die Vektoraddition ist die gewöhnliche Addition reeller Zahlen. Die Skalare sind jetzt aber nur rationale Zahlen. Die Skalarmultiplikation ist also

$$\mathbb{Q} \times \mathbb{R} \to \mathbb{R}, \quad (q, x) \mapsto qx.$$

Dieses Beispiel zeigt: Dieselbe Menge kann über verschiedenen Körpern als Vektorraum betrachtet werden. Der gewählte Körper gehört zur Struktur dazu. Man sollte also nicht nur sagen: „V ist ein Vektorraum." Genauer ist: „V ist ein Vektorraum über dem Körper k."

Bemerkung 3.1.17 (Ein letzter Perspektivwechsel)**.** Die Vorstellung, dass Vektoren Pfeile sind, ist manchmal sehr hilfreich. Sie erklärt gut, warum man addiert und skaliert. Aber sie ist nicht die Definition. Die Definition sagt: Vektoren sind Elemente einer Menge, auf der Addition und Skalarmultiplikation so funktionieren, wie es die Axiome verlangen. Das ist die Stärke des abstrakten Begriffs. Er löst die lineare Struktur aus einem einzelnen Bild heraus und macht sie in vielen verschiedenen Situationen wiedererkennbar.

3.2 Darstellungen von Vektoren

3.2.1 Lineare Unabhängigkeit

Bemerkung 3.2.1 (Zwei scheinbar verschiedene Beobachtungen)**.** Wir beginnen mit zwei Aussagen, die auf den ersten Blick ganz verschieden wirken.

1. Um zwei Unbekannte eindeutig zu bestimmen, braucht man zwei lineare Gleichungen.
2. Mit zwei Richtungen kommt man überall in der Ebene hin.

Beide Aussagen sind in dieser Form zu grob und damit falsch. Es kommt nicht nur darauf an, wie viele Gleichungen oder wie viele Richtungen wir haben. Es kommt darauf an, ob diese Gleichungen oder Richtungen wirklich neue Information enthalten.

Trotzdem vermitteln diese Aussagen aber eine richtige Intuition. Um den wahren Kern herauszuarbeiten müssen wir verstehen, was die Aussagen genau sagen wollen. Gemeint ist natürlich „zwei *verschiedene* lineare Gleichungen“ und „zwei *verschiedene* Richtungen“. Aber was genau heißt „verschieden“ hier? Diese Frage werden wir nun untersuchen! Und dann werden wir die korrigierten Versionen der obigen Aussagen beweisen.

Beispiel 3.2.2 (Zwei Gleichungen, aber unendlich viele Lösungen)**.** Wir betrachten das lineare Gleichungssystem

$$\begin{aligned} x + y &= 0, \\ 2x + 2y &= 0. \end{aligned}$$

Die zweite Gleichung ist genau das Doppelte der ersten Gleichung. Also liefert sie keine neue Bedingung. Wir rechnen die Lösungsmenge aus. Aus

$$x + y = 0$$

folgt

$$x = -y.$$

Setzen wir $y = t$ mit $t \in \mathbb{R}$, dann ist

$$x = -t.$$

Jede Lösung hat also die Form

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -t \\ t \end{pmatrix} \quad \text{mit} \quad t \in \mathbb{R}.$$

Wir prüfen die zweite Gleichung:

$$2x + 2y = 2(-t) + 2t = 0.$$

Also ist die Lösungsmenge

$$\left\{ \begin{pmatrix} -t \\ t \end{pmatrix} \mid t \in \mathbb{R} \right\}.$$

Das sind unendlich viele Lösungen. Zwei Gleichungen reichen hier also nicht aus, um zwei Unbekannte eindeutig zu bestimmen.

Beispiel 3.2.3 (Zwei Gleichungen, aber keine Lösung)**.** Wir betrachten nun das lineare Gleichungssystem

$$x + y = 0,$$
$$2x + 2y = 1.$$

Wenn die erste Gleichung gilt, dann folgt durch Multiplikation mit 2

$$2x + 2y = 0.$$

Die zweite Gleichung verlangt aber

$$2x + 2y = 1.$$

Das ist ein Widerspruch. Also hat das Gleichungssystem keine Lösung.

Auch hier sehen wir: Es genügt nicht, nur die Anzahl der Gleichungen zu zählen. Wir müssen verstehen, wie die Gleichungen voneinander abhängen.

Bemerkung 3.2.4 (Die entsprechende Frage für Richtungen)**.** Nun betrachten wir Vektoren in der Ebene. Die Frage

„Kommt man mit diesen Richtungen überall hin?“

bedeutet: Kann man jeden Vektor der Ebene als Kombination dieser gegebenen Vektoren schreiben?

Also: Wenn $v, w \in \mathbb{R}^2$ gegeben sind, betrachten wir alle Vektoren der Form

$$\lambda v + \mu w$$

mit $\lambda, \mu \in \mathbb{R}$.

Diese Menge werden wir später allgemeiner studieren und nennen sie den *Spann* oder die *lineare Hülle* von v und w.

Beispiel 3.2.5 (Zwei Vektoren, aber nicht die ganze Ebene)**.** Wir betrachten die Vektoren

$$\begin{pmatrix}1\\2\end{pmatrix} \quad \text{und} \quad \begin{pmatrix}2\\4\end{pmatrix}$$

aus dem $\mathbb{R}^2$. Der zweite Vektor ist das Doppelte des ersten:

$$\begin{pmatrix}2\\4\end{pmatrix} = 2\begin{pmatrix}1\\2\end{pmatrix}.$$

Die Elemente des Spann dieser Vektoren haben die Form

$$\lambda\begin{pmatrix}1\\2\end{pmatrix} + \mu\begin{pmatrix}2\\4\end{pmatrix}$$

mit $\lambda, \mu \in \mathbb{R}$. Wir rechnen:

$$\lambda\begin{pmatrix}1\\2\end{pmatrix} + \mu\begin{pmatrix}2\\4\end{pmatrix} = \begin{pmatrix}\lambda\\2\lambda\end{pmatrix} + \begin{pmatrix}2\mu\\4\mu\end{pmatrix} = \begin{pmatrix}\lambda + 2\mu\\2\lambda + 4\mu\end{pmatrix}.$$

Setzen wir

$$s := \lambda + 2\mu,$$

dann ist

$$2\lambda + 4\mu = 2s.$$

Also haben die Elemente des Spann die Form

$$\begin{pmatrix} s \\ 2s \end{pmatrix} \quad \text{mit} \quad s \in \mathbb{R}.$$

Das ist nur eine Gerade durch den Ursprung. Zum Beispiel liegt

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

nicht in dieser Menge, denn aus

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} s \\ 2s \end{pmatrix}$$

würde zuerst $s = 0$ folgen, aber dann wäre $2s = 0$ und nicht 1. Also spannen die Vektoren $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ und $\begin{pmatrix} 2 \\ 4 \end{pmatrix}$ nicht die ganze Ebene auf.

Beispiel 3.2.6 (Zwei Vektoren, die die ganze Ebene aufspannen)**.** Wir betrachten nun die Vektoren

$$\begin{pmatrix} 1 \\ 2 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Wir zeigen: Jeder Vektor

$$\begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{R}^2$$

liegt im Spann von $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ und $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

Wir suchen also $\lambda, \mu \in \mathbb{R}$ mit

$$\lambda \begin{pmatrix} 1 \\ 2 \end{pmatrix} + \mu \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}.$$

Die linke Seite ist

$$\lambda \begin{pmatrix} 1 \\ 2 \end{pmatrix} + \mu \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} \lambda + \mu \\ 2\lambda + \mu \end{pmatrix}.$$

Wir müssen also lösen:

$$\lambda + \mu = a,$$
$$2\lambda + \mu = b.$$

Subtrahieren wir die erste Gleichung von der zweiten, so erhalten wir

$$\lambda = b - a.$$

Daraus folgt

$$\mu = a - \lambda = a - (b - a) = 2a - b.$$

Wir prüfen nach:

$$(b - a) \begin{pmatrix} 1 \\ 2 \end{pmatrix} + (2a - b) \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} b - a \\ 2b - 2a \end{pmatrix} + \begin{pmatrix} 2a - b \\ 2a - b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}.$$

Also spannen die Vektoren $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ und $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ die ganze Ebene auf.

Bemerkung 3.2.7 (Eine erste Hypothese)**.** Die bisherigen Beispiele legen eine erste Hypothese nahe:

Eine Gleichung oder ein Vektor darf nicht einfach ein Vielfaches eines anderen sein.

Diese Hypothese ist richtig, aber noch nicht stark genug. In höheren Dimensionen gibt es aber subtilere Formen von Abhängigkeit.

Beispiel 3.2.8 (Drei Vektoren in $\mathbb{R}^3$, aber nicht der ganze Raum)**.** Wir betrachten die drei Vektoren

$$(1,0,0), \quad (0,1,0), \quad (1,1,0)$$

in $\mathbb{R}^3$. Keiner dieser drei Vektoren ist ein Vielfaches eines anderen. Trotzdem spannen sie nicht den ganzen $\mathbb{R}^3$ auf.

Egal wie wir die drei Vektoren kombinieren: Die dritte Komponente ist immer 0.

Also kann zum Beispiel der Vektor

$$(0,0,1)$$

nicht im Spann dieser drei Vektoren liegen. Die drei Vektoren spannen also nur die Ebene

$$\{(x,y,0) \mid x,y \in \mathbb{R}\}$$

auf.

Der Grund ist: Der dritte Vektor enthält keine neue Richtung. Es gilt

$$(1,1,0) = (1,0,0) + (0,1,0).$$

Also ist der dritte Vektor kein Vielfaches eines einzelnen vorherigen Vektors, aber er ist eine Linearkombination der beiden anderen.

Beispiel 3.2.9 (Drei Gleichungen, aber keine eindeutige Lösung)**.** Die gleiche Erscheinung gibt es bei linearen Gleichungssystemen. Wir betrachten das System

$$\begin{aligned} x &= 0, \\ y &= 0, \\ x + y &= 0. \end{aligned}$$

Das sind drei Gleichungen in drei Unbekannten x, y, z. Keine dieser Gleichungen ist ein Vielfaches einer anderen. Trotzdem gibt es keine eindeutige Lösung:

Aus den ersten beiden Gleichungen folgt

$$x = 0 \quad \text{und} \quad y = 0.$$

Dann ist auch die dritte Gleichung erfüllt, denn

$$x + y = 0 + 0 = 0.$$

Über z wird gar nichts gesagt. Also ist

$$(x,y,z) = (0,0,t)$$

für jedes $t \in \mathbb{R}$ eine Lösung.

Die Lösungsmenge ist

$$\{(0,0,t) \mid t \in \mathbb{R}\}.$$

Das sind unendlich viele Lösungen.

Die dritte Gleichung war also nicht nutzlos, weil sie ein Vielfaches einer anderen Gleichung war. Sie war nutzlos, weil sie aus den beiden ersten Gleichungen zusammengesetzt werden konnte.

Bemerkung 3.2.10 (Der gemeinsame Begriff)**.** Wir haben jetzt zwei scheinbar verschiedene Probleme gesehen.

1. Bei Gleichungssystemen fragen wir: Welche Gleichungen enthalten wirklich neue Information?

2. Bei Vektoren fragen wir: Welche Vektoren liefern wirklich neue Richtungen?

Der abstrakte Vektorraumbegriff erlaubt uns, beide Fragen mit derselben Sprache zu behandeln.
Denn sowohl Koeffizienten von Gleichungen als auch geometrische Richtungen können als Vektoren in geeigneten Vektorräumen betrachtet werden.
Der Begriff, den wir suchen, ist der Begriff der *linearen Unabhängigkeit*.

Wir haben oben bereits das folgende Konzept benutzt, nun formalisieren wir es:

Definition 3.2.11 (Linearkombination)**.** Sei V ein k-Vektorraum und seien

$$v_1, \dots, v_n \in V.$$

Ein Vektor $v \in V$ heißt eine *Linearkombination* von $v_1, \dots, v_n$, wenn es Skalare

$$\lambda_1, \dots, \lambda_n \in k$$

gibt mit

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n.$$

Definition 3.2.12 (Lineare Abhängigkeit und lineare Unabhängigkeit)**.** Sei V ein k-Vektorraum und seien

$$v_1, \dots, v_n \in V.$$

Das System $v_1, \dots, v_n$ heißt *linear abhängig*, wenn es

$$\lambda_1, \dots, \lambda_n \in k,$$

gibt, die nicht alle gleich 0 sind, sodass

$$\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$$

gilt. In Kurzform sagt man: Das System $v_1, \dots, v_n$ heißt *linear abhängig*, wenn der Nullvektor eine nichttriviale Darstellung als Linearkombination von $v_1, \dots, v_n$ besitzt.
Das System $v_1, \dots, v_n$ heißt *linear unabhängig*, wenn es nicht linear abhängig ist.
Das heißt: Gilt

$$\lambda_1 v_1 + \cdots + \lambda_n v_n = 0,$$

dann folgt bereits

$$\lambda_1 = \cdots = \lambda_n = 0.$$

Diese Definition ist kurz und unscheinbar. Dennoch gehört sie zu den wichtigsten Definitionen in der Linearen Algebra!

Leitbeispiel 3.2.13 (Der Signalraum: ein überflüssiger Sender)**.** Was bedeutet lineare Abhängigkeit im Signalraum Leitbeispiel 3.1.5? Wir denken an mehrere Sender und fragen: Ist einer davon überflüssig?

Zwei Sender strahlen die reinen Wellen s_{c_1} und s_{c_2} zweier verschiedener Frequenzen aus. Ein dritter Sender strahlt den „Akkord“ aus beiden aus:

$$a = s_{c_1} + s_{c_2}, \qquad \text{also} \qquad s_{c_1} + s_{c_2} - a = 0.$$

Das ist eine nichttriviale Darstellung der Stille, denn die Koeffizienten $(1, 1, -1)$ sind nicht alle null. Das System s_{c_1}, s_{c_2}, a ist also *linear abhängig*. Anschaulich: Alles, was der dritte Sender in die Luft bringt, können die ersten beiden zusammen schon — er ist überflüssig.

Reine Sinuswellen *verschiedener* Frequenzen sind dagegen *linear unabhängig*: Aus

$$\lambda_1 s_{c_1} + \cdots + \lambda_n s_{c_n} = 0 \qquad (c_1, \ldots, c_n \text{ paarweise verschieden})$$

folgt bereits $\lambda_1 = \cdots = \lambda_n = 0$. Keine reine Welle lässt sich also aus anderen Frequenzen zusammensetzen. Anschaulich ist das plausibel, denn die Summanden schwingen alle verschieden schnell; ein Beweis braucht allerdings Werkzeuge der Analysis, und wir nehmen die Aussage hier als Tatsache. Auf ihr ruht das ganze Leitbeispiel: Sie garantiert, dass in einer Überlagerung *eindeutig* feststeht, mit welcher Stärke jede Frequenz vertreten ist. (Bei Zahlentupeln konnten wir für solche Fragen einfach Komponenten vergleichen. Eine Funktion hat keine Komponenten — noch nicht. Genau das werden Basen ändern.)

Beispiel 3.2.14. Die Vektoren

$$(1, 0, 0), \quad (0, 1, 0), \quad (1, 1, 0)$$

sind linear abhängig.

Denn es gilt

$$(1, 0, 0) + (0, 1, 0) - (1, 1, 0) = (0, 0, 0).$$

Also haben wir eine Darstellung des Nullvektors gefunden, bei der nicht alle Koeffizienten gleich 0 sind:

$$1(1, 0, 0) + 1(0, 1, 0) + (-1)(1, 1, 0) = 0.$$

Bemerkung 3.2.15 (Lineare Unabhängigkeit ist eine Eigenschaft eines Systems)**.** Lineare Unabhängigkeit ist eine Eigenschaft eines ganzen Systems von Vektoren. Das ist wichtig.

Wenn man sagt, ein Vektor v sei linear unabhängig, meint man eigentlich: Das einelementige System

$$v$$

ist linear unabhängig. Dies ist genau dann der Fall, wenn

$$v \neq 0$$

gilt.

Noch wichtiger ist aber: Lineare Unabhängigkeit ist auch keine paarweise Eigenschaft. Es kann passieren, dass je zwei Vektoren eines Systems linear unabhängig sind, aber das ganze System trotzdem linear abhängig ist. Man darf lineare Unabhängigkeit also nicht dadurch prüfen, dass man nur alle Paare anschaut.

Beispiel 3.2.16 (Paarweise unabhängig, aber zusammen abhängig)**.** Sei k ein Körper. Wir betrachten in k^3 die sieben Vektoren

$$(1,0,0), \quad (0,1,0), \quad (0,0,1),$$

$$(1,1,0), \quad (1,0,1), \quad (0,1,1), \quad (1,1,1).$$

Das sind genau die Vektoren in k^3, deren Einträge nur 0 oder 1 sind, außer dem Nullvektor. Je zwei verschiedene Vektoren aus diesem System sind linear unabhängig.

Wir begründen das. Seien v und w zwei verschiedene Vektoren aus dieser Liste. Wir nehmen an, dass

$$\lambda v + \mu w = 0$$

gilt. Da v und w verschieden sind, gibt es eine Koordinate, in der einer der beiden Vektoren den Eintrag 1 und der andere den Eintrag 0 hat.

Angenommen, an dieser Stelle hat v den Eintrag 1 und w den Eintrag 0. Dann liefert der Vergleich dieser Koordinate

$$\lambda = 0.$$

Da $w \neq 0$ gilt, besitzt w irgendwo einen Eintrag 1.

Vergleichen wir diese Koordinate in der Gleichung

$$\lambda v + \mu w = 0,$$

und benutzen $\lambda = 0$, so folgt

$$\mu = 0.$$

Im anderen Fall, also wenn v an der unterscheidenden Stelle den Eintrag 0 und w den Eintrag 1 hat, argumentiert man genauso und erhält zuerst $\mu = 0$ und dann $\lambda = 0$.

Also sind je zwei verschiedene Vektoren aus unserer Liste linear unabhängig. Das ganze System aus sieben Vektoren ist aber linear abhängig. Denn es gilt zum Beispiel

$$(1,0,0) + (0,1,0) - (1,1,0) = (0,0,0).$$

Das ist eine nichttriviale Darstellung des Nullvektors. Also ist das System

$$(1,0,0), (0,1,0), (0,0,1), (1,1,0), (1,0,1), (0,1,1), (1,1,1)$$

linear abhängig, obwohl je zwei verschiedene Vektoren daraus linear unabhängig sind.

Bemerkung 3.2.17 (Warum diese Warnung wichtig ist)**.** Lineare Unabhängigkeit fragt nicht:

„Sind je zwei Vektoren unabhängig?“

Lineare Unabhängigkeit fragt:

„Gibt es irgendeine nichttriviale Linearkombination des ganzen Systems, die 0 ergibt?“

Eine Abhängigkeit kann also erst sichtbar werden, wenn mehrere Vektoren zusammenwirken.

Im Beispiel oben ist keiner der drei Vektoren

$$(1,0,0), \quad (0,1,0), \quad (1,1,0)$$

ein Vielfaches eines anderen.

Trotzdem gilt

$$(1,1,0) = (1,0,0) + (0,1,0).$$

Der dritte Vektor bringt also keine neue Richtung hinzu.

Beim Arbeiten mit linearer Unabhängigkeit muss man deshalb immer genau sagen, welches System gerade betrachtet wird.

Wenn man einen Vektor hinzufügt oder weglässt, spricht man über ein anderes System. Dadurch kann sich die Eigenschaft ändern.

Lemma 3.2.18 (Lineare Abhängigkeit und Mehrdeutigkeit von Darstellungen)**.** *Sei V ein k-Vektorraum und seien*

$$v_1, \dots, v_n \in V.$$

Dann sind die folgenden Aussagen äquivalent.

1. *Das System $v_1, \dots, v_n$ ist linear abhängig.*
2. *Es gibt einen Vektor $v \in V$, der zwei verschiedene Darstellungen als Linearkombination von $v_1, \dots, v_n$ besitzt.*

Beweis. Wir zeigen zuerst: Lineare Abhängigkeit impliziert Mehrdeutigkeit von Darstellungen.

Angenommen, $v_1, \dots, v_n$ ist linear abhängig.

Dann gibt es Skalare

$$\lambda_1, \dots, \lambda_n \in k,$$

die nicht alle gleich 0 sind, sodass

$$\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$$

gilt.

Andererseits gilt natürlich auch

$$0v_1 + \cdots + 0v_n = 0.$$

Da nicht alle λ_i gleich 0 sind, sind diese beiden Darstellungen des Nullvektors verschieden.

Also besitzt mindestens ein Vektor, nämlich der Nullvektor, zwei verschiedene Darstellungen.

Nun zeigen wir die Umkehrung.

Angenommen, es gibt einen Vektor $v \in V$ mit zwei verschiedenen Darstellungen als Linearkombination von $v_1, \dots, v_n$.

Dann gibt es Skalare

$$\lambda_1, \dots, \lambda_n, \mu_1, \dots, \mu_n \in k$$

mit

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n$$

und

$$v = \mu_1 v_1 + \cdots + \mu_n v_n,$$

wobei mindestens ein Koeffizient verschieden ist.

Durch Subtraktion erhalten wir

$$0 = v - v = (\lambda_1 - \mu_1)v_1 + \cdots + (\lambda_n - \mu_n)v_n.$$

Da die beiden Darstellungen verschieden sind, gibt es ein i mit

$$\lambda_i - \mu_i \neq 0.$$

Also ist dies eine nichttriviale Darstellung des Nullvektors.

Damit ist $v_1, \dots, v_n$ linear abhängig. □

3.2.2 Lineare Hülle

Definition 3.2.19 (Erzeugnis, Spann, lineare Hülle)**.** Sei V ein k-Vektorraum und seien

$$v_1, \dots, v_n \in V.$$

Das *Erzeugnis*, der *Spann* oder die *lineare Hülle* von $v_1, \dots, v_n$ ist die Menge aller Linearkombinationen dieser Vektoren.

Wir schreiben

$$\mathrm{Span}(v_1, \dots, v_n) := \mathrm{Span}(\{v_1, \dots, v_n\}) := \{\lambda_1 v_1 + \cdots + \lambda_n v_n \mid \lambda_1, \dots, \lambda_n \in k\}.$$

Wenn

$$\mathrm{Span}(v_1, \dots, v_n) = V$$

gilt, dann sagen wir: Die Vektoren $v_1, \dots, v_n$ *erzeugen* den Vektorraum V.

In diesem Fall heißt $v_1, \dots, v_n$ ein *Erzeugendensystem* von V.

Beispiel 3.2.20. Im Beispiel mit

$$\begin{pmatrix}1\\2\end{pmatrix} \quad \text{und} \quad \begin{pmatrix}2\\4\end{pmatrix}$$

gilt

$$\mathrm{Span}(\begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}2\\4\end{pmatrix}) = \{\begin{pmatrix}s\\2s\end{pmatrix} \mid s \in \mathbb{R}\}.$$

Also ist

$$\mathrm{Span}(\begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}2\\4\end{pmatrix}) \neq \mathbb{R}^2.$$

Im Beispiel mit

$$\begin{pmatrix}1\\2\end{pmatrix} \quad \text{und} \quad \begin{pmatrix}1\\1\end{pmatrix}$$

haben wir dagegen gezeigt:

$$\mathrm{Span}(\begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}) = \mathbb{R}^2.$$

Leitbeispiel 3.2.21 (Der Signalraum: welche Signale kann man senden?)**.** Der Spann einer Menge von Sendern hat im Signalraum Leitbeispiel 3.1.5 eine unmittelbare Bedeutung: Es ist die Menge *aller Signale, die sie gemeinsam erzeugen können*, also aller Überlagerungen $\lambda_1 v_1 + \cdots + \lambda_n v_n$.

Zwei Sender mit den Frequenzen c_1 und c_2 erreichen jede Mischung ihrer beiden Töne, aber niemals eine dritte Frequenz c_3:

$$s_{c_3} \notin \mathrm{Span}(s_{c_1}, s_{c_2}),$$

denn sonst wären $s_{c_1}, s_{c_2}, s_{c_3}$ linear abhängig — im Widerspruch zur Unabhängigkeit reiner Wellen verschiedener Frequenzen, die wir in Leitbeispiel 3.2.13 als Tatsache festgehalten haben. Insbesondere ist $\mathrm{Span}(s_{c_1}, s_{c_2}) \subsetneq S$; zwei Sender sind *kein Erzeugendensystem* des Signalraums. Tatsächlich reichen endlich viele Sender *niemals* für ganz S: Endlich viele Sender bringen zusammen nur endlich viele Frequenzen ins Spiel, und schon die reine Welle einer einzigen weiteren Frequenz liegt außerhalb ihres Spanns.

Der überflüssige Akkord-Sender von vorhin fügt dem Spann dagegen nichts hinzu:

$$\mathrm{Span}(s_{c_1}, s_{c_2}, a) = \mathrm{Span}(s_{c_1}, s_{c_2}),$$

denn $a = s_{c_1} + s_{c_2}$ war ja schon erzeugbar. Das ist der allgemeine Mechanismus des nachfolgenden Lemma 3.2.22: Einen linear abhängigen Vektor darf man weglassen, ohne den Spann zu verkleinern.

Was kann eine Messstation, die nur auf endlich viele Frequenzen lauscht, dann überhaupt vom Funkverkehr mitbekommen? Das klärt der nächste Abschnitt (Leitbeispiel 3.3.6).

Lemma 3.2.22 (Lineare Abhängigkeit und Weglassen eines Vektors)**.** *Sei V ein k-Vektorraum und seien*

$$v_1, \dots, v_n \in V$$

mit $n \geq 1$.

Dann sind die folgenden Aussagen äquivalent.

1. *Das System $v_1, \dots, v_n$ ist linear abhängig.*
2. *Es gibt ein $i \in \{1, \dots, n\}$, sodass*

$$\operatorname{Span}(v_1, \dots, v_n) = \operatorname{Span}(v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n).$$

Beweis. Wir zeigen zuerst: Lineare Abhängigkeit erlaubt das Weglassen eines Vektors.

Angenommen, $v_1, \dots, v_n$ ist linear abhängig.

Dann gibt es Skalare

$$\lambda_1, \dots, \lambda_n \in k,$$

die nicht alle gleich 0 sind, sodass

$$\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$$

gilt.

Da nicht alle Koeffizienten gleich 0 sind, gibt es ein i mit

$$\lambda_i \neq 0.$$

Wir lösen die Gleichung nach v_i auf.

Aus

$$\lambda_1 v_1 + \cdots + \lambda_i v_i + \cdots + \lambda_n v_n = 0$$

folgt

$$\lambda_i v_i = -\sum_{\substack{j=1 \\ j \neq i}}^{n} \lambda_j v_j.$$

Da $\lambda_i \neq 0$ ist und k ein Körper ist, dürfen wir durch λ_i teilen.

Also erhalten wir

$$v_i = \sum_{\substack{j=1 \\ j \neq i}}^{n} \left(-\frac{\lambda_j}{\lambda_i}\right) v_j.$$

Der Vektor v_i ist also eine Linearkombination der übrigen Vektoren.

Daraus folgt: Jede Linearkombination von $v_1, \dots, v_n$ lässt sich auch ohne v_i schreiben.

Also gilt

$$\operatorname{Span}(v_1, \dots, v_n) \subseteq \operatorname{Span}(v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n).$$

Die andere Inklusion ist klar, denn jede Linearkombination der übrigen Vektoren ist insbesondere eine Linearkombination aller Vektoren.

Also gilt Gleichheit der beiden Erzeugnisse.
Nun zeigen wir die Umkehrung.
Angenommen, es gibt ein $i \in \{1, \dots, n\}$ mit

$$\mathrm{Span}(v_1, \dots, v_n) = \mathrm{Span}(v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n).$$

Da v_i natürlich in

$$\mathrm{Span}(v_1, \dots, v_n)$$

liegt, liegt v_i wegen der Gleichheit auch im Spann der übrigen Vektoren.
Also gibt es Skalare $\mu_j \in k$ für $j \neq i$ mit

$$v_i = \sum_{\substack{j=1 \\ j \neq i}}^{n} \mu_j v_j.$$

Dann gilt

$$v_i - \sum_{\substack{j=1 \\ j \neq i}}^{n} \mu_j v_j = 0.$$

Das ist eine nichttriviale Darstellung des Nullvektors als Linearkombination von $v_1, \dots, v_n$, denn der Koeffizient von v_i ist 1.
Also ist $v_1, \dots, v_n$ linear abhängig. □

Bemerkung 3.2.23 (Was die Begriffe leisten)**.** Lineare Unabhängigkeit sagt: Keiner der gegebenen Vektoren ist aus den anderen linear zusammengesetzt.
Erzeugen sagt: Mit den gegebenen Vektoren erreicht man durch Linearkombinationen den ganzen gewünschten Raum.
Diese beiden Eigenschaften beantworten unterschiedliche Fragen. Lineare Unabhängigkeit fragt nach Redundanz. Erzeugen fragt nach Reichweite.
Später werden wir beide Eigenschaften zusammenführen: Eine Basis ist ein linear unabhängiges Erzeugendensystem.

3.2.3 Untervektorräume

Sei k ein Körper und V ein k-Vektorraum.

Definition 3.2.24 (Untervektorraum (Idee))**.** Sei $U \subseteq V$ eine Teilmenge. Wir nennen U einen *Untervektorraum*, genau dann wenn U mit den auf U eingeschränkten Operationen ein k-Vektorraum ist.

Bemerkung 3.2.25 (Was bei Untervektorräumen wirklich geprüft werden muss)**.** Sei V ein k-Vektorraum. Wenn wir eine Teilmenge $U \subseteq V$ betrachten, dann wollen wir wissen, ob U selbst wieder ein k-Vektorraum ist. Dabei benutzen wir auf U keine neuen Rechenoperationen. Wir benutzen die Addition und die Skalarmultiplikation aus V und schränken sie auf U ein.
Bei der Definition eines Vektorraums war die Abgeschlossenheit noch in der Funktionssignatur versteckt. Wir hatten dort

$$+ : V \times V \to V$$

und

$$\cdot : k \times V \to V.$$

Das bedeutet bereits: Wenn $v, w \in V$ sind, dann liegt $v + w$ wieder in V. Wenn $\lambda \in k$ und $v \in V$ sind, dann liegt λv wieder in V. Die Abgeschlossenheit war also keine zusätzliche Zeile unter den Axiomen. Sie war schon dadurch eingebaut, dass Addition und Skalarmultiplikation überhaupt als Abbildungen mit Zielmenge V definiert waren.

Für eine Teilmenge $U \subseteq V$ ist das anders. Aus $u, w \in U$ folgt zwar automatisch $u + w \in V$. Es folgt aber nicht automatisch $u + w \in U$. Ebenso folgt aus $\lambda \in k$ und $u \in U$ zwar automatisch $\lambda u \in V$. Es folgt aber nicht automatisch $\lambda u \in U$.

Die Hauptfrage ist also: Bleiben wir beim Rechnen in U? Genau diese Frage nennt man *Abgeschlossenheit*.

Proposition 3.2.26 (Untervektorraumkriterium)**.** *Sei V ein k-Vektorraum und sei $U \subseteq V$ eine Teilmenge. Angenommen:*

1. $0 \in U$.
2. *Für alle $u, w \in U$ gilt $u + w \in U$.*
3. *Für alle $\lambda \in k$ und alle $u \in U$ gilt $\lambda u \in U$.*

Dann ist U mit der eingeschränkten Addition

$$+ : U \times U \to U, \quad (u, w) \mapsto u + w,$$

und der eingeschränkten Skalarmultiplikation

$$\cdot : k \times U \to U, \quad (\lambda, u) \mapsto \lambda u,$$

ein k-Vektorraum.

Beweis. Die Bedingungen (2) und (3) sagen genau, dass die eingeschränkte Addition und die eingeschränkte Skalarmultiplikation tatsächlich Abbildungen mit Zielmenge U sind. Damit sind die Rechenoperationen auf U wohldefiniert.

Nun müssen wir die Vektorraumaxiome auf U prüfen. Die meisten Axiome werden aber direkt aus V geerbt.

Seien zum Beispiel $u, w, z \in U$. Dann gilt in V

$$u + (w + z) = (u + w) + z.$$

Da beide Seiten Elemente von U sind, gilt dieselbe Gleichung auch in U. Also ist die Addition auf U assoziativ.

Genauso wird die Kommutativität der Addition geerbt. Für $u, w \in U$ gilt in V

$$u + w = w + u.$$

Also gilt diese Gleichung auch in U.

Nach Voraussetzung gilt $0 \in U$. Da 0 in V das neutrale Element der Addition ist, gilt für alle $u \in U$

$$0 + u = u \quad \text{und} \quad u + 0 = u.$$

Also ist 0 auch in U ein neutrales Element.

Es bleibt für die additive Gruppenstruktur noch die Existenz additiver Inverser. Sei $u \in U$. Dann gilt wegen der Abgeschlossenheit unter Skalarmultiplikation

$$(-1)u \in U.$$

In V gilt

$$(-1)u = -u.$$

Also enthält U mit jedem Element u auch sein additives Inverses $-u$.

Damit ist $(U, +, 0)$ eine abelsche Gruppe.

Die übrigen Vektorraumaxiome werden ebenfalls aus V geerbt. Für $\lambda, \mu \in k$ und $u, w \in U$ gelten in V die Gleichungen

$$(\lambda\mu)u = \lambda(\mu u),$$

$$\lambda(u + w) = \lambda u + \lambda w,$$

$$(\lambda + \mu)u = \lambda u + \mu u,$$

und

$$1u = u.$$

Da alle auftretenden Vektoren wegen der Abgeschlossenheit wieder in U liegen, gelten diese Gleichungen auch als Gleichungen in U.

Also ist U ein k-Vektorraum. □

Wir definieren nun den Begriff des Untervektorraumes erneut. Eigentlich ist es strengstens verboten den selben Begriff mehrfach zu definieren, aber wir haben bereits bewiesen, dass die beiden Definitionen äquivalent sind. Wir stellen beide Definitionen vor, da die eine die Idee gut vermittelt, die andere aber deutlich leichter zum arbeiten ist.

Definition 3.2.27 (Untervektorraum (Kriterium))**.** Sei V ein k-Vektorraum. Eine Teilmenge $U \subseteq V$ heißt *Untervektorraum* von V, wenn gilt:

1. $0 \in U$.
2. Für alle $u, w \in U$ gilt $u + w \in U$.
3. Für alle $\lambda \in k$ und alle $u \in U$ gilt $\lambda u \in U$.

Bemerkung 3.2.28 (Warum so wenige Bedingungen genügen)**.** Die Definition sieht viel kürzer aus als die Definition eines Vektorraums. Das liegt daran, dass wir nicht bei null anfangen. Wir sitzen bereits in einem Vektorraum V. Alle Rechenregeln gelten dort schon.

Für eine Teilmenge $U \subseteq V$ müssen wir deshalb nicht noch einmal beweisen, dass die Addition assoziativ oder kommutativ ist. Wir müssen auch nicht noch einmal beweisen, dass die Distributivgesetze gelten. Diese Gleichungen gelten bereits in V und werden auf U vererbt.

Was nicht automatisch vererbt wird, ist die Tatsache, dass die Ergebnisse unserer Rechnungen wieder in U liegen. Deshalb steht bei Untervektorräumen die Abgeschlossenheit im Mittelpunkt.

Wir können das Kriterium sogar durch einige Tricks noch weiter vereinfachen:

Lemma 3.2.29 (Ein einfaches Untervektorraumkriterium)**.** *Sei V ein k-Vektorraum und sei $U \subseteq V$ eine Teilmenge. Dann sind äquivalent:*

1. *U ist ein Untervektorraum von V.*
2. *$U \neq \emptyset$ und für alle $v, w \in U$ und alle $r \in k$ gilt*

$$rv + w \in U.$$

Beweis. Angenommen, U ist ein Untervektorraum von V. Dann gilt insbesondere $0 \in U$. Also ist $U \neq \emptyset$.

Seien nun $v, w \in U$ und $r \in k$. Da U unter Skalarmultiplikation abgeschlossen ist, gilt

$$rv \in U.$$

Da U unter Addition abgeschlossen ist, folgt

$$rv + w \in U.$$

Also gilt die Bedingung aus (2).

Umgekehrt nehmen wir an, dass $U \neq \emptyset$ ist und dass für alle $v, w \in U$ und alle $r \in k$ gilt:

$$rv + w \in U.$$

Da $U \neq \emptyset$ ist, gibt es ein Element $u \in U$. Wenden wir die Bedingung mit $v = u$, $w = u$ und $r = -1$ an, dann erhalten wir

$$(-1)u + u \in U.$$

In V gilt aber

$$(-1)u + u = 0.$$

Also gilt

$$0 \in U.$$

Nun zeigen wir die Abgeschlossenheit unter Skalarmultiplikation. Seien $r \in k$ und $v \in U$. Da $0 \in U$ ist, dürfen wir die Bedingung mit $w = 0$ anwenden. Dann erhalten wir

$$rv + 0 \in U.$$

Also gilt

$$rv \in U.$$

Jetzt zeigen wir die Abgeschlossenheit unter Addition. Seien $v, w \in U$. Wenden wir die Bedingung mit $r = 1$ an, dann erhalten wir

$$1v + w \in U.$$

Da $1v = v$ gilt, folgt

$$v + w \in U.$$

Wir haben also gezeigt:

$$0 \in U,$$

U ist unter Addition abgeschlossen und U ist unter Skalarmultiplikation abgeschlossen. Nach dem Untervektorraumkriterium ist U ein Untervektorraum von V. □

Bemerkung 3.2.30 (Warum die Nichtleere wichtig ist)**.** In dem einfachen Kriterium darf man die Bedingung $U \neq \emptyset$ nicht einfach weglassen. Für $U = \emptyset$ ist die Aussage

$$\text{für alle } v, w \in U \text{ und alle } r \in k \text{ gilt } rv + w \in U$$

nämlich leer wahr: Es gibt in der leeren Menge keine Gegenbeispiele.

Aber $\emptyset$ ist kein Untervektorraum, denn ein Untervektorraum muss den Nullvektor enthalten. Deshalb braucht das Kriterium entweder die Voraussetzung $U \neq \emptyset$ oder direkt die Voraussetzung $0 \in U$.

Lemma 3.2.31. *Für jedes System $v_1, \dots, v_n$ ist* $\mathrm{Span}(v_1, \dots, v_n)$ *ein Untervektorraum. Es ist der kleinste Untervektorraum der $v_1, \dots, v_n$ enthält.*

Beweis. Das ist Hausaufgabe. □

3.2.4 Erzeugendensystem

Sei k ein Körper und V ein k-Vektorraum.

Definition 3.2.32 (Erzeugendensystem)**.** Ein System $v_1, \dots, v_n \in V$ heißt *Erzeugendensystem von V* falls $\mathrm{Span}(v_1, \dots, v_n) = V$. Allgemeiner sei $U \leq V$ ein Untervektorraum. Wir nennen $v_1, \dots, v_n \in U$ ein *Erzeugendensystem von U* falls $\mathrm{Span}(v_1, \dots, v_n) = U$.

Definition 3.2.33 (endlich Erzeugt)**.** Wir nennen V *endlich erzeugt* wenn es ein endliches System $v_1, \dots, v_n$ gibt sodass $V = \mathrm{Span}(v_1, \dots, v_n)$.

Wir interessieren uns in dieser Vorlesung vor allem für endlich erzeugte Vektorräume. Dennoch gibt es wichtige Beispiele von Vektorräumen die *nicht* endlich erzeugt werden. Das erste solche Beispiel kennen wir schon: In Leitbeispiel 3.2.21 haben wir gesehen, dass endlich viele Sender niemals den ganzen Signalraum S erzeugen — S ist also nicht endlich erzeugt. Diese werden ihnen im Laufe ihres Studiums mit einiger Wahrscheinlichkeit auch näher begegnen.

Bemerkung 3.2.34 (Nicht Endlich Erzeugt)**.** Endlich erzeugt heißt: Es gibt endlich viele Vektoren

$$v_1, \dots, v_n \in V,$$

sodass

$$\mathrm{Span}(v_1, \dots, v_n) = V$$

gilt.

Nicht endlich erzeugt heißt dann: Kein endliches System von Vektoren reicht aus, um den ganzen Raum zu erzeugen.

Beispiel 3.2.35 (Polynome)**.** Sei k ein Körper. Der Polynomring

$$k[x]$$

ist ein k-Vektorraum. Die Vektoraddition ist die gewöhnliche Addition von Polynomen. Die Skalarmultiplikation ist die Multiplikation eines Polynoms mit einem Skalar aus k.

Dieser Vektorraum ist nicht endlich erzeugt.

Wir begründen das. Angenommen,

$$p_1, \dots, p_n \in k[x]$$

erzeugen $k[x]$.

Dann haben alle diese Polynome einen endlichen Grad. Wir setzen

$$N := \max\{\deg(p_1), \dots, \deg(p_n)\}.$$

Jede Linearkombination

$$\lambda_1 p_1 + \cdots + \lambda_n p_n$$

hat dann Grad höchstens N. Durch Linearkombinationen von $p_1, \dots, p_n$ können also keine Polynome von Grad größer als N entstehen.

Aber das Polynom

$$x^{N+1}$$

liegt natürlich in $k[x]$. Es kann also nicht im Spann von $p_1, \dots, p_n$ liegen.

Das ist ein Widerspruch. Also ist $k[x]$ nicht endlich erzeugt.

Mathematisch ist $k[x]$ eines der wichtigsten Beispiele für einen unendlich-dimensionalen Vektorraum. In der Physik treten Polynome zum Beispiel bei Taylor-Approximationen, Potentialen und Näherungsverfahren auf.

Beispiel 3.2.36 (Endlich getragene Folgen)**.** Sei k ein Körper. Wir betrachten den Vektorraum

$$k^{(\mathbb{N})} := \{(a_1, a_2, a_3, \ldots) \mid a_i \in k \text{ und nur endlich viele } a_i \text{ sind ungleich } 0\}.$$

Die Elemente dieses Vektorraums sind also unendliche Folgen, bei denen aber nur endlich viele Einträge von 0 verschieden sind.

Dieser Vektorraum ist nicht endlich erzeugt.

Wir begründen das direkt. Angenommen,

$$v_1, \ldots, v_n \in k^{(\mathbb{N})}$$

erzeugen $k^{(\mathbb{N})}$.

Da jeder Vektor v_i nur endlich viele von 0 verschiedene Einträge besitzt, gibt es insgesamt nur endlich viele Stellen, an denen irgendeiner der Vektoren

$$v_1, \ldots, v_n$$

einen von 0 verschiedenen Eintrag hat.

Also gibt es ein $m \in \mathbb{N}$, sodass alle Vektoren

$$v_1, \ldots, v_n$$

ab der Stelle m nur noch Nullen besitzen.

Dann hat aber auch jede Linearkombination von $v_1, \ldots, v_n$ ab der Stelle m nur noch Nullen.

Der Vektor

$$e_m = (0, \ldots, 0, 1, 0, 0, \ldots)$$

mit einer 1 an der m-ten Stelle liegt aber in $k^{(\mathbb{N})}$.

Er kann nicht aus $v_1, \ldots, v_n$ erzeugt werden.

Das ist ein Widerspruch. Also ist $k^{(\mathbb{N})}$ nicht endlich erzeugt.

Anschaulich: Jeder endliche Satz von Erzeugern benutzt nur endlich viele Koordinaten. Der Raum selbst hat aber unendlich viele mögliche Koordinatenrichtungen.

Beispiel 3.2.37 (Alle Folgen)**.** Sei k ein Körper. Wir betrachten den Vektorraum

$$k^{\mathbb{N}} = \{(a_1, a_2, a_3, \ldots) \mid a_i \in k\}.$$

Dies ist der Vektorraum aller Folgen mit Einträgen in k.

Auch dieser Vektorraum ist nicht endlich erzeugt. Die Idee ist: Er enthält einen nicht endlich erzeugten anderen Vektorraum (den der endlich getragenen Folgen).

In Anwendungen kann man Folgen als diskrete Signale oder als Zustände auf einem eindimensionalen Gitter interpretieren. In der Physik denkt man dabei zum Beispiel an unendlich viele gekoppelte Freiheitsgrade.

Beispiel 3.2.38 (Funktionen auf einer unendlichen Menge)**.** Sei X eine unendliche Menge und sei k ein Körper. Wir betrachten den Vektorraum

$$\mathcal{F}(X, k) := \{f : X \to k\}$$

aller Funktionen von X nach k.

Dieser Vektorraum ist nicht endlich erzeugt.

Die Idee ist: Zu jedem Punkt $x \in X$ gibt es die Indikatorfunktion

$$\chi_x : X \to k$$

mit

$$\chi_x(y) = \begin{cases} 1, & y = x, \\ 0, & y \neq x. \end{cases}$$

Wählen wir verschiedene Punkte

$$x_1, \dots, x_m \in X,$$

dann sind die Funktionen

$$\chi_{x_1}, \cdots, \chi_{x_m}$$

linear unabhängig.

Denn aus

$$\lambda_1 \chi_{x_1} + \cdots + \lambda_m \chi_{x_m} = 0$$

folgt durch Einsetzen von x_i:

$$\lambda_i = 0.$$

Da X unendlich ist, können wir solche linear unabhängigen Systeme beliebiger Länge finden.

Wir werden später sehen, dass deshalb $\mathscr{F}(X, k)$ nicht endlich erzeugt sein kann.

Dieses Beispiel ist sehr grundlegend. Physikalisch kann man sich eine Funktion als Feld vorstellen, das jedem Punkt eines Raumes einen Wert zuordnet. Ein Feld hat dann nicht nur endlich viele Freiheitsgrade, sondern im Idealfall einen Freiheitsgrad an jedem Punkt.

Beispiel 3.2.39 (Stetige und glatte Funktionen)**.** Der Vektorraum

$$C(\mathbb{R}, \mathbb{R})$$

aller stetigen Funktionen

$$f : \mathbb{R} \to \mathbb{R}$$

ist nicht endlich erzeugt.

Ebenso ist der Vektorraum

$$C^\infty(\mathbb{R}, \mathbb{R})$$

aller glatten Funktionen

$$f : \mathbb{R} \to \mathbb{R}$$

nicht endlich erzeugt.

Hier ist der Grund wieder, dass sie die Polynome enthalten und diese bereits nicht endlich erzeugt sind.

In der Physik treten solche Räume zum Beispiel als Räume möglicher Bahnkurven, Felder, Wellenprofile oder Temperaturverteilungen auf.

Wichtig ist hier eine feine Unterscheidung: In der Analysis approximiert man Funktionen oft durch Polynome, Fourier-Reihen oder andere endliche Näherungen. Das bedeutet aber nicht, dass der Funktionenraum als Vektorraum endlich erzeugt ist. Eine Approximation ist etwas anderes als eine exakte Darstellung durch eine endliche Linearkombination fester Erzeuger.

Beispiel 3.2.40 (Hilberträume in der Quantenmechanik)**.** Der Raum

$$\ell^2(\mathbb{N})$$

besteht aus allen komplexen Folgen

$$(a_1, a_2, a_3, \dots)$$

mit

$$\sum_{i=1}^{\infty} |a_i|^2 < \infty.$$

Dies ist ein $\mathbb{C}$-Vektorraum. Er ist nicht endlich erzeugt.

Denn für jedes $m \in \mathbb{N}$ enthält $\ell^2(\mathbb{N})$ die Vektoren

$$e_1, \dots, e_m,$$

wobei e_i an der i-ten Stelle eine 1 und sonst nur Nullen hat.

Diese Vektoren sind linear unabhängig. Also enthält $\ell^2(\mathbb{N})$ linear unabhängige Systeme beliebiger Länge.

Deshalb kann $\ell^2(\mathbb{N})$ nicht endlich erzeugt sein.

In der Quantenmechanik werden Zustandsräume häufig durch Hilberträume modelliert. Endlichdimensionale Vektorräume beschreiben dann Systeme mit endlich vielen unabhängigen Zustandsrichtungen. Unendlichdimensionale Hilberträume beschreiben Systeme mit unendlich vielen möglichen unabhängigen Zustandsrichtungen.

Ein typisches Beispiel ist ein Quantensystem, dessen Zustände durch Wellenfunktionen beschrieben werden.

Bemerkung 3.2.41 (Was diese Beispiele gemeinsam haben)**.** Alle Beispiele zeigen dieselbe Grundidee.

Ein endlich erzeugter Vektorraum besitzt nur endlich viele unabhängige Richtungen.

Die Räume oben besitzen dagegen immer wieder neue Richtungen:

$$1, x, x^2, x^3, \dots$$

bei Polynomen und Potenzreihen,

$$e_1, e_2, e_3, \dots$$

bei Folgenräumen, und viele verschiedene unabhängige Funktionen bei Funktionenräumen.

Deshalb sind sie nicht endlich erzeugt.

Intuitiv: Endlichdimensionale Vektorräume beschreiben Systeme mit endlich vielen Freiheitsgraden. Unendlichdimensionale Vektorräume beschreiben Systeme, in denen immer neue unabhängige Freiheitsgrade auftauchen können.

3.3 Basen und Dimension

3.3.1 Was sind Basen – Existenz & Konstruktion

Sei k ein Körper und V ein k-Vektorraum.

Definition 3.3.1 (Basis)**.** Ein System $v_1, \dots, v_n$ von Vektoren in V heißt eine *Basis* von V, wenn es linear unabhängig ist und V erzeugt.

Bemerkung 3.3.2. Das heißt, $v_1, \dots, v_n$ ist eine Basis, wenn

$$V = \operatorname{Span}(v_1, \dots, v_n)$$

und wenn aus

$$\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$$

bereits

$$\lambda_1 = \cdots = \lambda_n = 0$$

folgt.

Lemma 3.3.3 (Basen und eindeutige Darstellung)**.** *Sei $v_1, \dots, v_n \in V$ ein System von Vektoren. Es gilt*

1. *Das System $v_1, \dots, v_n$ ist genau dann linear unabhängig wenn jedes $v \in V$* höchstens *eine Darstellung als Linearkombination von $v_1, \dots, v_n$ hat.*
2. *Das System $v_1, \dots, v_n$ ist genau dann ein Erzeugendensystem wenn jedes $v \in V$* mindestens *eine Darstellung als Linearkombination von $v_1, \dots, v_n$ hat.*
3. *Das System $v_1, \dots, v_n$ ist genau dann eine Basis wenn jedes $v \in V$* genau *eine Darstellung als Linearkombination von $v_1, \dots, v_n$ hat.*

1. *Beweis.* Das ist Lemma 3.2.18.

   Wir wiederholen den Beweis: Angenommen, das System $v_1, \dots, v_n$ ist linear unabhängig. Sei $v \in V$ ein Vektor mit zwei Darstellungen

   $$v = \lambda_1 v_1 + \cdots + \lambda_n v_n = \mu_1 v_1 + \cdots + \mu_n v_n.$$

   Dann folgt durch Subtraktion

   $$0 = (\lambda_1 - \mu_1)v_1 + \cdots + (\lambda_n - \mu_n)v_n.$$

   Da $v_1, \dots, v_n$ linear unabhängig ist, muss

   $$\lambda_i - \mu_i = 0$$

   für alle i gelten. Also ist $\lambda_i = \mu_i$ für alle i. Die beiden Darstellungen waren also dieselbe Darstellung.

   Umgekehrt nehmen wir an, dass jedes $v \in V$ höchstens eine Darstellung als Linearkombination von $v_1, \dots, v_n$ hat. Insbesondere hat dann der Nullvektor höchstens eine solche Darstellung. Er hat aber immer die triviale Darstellung

   $$0 = 0v_1 + \cdots + 0v_n.$$

   Also kann es keine nichttriviale Darstellung des Nullvektors geben. Das bedeutet genau, dass $v_1, \dots, v_n$ linear unabhängig ist.

2. Das ist die Definition von „Erzeugendensystem“.

3. Das folgt aus den ersten beiden Aussagen:

   Eine Basis ist genau ein linear unabhängiges Erzeugendensystem. Linear unabhängig bedeutet: höchstens eine Darstellung. Erzeugendensystem bedeutet: mindestens eine Darstellung. Zusammen bedeutet das: genau eine Darstellung.

□

Beispiel 3.3.4 (Die Standardbasis)**.** Die Vektoren

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

bilden eine Basis von k^n. Denn jeder Vektor $(x_1, \dots, x_n) \in k^n$ hat die Darstellung

$$(x_1, \dots, x_n) = x_1 e_1 + \cdots + x_n e_n.$$

Außerdem ist diese Darstellung eindeutig.

Bemerkung 3.3.5 (Die Bedeutung des Basisbegriffs)**.** Eine Basis erlaubt ein Koordinatensystem ohne überflüssige Information. Das Erzeugendensystem sagt: Alle Vektoren können beschrieben werden. Die lineare Unabhängigkeit sagt: Diese Beschreibung ist eindeutig.

Leitbeispiel 3.3.6 (Die Messstation: drei Detektoren, drei Dimensionen)**.** Eine Messstation lauscht in den Äther. Sie besitzt drei Detektoren, fest eingestellt auf drei verschiedene Frequenzen c_1, c_2, c_3. Detektor i zeigt eine einzige Zahl an: die Stärke, mit der die reine Welle s_{c_i} im ankommenden Signal vertreten ist. Auf alle anderen Frequenzen reagiert er nicht. Wir idealisieren dabei kräftig: Ein realer Detektor hört immer ein ganzes Frequenzfenster mit, unsere Detektoren dagegen sehen *ausschließlich* ihre eigene, scharfe Frequenz. Das ist unphysikalisch, aber es macht sichtbar, worauf es ankommt.

Zuerst lauert hier ein Problem: Warum ist die Anzeige überhaupt *wohldefiniert*? Könnte ein und dasselbe Signal auf *zwei* Weisen Überlagerung sein — etwa $v = 3s_{c_1} + 5s_{c_2}$ und zugleich $v = 4s_{c_1} + 2s_{c_2} + s_{c_3}$ —, dann wüsste Detektor 1 nicht, ob er 3 oder 4 anzeigen soll. Genau das kann nicht passieren: Empfängt die Station ein Signal aus dem Spann

$$W := \operatorname{Span}(s_{c_1}, s_{c_2}, s_{c_3}),$$

so ist es eine Überlagerung $v = \lambda_1 s_{c_1} + \lambda_2 s_{c_2} + \lambda_3 s_{c_3}$. Die drei reinen Wellen sind linear unabhängig (Leitbeispiel 3.2.13) und erzeugen W — sie sind also eine *Basis* von W. Nach Lemma 3.3.3 sind die Koeffizienten $(\lambda_1, \lambda_2, \lambda_3)$ durch v eindeutig bestimmt. Genau deshalb kann Detektor i guten Gewissens die Zahl λ_i anzeigen — genauer: den *Vorfaktor* λ_i, der auch negativ sein kann — und die Anzeige der Station ist das Koordinatentripel des Signals bezüglich der Basis $s_{c_1}, s_{c_2}, s_{c_3}$. (Enthält das Signal noch weitere Frequenzen, ist auch dann eindeutig bestimmt, wie stark c_i darin vertreten ist. Streicht man aus der Überlagerung alle Summanden mit fremden Frequenzen, bleibt der *W-Anteil* des Signals übrig — nur ihn zeigen die Detektoren an, vom Rest bemerken sie nichts.)

Was die Station von der Welt mitbekommt, sind also drei Zahlen. Ihre Welt ist der dreidimensionale Raum W — egal wie reichhaltig der Funkverkehr draußen tatsächlich ist. (Das Wort *Dimension* definieren wir im nächsten Abschnitt präzise; hier meint es einfach: die Länge einer Basis.) Installiert die Station einen vierten Detektor für eine neue Frequenz c_4, so wächst ihre Welt auf $\operatorname{Span}(s_{c_1}, s_{c_2}, s_{c_3}, s_{c_4})$, einen Raum der Dimension vier: Jeder Detektor für eine neue Frequenz erhöht die Dimension der Messdaten um eins. Die Dimension ist hier also keine abstrakte Kennzahl, sondern zählt die unabhängigen Fragen, die die Station an das Signal stellen kann.

Das ist übrigens nicht weit von unserer eigenen Lage entfernt: Das menschliche Auge misst das einfallende Licht mit drei Zapfensorten — auch unser Farbensehen ist in diesem Sinne dreidimensional.

Ausblick. Zwei Dinge haben wir unterschlagen. Reale Wellen sind gegeneinander *phasenverschoben*: Statt $\sin(cx)$ kommt $\sin(cx + b)$ an. Ein Additionstheorem aus der Schule zerlegt diese Welle in eine Überlagerung — mit Skalaren als Vorfaktoren, ganz in der Sprache dieses Kapitels:

$$\sin(cx + b) = \cos(b)\,\sin(cx) + \sin(b)\,\cos(cx).$$

Pro Frequenz braucht man dann zwei Zahlen statt einer. (Der passende Signalraum enthält dann neben den Sinus- auch die Kosinuswellen — ein größerer Vektorraum nach demselben Bauplan, denn $\cos(cx)$ liegt nicht in unserem S.) Und reale Detektoren haben eine *Bandbreite*: Sie messen nicht den Koeffizienten einer scharfen Frequenz, sondern einen gewichteten Mittelwert über ein Frequenzfenster — beschrieben durch ein Integral. Beides ändert nichts am Grundbild: Endlich viele Detektoren, endlichdimensionale Messdaten.

Lemma 3.3.7 (Streichen überflüssiger Vektoren)**.** *Sei $v_1, \dots, v_n$ ein System von Vektoren in V. Sei $i_0 \in \{1, \dots, n\}$. Angenommen, v_{i_0} ist eine Linearkombination der übrigen Vektoren*

$$\{v_1, \dots, v_n\} \setminus \{v_{i_0}\}.$$

Dann gilt

$$\mathrm{Span}(v_1, \dots, v_n) = \mathrm{Span}(\{v_1, \dots, v_n\} \setminus \{v_{i_0}\}).$$

Beweis. Die Inklusion

$$\mathrm{Span}(\{v_1, \dots, v_n\} \setminus \{v_{i_0}\}) \subseteq \mathrm{Span}(v_1, \dots, v_n)$$

ist klar, denn rechts stehen mehr Vektoren zur Verfügung.

Für die andere Inklusion reicht es zu zeigen, dass jeder der Vektoren $v_1, \dots, v_n$ im rechten Erzeugnis liegt. Der Grund dafür, dass das reicht, ist dass falls wir $w = \sum_{i=1}^{n} a_i v_i$ haben und $v_j = \sum_{i \neq j} b_i v_i$ haben, dass wir dann das v_j in der ersten Summe durch die Linearkombination ersetzen können und damit v_j in der ersten Summe auch nicht brauchen:

$$\begin{aligned} w &= \sum_{i=1}^{n} a_i v_i && = \left(\sum_{i \neq j} a_i v_i\right) + a_j v_j \\ &= \left(\sum_{i \neq j} a_i v_i\right) + a_j \cdot \left(\sum_{i \neq j} b_i v_i\right) \\ &= \sum_{i \neq j} \left(a_i v_i + a_j b_i v_i\right) \\ &= \sum_{i \neq j} \left((a_i + a_j b_i) \cdot v_i\right) \end{aligned}$$

Oder als Slogan: „Linearkombinationen von Linearkombinationen sind Linearkombinationen".

Für alle Vektoren außer v_{i_0} ist das klar. Der Vektor v_{i_0} liegt nach Voraussetzung im Erzeugnis der übrigen Vektoren. Also liegt jede Linearkombination von $v_1, \dots, v_n$ schon im Erzeugnis der übrigen Vektoren. Damit folgt die Gleichheit. □

Lemma 3.3.8 (Lineare Abhängigkeit erkennt überflüssige Vektoren)**.** *Sei $v_1, \dots, v_n$ ein linear abhängiges System. Dann gibt es ein $i_0 \in \{1, \dots, n\}$, sodass v_{i_0} eine Linearkombination der übrigen Vektoren ist.*

Beweis. Da das System linear abhängig ist, gibt es Skalare $\lambda_1, \dots, \lambda_n \in k$, die nicht alle Null sind, mit

$$\lambda_1 v_1 + \cdots + \lambda_n v_n = 0.$$

Wähle ein i_0 mit $\lambda_{i_0} \neq 0$. Dann können wir nach v_{i_0} auflösen:

$$v_{i_0} = -\sum_{\substack{i=1 \\ i \neq i_0}}^{n} \frac{\lambda_i}{\lambda_{i_0}} v_i.$$

Also ist v_{i_0} eine Linearkombination der übrigen Vektoren. □

Theorem 3.3.9 (Auswahlsatz)**.** *Sei V ein k-Vektorraum. Sei $v_1, \dots, v_n$ ein Erzeugendensystem von V. Dann kann man aus diesem System geeignete Vektoren streichen, sodass die verbleibenden Vektoren eine Basis von V bilden.*

Genauer: Es gibt Indizes

$$1 \leq i_1 < \cdots < i_r \leq n$$

sodass

$$v_{i_1}, \dots, v_{i_r}$$

eine Basis von V ist.

Beweis. Wir beginnen mit dem Erzeugendensystem $v_1, \dots, v_n$.

Ist dieses System linear unabhängig, dann ist es bereits eine Basis, und wir sind fertig.

Ist es linear abhängig, dann ist nach Lemma 3.3.8 einer der Vektoren eine Linearkombination der übrigen Vektoren. Nach Lemma 3.3.7 können wir diesen Vektor streichen, ohne das Erzeugnis zu verändern.

Wir wiederholen dieses Verfahren. Bei jedem Schritt wird das System um einen Vektor kürzer, erzeugt aber weiterhin denselben Vektorraum V. Da wir mit nur endlich vielen Vektoren begonnen haben, muss dieses Verfahren nach endlich vielen Schritten enden.

Am Ende erhalten wir ein Erzeugendensystem von V, aus dem kein weiterer Vektor mehr wegen linearer Abhängigkeit gestrichen werden kann. Also ist dieses verbleibende System linear unabhängig. Damit ist es ein linear unabhängiges Erzeugendensystem, also eine Basis von V. □

Korollar 3.3.10 (Existenzsatz für Basen)**.** *Jeder endlich erzeugte k-Vektorraum besitzt eine Basis.*

Beweis. Sei V endlich erzeugt. Dann besitzt V ein endliches Erzeugendensystem. Nach dem Auswahlsatz kann man daraus eine Basis auswählen. □

Theorem 3.3.11 (Basisergänzungssatz)**.** *Sei V ein endlich erzeugter k-Vektorraum. Sei $v_1, \dots, v_r$ ein linear unabhängiges System in V. Dann kann man dieses System zu einer Basis von V ergänzen.*

Das heißt: Es gibt Vektoren $w_1, \dots, w_s \in V$, sodass

$$v_1, \dots, v_r, w_1, \dots, w_s$$

eine Basis von V ist.

Beweis. Da V endlich erzeugt ist, gibt es ein endliches Erzeugendensystem

$$u_1, \dots, u_m$$

von V.

Dann ist auch das längere System

$$v_1, \dots, v_r, u_1, \dots, u_m$$

ein Erzeugendensystem von V.

Nun streichen wir aus diesem System so lange überflüssige Vektoren, bis eine Basis übrig bleibt. Dabei streichen wir nie einen der Vektoren $v_1, \dots, v_r$.

Warum ist das möglich? Solange das gesamte System linear abhängig ist, gibt es eine nichttriviale lineare Relation. Da $v_1, \dots, v_r$ selbst linear unabhängig ist, kann diese Relation nicht nur die Vektoren $v_1, \dots, v_r$ betreffen. Also kommt in einer solchen Relation mindestens einer der später hinzugefügten Vektoren mit Koeffizient ungleich Null vor. Diesen Vektor können wir nach den anderen auflösen und streichen.

Nach endlich vielen Schritten erhalten wir eine Basis von V, die alle ursprünglichen Vektoren $v_1, \dots, v_r$ noch enthält. □

3.3.2 Die Länge von Basen – Dimension

Lemma 3.3.12 (Austauschlemma)**.** *Sei $v_1, \dots, v_n$ eine Basis des k-Vektorraums V. Sei $w \in V$ mit $w \neq 0$. Dann gibt es eindeutig bestimmte Skalare $\lambda_1, \dots, \lambda_n \in k$ mit*

$$w = \lambda_1 v_1 + \cdots + \lambda_n v_n.$$

Da $w \neq 0$ ist, ist mindestens einer dieser Skalare ungleich 0.

Sei nun $i_0 \in \{1, \dots, n\}$ mit $\lambda_{i_0} \neq 0$. Dann ist auch

$$v_1, \dots, v_{i_0-1}, w, v_{i_0+1}, \dots, v_n$$

eine Basis von V.

Beweis. Da $v_1, \dots, v_n$ eine Basis ist, hat jeder Vektor in V genau eine Darstellung als Linearkombination von $v_1, \dots, v_n$. Also gibt es eindeutig bestimmte Skalare $\lambda_1, \dots, \lambda_n \in k$ mit

$$w = \lambda_1 v_1 + \cdots + \lambda_n v_n.$$

Wären alle $\lambda_i = 0$, dann wäre $w = 0$. Das widerspricht der Voraussetzung $w \neq 0$.

Wir zeigen nun, dass nach dem Austausch wieder eine Basis vorliegt.

Zuerst zeigen wir, dass das neue System V erzeugt. Aus

$$w = \lambda_1 v_1 + \cdots + \lambda_n v_n$$

und $\lambda_{i_0} \neq 0$ folgt

$$v_{i_0} = \frac{1}{\lambda_{i_0}} w - \sum_{\substack{i=1 \\ i \neq i_0}}^{n} \frac{\lambda_i}{\lambda_{i_0}} v_i.$$

Also liegt der entfernte Vektor v_{i_0} im Erzeugnis des neuen Systems. Alle anderen Basisvektoren liegen ohnehin im neuen System. Daher erzeugt das neue System ganz V.

Es bleibt die lineare Unabhängigkeit. Angenommen, es gilt

$$\mu w + \sum_{\substack{i=1 \\ i \neq i_0}}^{n} v_i v_i = 0.$$

Setzen wir die Darstellung von w ein, so erhalten wir

$$\mu \lambda_{i_0} v_{i_0} + \sum_{\substack{i=1 \\ i \neq i_0}}^{n} (v_i + \mu \lambda_i) v_i = 0.$$

Da $v_1, \dots, v_n$ linear unabhängig ist, müssen alle Koeffizienten verschwinden. Insbesondere gilt

$$\mu \lambda_{i_0} = 0.$$

Da $\lambda_{i_0} \neq 0$ ist, folgt $\mu = 0$. Dann folgt auch $v_i = 0$ für alle $i \neq i_0$. Also ist das neue System linear unabhängig.

Damit ist das neue System ein linear unabhängiges Erzeugendensystem, also eine Basis. □

Theorem 3.3.13 (Steinitzscher Austauschsatz)**.** *Sei $a_1, \dots, a_m$ ein linear unabhängiges System im k-Vektorraum V. Sei $b_1, \dots, b_n$ eine Basis von V. Dann gilt $m \leq n$.*

Genauer: Man kann die Basis $b_1, \dots, b_n$ so austauschen, dass man eine Basis der Länge n erhält, die alle Vektoren $a_1, \dots, a_m$ enthält.

Beweis. Wir beweisen die Aussage durch Induktion über m.

Für $m = 0$ ist nichts zu zeigen.

Sei also $m \geq 1$. Nach Induktionsvoraussetzung können wir die Vektoren

$$a_1, \dots, a_{m-1}$$

in eine Basis der Länge n einbauen. Wir erhalten also eine Basis der Form

$$a_1, \dots, a_{m-1}, c_m, \dots, c_n,$$

wobei die Vektoren $c_m, \dots, c_n$ aus der ursprünglichen Basis

$$b_1, \dots, b_n$$

stammen.

Wir schreiben nun a_m bezüglich dieser Basis:

$$a_m = \lambda_1 a_1 + \cdots + \lambda_{m-1} a_{m-1} + \mu_m c_m + \cdots + \mu_n c_n.$$

Es muss mindestens ein Koeffizient μ_j ungleich 0 sein. Andernfalls läge a_m im Erzeugnis von $a_1, \dots, a_{m-1}$. Dann wäre das System $a_1, \dots, a_m$ linear abhängig, im Widerspruch zur Voraussetzung.

Insbesondere gibt es überhaupt einen Index $j \in \{m, \dots, n\}$. Also gilt $m \leq n$.

Da $\mu_j \neq 0$ ist, dürfen wir nach dem Austauschlemma den Basisvektor c_j durch a_m ersetzen. Dadurch erhalten wir eine Basis der Länge n, die nun

$$a_1, \dots, a_m$$

enthält. □

Korollar 3.3.14 (Lineare Unabhängigkeit ist durch Erzeugendensysteme beschränkt)**.** *Sei V ein k-Vektorraum. Sei $a_1, \dots, a_m$ ein linear unabhängiges System in V. Sei $b_1, \dots, b_n$ ein Erzeugendensystem von V. Dann gilt*

$$m \leq n.$$

Beweis. Nach dem Auswahlsatz kann man aus dem Erzeugendensystem $b_1, \dots, b_n$ eine Basis auswählen. Diese Basis hat eine Länge $r \leq n$. Nach dem Steinitzschen Austauschsatz gilt $m \leq r$. Also gilt insgesamt

$$m \leq r \leq n.$$

□

Korollar 3.3.15 (Alle Basen haben dieselbe Länge)**.** *Sei V ein endlich erzeugter k-Vektorraum. Dann besitzt V eine Basis, und alle Basen von V haben dieselbe Länge.*

Beweis. Nach dem Existenzsatz besitzt V mindestens eine Basis.

Seien nun

$$a_1, \dots, a_m \quad \text{und} \quad b_1, \dots, b_n$$

zwei Basen von V. Da $a_1, \dots, a_m$ linear unabhängig ist und $b_1, \dots, b_n$ ein Erzeugendensystem ist, folgt aus Korollar 3.3.14

$$m \leq n.$$

Vertauschen wir die Rollen der beiden Basen, so erhalten wir ebenso

$$n \leq m.$$

Also ist $m = n$. □

Definition 3.3.16 (Dimension)**.** Sei V ein endlich erzeugter k-Vektorraum. Die gemeinsame Länge n aller Basen von V heißt die *Dimension* von V. Wir schreiben

$$\dim(V) := n.$$

Ist $\dim(V) = n$, so sagen wir: V ist n-dimensional.

Beispiel 3.3.17. Es gilt

$$\dim(k^n) = n.$$

Denn die Standardbasis $e_1, \dots, e_n$ ist eine Basis von k^n.

Korollar 3.3.18 (Lineare Unabhängigkeit plus richtige Länge)**.** *Sei V ein endlich erzeugter k-Vektorraum mit*

$$\dim(V) = n.$$

Sei $a_1, \dots, a_n$ ein linear unabhängiges System in V. Dann ist $a_1, \dots, a_n$ eine Basis von V.

Beweis. Nach dem Basisergänzungssatz kann man das linear unabhängige System

$$a_1, \dots, a_n$$

zu einer Basis von V ergänzen. Diese Basis hat aber nach Definition der Dimension Länge n. Also kann kein weiterer Vektor ergänzt worden sein. Daher ist bereits $a_1, \dots, a_n$ eine Basis von V. □

Korollar 3.3.19 (Erzeugendensystem plus richtige Länge)**.** *Sei V ein endlich erzeugter k-Vektorraum mit*

$$\dim(V) = n.$$

Sei $a_1, \dots, a_n$ ein Erzeugendensystem von V. Dann ist $a_1, \dots, a_n$ eine Basis von V.

Beweis. Nach dem Auswahlsatz kann man aus $a_1, \dots, a_n$ eine Basis von V auswählen. Diese Basis hat nach Definition der Dimension Länge n. Da das ursprüngliche System ebenfalls aus genau n Vektoren besteht, wurde beim Auswählen kein Vektor gestrichen. Also ist bereits $a_1, \dots, a_n$ eine Basis von V. □

Beispiel 3.3.20 (Zwei Vektoren in $\mathbb{R}^2$)**.** Seien $a, b > 0$. Wir betrachten die beiden Vektoren

$$v_1 = \begin{pmatrix} a \\ b \end{pmatrix}, \qquad v_2 = \begin{pmatrix} a+1 \\ b \end{pmatrix}$$

in $\mathbb{R}^2$.

Beide Vektoren sind ungleich 0. Außerdem ist keiner ein Vielfaches des anderen: Wäre etwa

$$\begin{pmatrix} a+1 \\ b \end{pmatrix} = \lambda \begin{pmatrix} a \\ b \end{pmatrix},$$

dann folgt aus der zweiten Komponente

$$b = \lambda b.$$

Da $b > 0$ ist, folgt $\lambda = 1$. Dann würde aus der ersten Komponente aber

$$a + 1 = a$$

folgen, ein Widerspruch.

Also sind v_1 und v_2 linear unabhängig. Da

$$\dim(\mathbb{R}^2) = 2$$

gilt, folgt aus Korollar 3.3.18, dass v_1, v_2 eine Basis von $\mathbb{R}^2$ bilden.

Insbesondere erzeugen sie $\mathbb{R}^2$:

$$\operatorname{Span}\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \mathbb{R}^2.$$

3.3.3 Anwendungen und Rechenregeln der Dimension

Korollar 3.3.21 (Effektivität der Dimension)**.** *Sei V ein endlich erzeugter k-Vektorraum, und sei $U \subseteq V$ ein Untervektorraum. Dann ist U endlich erzeugt und es gilt*

$$\dim(U) \leq \dim(V).$$

Außerdem gilt

$$\dim(U) = \dim(V) \quad \Longleftrightarrow \quad U = V.$$

Beweis. Setze

$$n := \dim(V).$$

Jedes linear unabhängige System in U ist auch ein linear unabhängiges System in V. Nach Korollar 3.3.14 kann ein solches System höchstens Länge n haben.

Wir konstruieren nun eine Basis von U. Ist $U = \{0\}$, dann ist das leere System eine Basis von U. Sei also $U \neq \{0\}$. Dann wählen wir einen Vektor $u_1 \in U$ mit $u_1 \neq 0$. Falls u_1 noch nicht ganz U erzeugt, wählen wir einen Vektor

$$u_2 \in U \setminus \operatorname{Span}(u_1).$$

Dann ist u_1, u_2 linear unabhängig. Falls u_1, u_2 noch nicht ganz U erzeugen, wählen wir

$$u_3 \in U \setminus \operatorname{Span}(u_1, u_2).$$

Auf diese Weise fahren wir fort.

Dieser Prozess muss nach höchstens n Schritten enden, denn in U kann es kein linear unabhängiges System der Länge $n + 1$ geben. Am Ende erhalten wir also ein linear unabhängiges System

$$u_1, \dots, u_r$$

in U, das ganz U erzeugt. Also ist $u_1, \dots, u_r$ eine Basis von U. Damit ist U endlich erzeugt, und es gilt

$$\dim(U) = r \leq n = \dim(V).$$

Ist $U = V$, dann ist natürlich $\dim(U) = \dim(V)$.

Sei umgekehrt $\dim(U) = \dim(V) = n$. Sei $u_1, \dots, u_n$ eine Basis von U. Dann ist $u_1, \dots, u_n$ insbesondere ein linear unabhängiges System in V der Länge $\dim(V)$. Nach Korollar 3.3.18 ist $u_1, \dots, u_n$ also eine Basis von V. Daher gilt

$$V = \operatorname{Span}(u_1, \dots, u_n) = U. \qquad \square$$

Definition 3.3.22 (Summe von Untervektorräumen)**.** Seien $U, W \subseteq V$ Untervektorräume. Die *Summe* von U und W ist

$$U + W := \{u + w \mid u \in U,\ w \in W\}.$$

Lemma 3.3.23. *Seien $U, W \subseteq V$ Untervektorräume. Dann sind auch*

$$U \cap W \quad \textit{und} \quad U + W$$

Untervektorräume von V.

Beweis. Für den Schnitt ist klar, dass $0 \in U \cap W$ gilt. Sind $x, y \in U \cap W$ und $\lambda, \mu \in k$, dann liegen x, y sowohl in U als auch in W. Also liegt auch

$$\lambda x + \mu y$$

sowohl in U als auch in W. Damit liegt $\lambda x + \mu y$ in $U \cap W$.

Für die Summe gilt $0 = 0 + 0 \in U + W$. Seien nun $x, y \in U + W$. Dann gibt es $u_1, u_2 \in U$ und $w_1, w_2 \in W$ mit

$$x = u_1 + w_1, \qquad y = u_2 + w_2.$$

Für $\lambda, \mu \in k$ gilt dann

$$\lambda x + \mu y = (\lambda u_1 + \mu u_2) + (\lambda w_1 + \mu w_2).$$

Der erste Summand liegt in U, der zweite in W. Also liegt $\lambda x + \mu y$ in $U + W$. □

Theorem 3.3.24 (Dimensionsformel für Untervektorräume)**.** *Seien $U, W \subseteq V$ endlich dimensionale Untervektorräume. Dann gilt*

$$\dim(U + W) + \dim(U \cap W) = \dim(U) + \dim(W).$$

Beweis. Sei

$$b_1, \dots, b_n$$

eine Basis von $U \cap W$.

Nach dem Basisergänzungssatz ergänzen wir diese Basis zu einer Basis von U:

$$b_1, \dots, b_n, a_1, \dots, a_r.$$

Ebenso ergänzen wir sie zu einer Basis von W:

$$b_1, \dots, b_n, c_1, \dots, c_s.$$

Wir behaupten, dass

$$b_1, \dots, b_n, a_1, \dots, a_r, c_1, \dots, c_s$$

eine Basis von $U + W$ ist.

Zuerst zeigen wir, dass dieses System $U + W$ erzeugt. Sei $v \in U + W$. Dann gibt es $u \in U$ und $w \in W$ mit

$$v = u + w.$$

Da $b_1, \dots, b_n, a_1, \dots, a_r$ eine Basis von U ist, ist u eine Linearkombination dieser Vektoren. Da $b_1, \dots, b_n, c_1, \dots, c_s$ eine Basis von W ist, ist w eine Linearkombination dieser Vektoren. Also ist $v = u + w$ eine Linearkombination von

$$b_1, \dots, b_n, a_1, \dots, a_r, c_1, \dots, c_s.$$

Nun zeigen wir die lineare Unabhängigkeit. Angenommen, es gilt

$$\sum_{i=1}^{n} \lambda_i b_i + \sum_{j=1}^{r} \mu_j a_j + \sum_{\ell=1}^{s} \nu_\ell c_\ell = 0.$$

Dann gilt

$$\sum_{i=1}^{n} \lambda_i b_i + \sum_{j=1}^{r} \mu_j a_j = -\sum_{\ell=1}^{s} \nu_\ell c_\ell.$$

Die linke Seite liegt in U, die rechte Seite liegt in W. Also liegen beide Seiten in $U \cap W$.

Da $b_1, \dots, b_n$ eine Basis von $U \cap W$ ist, gibt es Skalare $\rho_1, \dots, \rho_n \in k$ mit

$$\sum_{i=1}^{n} \lambda_i b_i + \sum_{j=1}^{r} \mu_j a_j = \sum_{i=1}^{n} \rho_i b_i.$$

Also gilt

$$\sum_{i=1}^{n} (\lambda_i - \rho_i) b_i + \sum_{j=1}^{r} \mu_j a_j = 0.$$

Da $b_1, \dots, b_n, a_1, \dots, a_r$ eine Basis von U ist, folgt

$$\lambda_i = \rho_i \quad \text{für alle } i, \qquad \mu_j = 0 \quad \text{für alle } j.$$

Außerdem gilt

$$\sum_{i=1}^{n} \rho_i b_i + \sum_{\ell=1}^{s} \nu_\ell c_\ell = 0.$$

Da $b_1, \dots, b_n, c_1, \dots, c_s$ eine Basis von W ist, folgt

$$\rho_i = 0 \quad \text{für alle } i, \qquad \nu_\ell = 0 \quad \text{für alle } \ell.$$

Damit sind auch alle $\lambda_i = 0$. Also ist das System linear unabhängig.

Damit ist

$$b_1, \dots, b_n, a_1, \dots, a_r, c_1, \dots, c_s$$

eine Basis von $U + W$. Also gilt

$$\dim(U + W) = n + r + s.$$

Andererseits gilt

$$\dim(U) = n + r, \qquad \dim(W) = n + s, \qquad \dim(U \cap W) = n.$$

Daraus folgt

$$\dim(U + W) + \dim(U \cap W) = (n + r + s) + n = (n + r) + (n + s) = \dim(U) + \dim(W). \qquad \square$$

Beispiel 3.3.25. In $\mathbb{R}^3$ seien

$$U = \operatorname{Span}(e_1, e_2), \qquad W = \operatorname{Span}(e_2, e_3).$$

Dann ist

$$U \cap W = \operatorname{Span}(e_2), \qquad U + W = \mathbb{R}^3.$$

Die Dimensionsformel lautet hier

$$3 + 1 = 2 + 2.$$

Definition 3.3.26 (Direkte Summe)**.** Seien $U, W \subseteq V$ Untervektorräume. Die Summe $U + W$ heißt *direkt*, wenn

$$U \cap W = \{0\}$$

gilt. In diesem Fall schreiben wir

$$U \oplus W$$

statt $U + W$.

Lemma 3.3.27 (Charakterisierung direkter Summen)**.** *Seien $U, W \subseteq V$ Untervektorräume. Dann sind äquivalent:*

1. *Es gilt $U \cap W = \{0\}$.*
2. *Jeder Vektor $v \in U + W$ hat genau eine Darstellung*

$$v = u + w$$

mit $u \in U$ und $w \in W$.

Beweis. Angenommen, $U \cap W = \{0\}$. Sei

$$v = u + w = u' + w'$$

mit $u, u' \in U$ und $w, w' \in W$. Dann gilt

$$u - u' = w' - w.$$

Die linke Seite liegt in U, die rechte Seite liegt in W. Also liegt dieser Vektor in $U \cap W$. Daher ist

$$u - u' = 0.$$

Also ist $u = u'$. Dann folgt auch $w = w'$. Die Darstellung ist also eindeutig.

Umgekehrt nehmen wir an, dass jedes Element von $U + W$ eine eindeutige Darstellung hat. Sei $x \in U \cap W$. Dann gelten

$$x = x + 0 = 0 + x.$$

Beide Darstellungen sind Darstellungen von x als Summe eines Vektors aus U und eines Vektors aus W. Wegen der Eindeutigkeit folgt $x = 0$. Also ist $U \cap W = \{0\}$. □

Korollar 3.3.28 (Dimension einer direkten Summe)**.** *Seien $U, W \subseteq V$ endlich dimensionale Untervektorräume. Ist die Summe $U + W$ direkt, dann gilt*

$$\dim(U \oplus W) = \dim(U) + \dim(W).$$

Beweis. Nach der Dimensionsformel gilt

$$\dim(U + W) + \dim(U \cap W) = \dim(U) + \dim(W).$$

Da die Summe direkt ist, gilt

$$U \cap W = \{0\}.$$

Also ist $\dim(U \cap W) = 0$. Damit folgt die Behauptung. □

Beispiel 3.3.29. In $\mathbb{R}^2$ gilt

$$\mathbb{R}^2 = \text{Span}(e_1) \oplus \text{Span}(e_2).$$

Denn jeder Vektor (x, y) hat genau die Darstellung

$$(x, y) = xe_1 + ye_2.$$

Definition 3.3.30 (Komplement)**.** Seien $U, W \subseteq V$ Untervektorräume. Wir nennen W ein *Komplement* von U in V, wenn

$$V = U \oplus W$$

gilt.

Bemerkung 3.3.31 (Vektorraum-Komplemente sind keine Mengenkomplemente)**.** Ein Komplement von U in V ist ein Untervektorraum $W \subseteq V$ mit

$$V = U \oplus W.$$

Das ist nicht dasselbe wie das Mengenkomplement

$$V \setminus U.$$

Das Mengenkomplement ist im Allgemeinen kein Untervektorraum. Insbesondere enthält es nicht einmal den Nullvektor, sobald U ein Untervektorraum ist.

Außerdem sind Vektorraum-Komplemente im Allgemeinen nicht eindeutig.

Beispiel 3.3.32 (Komplemente sind nicht eindeutig)**.** In $\mathbb{R}^2$ sei

$$U = \text{Span}(e_1).$$

Dann sind sowohl

$$W_1 = \text{Span}(e_2)$$

als auch

$$W_2 = \text{Span}(e_1 + e_2)$$

Komplemente von U in $\mathbb{R}^2$. Also besitzt U nicht nur ein einziges Komplement.

Theorem 3.3.33 (Existenz eines Komplements)**.** *Sei V ein endlich dimensionaler k-Vektorraum. Dann gilt:*

1. *Jeder Untervektorraum $U \subseteq V$ besitzt mindestens ein Komplement.*
2. *Ist W ein Komplement von U in V, dann gilt*

$$\dim(W) = \dim(V) - \dim(U).$$

Beweis. Zuerst zeigen wir die Existenz. Sei

$$u_1, \dots, u_r$$

eine Basis von U. Nach dem Basisergänzungssatz können wir diese Basis zu einer Basis von V ergänzen. Es gibt also Vektoren

$$w_1, \dots, w_s \in V$$

sodass

$$u_1, \dots, u_r, w_1, \dots, w_s$$

eine Basis von V ist.

Wir setzen

$$W := \operatorname{Span}(w_1, \dots, w_s).$$

Dann gilt

$$V = U + W,$$

denn jeder Vektor aus V ist eine Linearkombination der Basisvektoren

$$u_1, \dots, u_r, w_1, \dots, w_s.$$

Die Anteile mit den u_i liegen in U, die Anteile mit den w_j liegen in W.

Außerdem gilt

$$U \cap W = \{0\}.$$

Denn sei $x \in U \cap W$. Dann lässt sich x einerseits als Linearkombination der u_i schreiben, andererseits als Linearkombination der w_j. Subtrahieren wir diese beiden Darstellungen, so erhalten wir eine lineare Relation zwischen den Basisvektoren

$$u_1, \dots, u_r, w_1, \dots, w_s.$$

Da diese Vektoren linear unabhängig sind, müssen alle Koeffizienten 0 sein. Also ist $x = 0$.

Damit gilt

$$V = U \oplus W.$$

Also ist W ein Komplement von U.

Sei nun umgekehrt W ein beliebiges Komplement von U in V. Dann gilt

$$V = U \oplus W.$$

Nach Korollar 3.3.28 folgt

$$\dim(V) = \dim(U) + \dim(W).$$

Also gilt

$$\dim(W) = \dim(V) - \dim(U).$$

□

Kapitel 4

Lineare Abbildungen

4.1 Definition

Sei k ein Körper. Seien V und W zwei k-Vektorräume.

Definition 4.1.1 (Lineare Abbildung)**.** Eine Abbildung

$$f : V \to W$$

heißt *linear*, wenn für alle $v, w \in V$ und alle $\lambda \in k$ gilt:

$$f(v + w) = f(v) + f(w)$$

und

$$f(\lambda v) = \lambda f(v).$$

Bemerkung 4.1.2 (Vergleich mit Gruppenhomomorphismen)**.** Ein Gruppenhomomorphismus ist eine Abbildung, die mit der Gruppenverknüpfung verträglich ist.

Ein Vektorraum besitzt mehr Struktur als nur seine Addition. Er besitzt zusätzlich die Skalarmultiplikation. Daher muss eine lineare Abbildung zwei Dinge respektieren:

1. Sie respektiert Addition. Das heißt:

   $$f(v + w) = f(v) + f(w).$$

   Als Abbildung

   $$(V, +) \to (W, +)$$

   ist sie also ein Gruppenhomomorphismus.

2. Sie respektiert Skalarmultiplikation. Das heißt:

   $$f(\lambda v) = \lambda f(v).$$

Lineare Abbildungen sind also die Homomorphismen von Vektorräumen. Sie sind genau die Abbildungen, die die lineare Struktur erhalten.

Bemerkung 4.1.3 (Lineare Abbildungen erhalten Linearkombinationen)**.** Die wichtigste Bedeutung der Definition ist: Lineare Abbildungen vertragen sich mit Linearkombinationen.

Man darf also lineare Abbildungen in Linearkombinationen hineinziehen:

$$f(\lambda_1 v_1 + \cdots + \lambda_n v_n) = \lambda_1 f(v_1) + \cdots + \lambda_n f(v_n).$$

Dies beweisen wir gleich. Diese Eigenschaft ist der Grund, warum lineare Abbildungen in der linearen Algebra so nützlich sind.

Beispiel 4.1.4 (Grundbeispiele)**.**

1. Die Identitätsabbildung
$$\mathrm{Id}_V : V \to V, \quad v \mapsto v$$
ist linear.

2. Die Nullabbildung
$$0 : V \to W, \quad v \mapsto 0$$
ist linear.

3. Die Abbildung
$$f : \mathbb{R}^2 \to \mathbb{R}^3, \quad (x, y) \mapsto (y, x - 3y, 2x + y)$$
ist linear. Alle Komponenten sind lineare Ausdrücke in x und y.

4. Sei P_n der $\mathbb{R}$-Vektorraum der Polynome vom Grad höchstens n. Die Ableitung
$$D : P_n \to P_{n-1}, \quad p \mapsto p'$$
ist linear, denn
$$(\lambda p + \mu q)' = \lambda p' + \mu q'.$$

5. Für $a \in \mathbb{R}$ ist die Auswertungsabbildung
$$\mathrm{ev}_a : P_n \to \mathbb{R}, \quad p \mapsto p(a)$$
linear, denn
$$(\lambda p + \mu q)(a) = \lambda p(a) + \mu q(a).$$

6. Die Abbildung
$$I : P_n \to \mathbb{R}, \quad p \mapsto \int_0^1 p(x)\,dx$$
ist linear. Das ist genau die Linearität des Integrals:
$$\int_0^1 (\lambda p(x) + \mu q(x))\,dx = \lambda \int_0^1 p(x)\,dx + \mu \int_0^1 q(x)\,dx.$$

7. Die endliche Fouriertransformation ist linear. Setze
$$\omega := e^{-2\pi i/n}.$$
Wir definieren
$$\mathscr{F} : \mathbb{C}^n \to \mathbb{C}^n$$

durch

$$(\mathscr{F}x)_j := \sum_{\ell=0}^{n-1} x_\ell \omega^{j\ell} \quad \text{für } j = 0, \dots, n-1.$$

Dann gilt

$$\mathscr{F}(\lambda x + \mu y) = \lambda \mathscr{F}(x) + \mu \mathscr{F}(y),$$

weil jede Komponente durch eine Summe linearer Terme gegeben ist. Die Fouriertransformation ist also kein Sondertrick, sondern ein wichtiges Beispiel einer linearen Abbildung.

Leitbeispiel 4.1.5 (Der Schattenwurf)**.** Dieses Beispiel begleitet uns durch das ganze Kapitel:

Die Sonne steht am Himmel und schickt parallele Strahlen — genauer: Sie ist so weit entfernt, dass wir ihre Strahlen guten Gewissens als parallel idealisieren dürfen. Ein Gegenstand im Raum wirft einen Schatten auf den ebenen Boden. Wir legen den Ursprung auf den Boden und beschreiben Punkte des Raumes durch ihre Ortsvektoren $(x, y, z) \in \mathbb{R}^3$, wobei z die Höhe über dem Boden ist. Die Bodenebene ist dann $\{(x, y, 0) \mid x, y \in \mathbb{R}\}$.

Die Sonnenstrahlen laufen alle in einer festen Richtung d. Wir wählen die Beleuchtung

$$d = (1, 1, -1),$$

also schräg von oben. Der Schatten eines Punktes p ist der Punkt, an dem der Strahl $p + td$ den Boden trifft. Aus der Höhengleichung $z + t \cdot (-1) = 0$ folgt $t = z$, und Einsetzen liefert die *Schattenabbildung*

$$P : \mathbb{R}^3 \to \mathbb{R}^3, \qquad P(x, y, z) = (x + z,\ y + z,\ 0).$$

(Für Punkte unterhalb des Bodens, also $z < 0$, rechnet die Formel unbeirrt weiter — der Mathematik ist gleichgültig, dass echtes Licht nur von oben kommt.)

P ist linear — und das kann man sehen. Verschiebt man den Gegenstand um einen Vektor v, so verschiebt sich sein Schatten um $P(v)$; verschiebt man um $v + w$, so wandert der Schatten um $P(v) + P(w)$. Der Schatten einer Summe ist die Summe der Schatten, der Schatten des Doppelten ist das Doppelte des Schattens. Formal steht das schon in der Formel: jede Komponente von $P(x, y, z)$ ist ein linearer Ausdruck in x, y, z.

Schatten eines Schattens. Ein Punkt, der schon auf dem Boden liegt, ist sein eigener Schatten. Also ändert ein zweiter Wurf nichts mehr:

$$P\big(P(x, y, z)\big) = P(x + z,\ y + z,\ 0) = (x + z,\ y + z,\ 0) = P(x, y, z).$$

Es gilt $P \circ P = P$. Eine lineare Abbildung mit dieser Eigenschaft heißt *Projektion* — auch die mathematische Begriffswahl folgt hier dem Beispiel des Schattenwurfs.

Zwei Fragen drängen sich auf, und sie sind die Leitfragen dieses Kapitels:

- *Welche Information verliert der Schatten?* Welche Punkte wirft die Sonne auf denselben Fleck, ja sogar auf den Ursprung? Das wird der *Kern* von P sein.
- *Was erreicht der Schatten?* Welche Flecken des Bodens kommen überhaupt als Schatten vor? Das wird das *Bild* von P sein.

Wir nehmen die Antworten vorweg, damit man beim Lesen darauf wartet: Der Kern ist genau die Sonnenrichtung $\operatorname{Span}(1, 1, -1)$, denn Punkte auf ein und demselben Strahl haben denselben Schatten. Das Bild ist die ganze Bodenebene. Und die sogenannte Rangformel wird sagen:

$$\underbrace{3}_{\dim \mathbb{R}^3} = \underbrace{1}_{\text{Sonnenrichtung}} + \underbrace{2}_{\text{Bodenebene}}.$$

Die drei Dimensionen des Raumes zerfallen in „eine Richtung, die der Schatten platt drückt“ und „zwei Richtungen, die er behält“.

Bemerkung 4.1.6 (Ein schneller Nicht-Beispiel-Test)**.** Eine lineare Abbildung muss den Nullvektor auf den Nullvektor abbilden. Daher ist etwa

$$f : \mathbb{R}^2 \to \mathbb{R}^2, \quad (x, y) \mapsto (x + 1, y)$$

nicht linear. Denn

$$f(0, 0) = (1, 0) \neq (0, 0).$$

Translationen sind also im Allgemeinen nicht linear. Das widerspricht nicht dem Schattenbild von eben: Dort war das Verschieben des Gegenstands nur ein Mittel, um $P(v + w) = P(v) + P(w)$ zu *sehen* — die Schattenabbildung selbst verschiebt nichts.

Lemma 4.1.7 (Grundregeln für lineare Abbildungen)**.** *Sei $f : V \to W$ eine Abbildung. Dann gilt:*

1. *Die Definition von Linearität ist äquivalent zu der folgenden Bedingung: Für alle $v, w \in V$ und alle $\lambda, \mu \in k$ gilt*
$$f(\lambda v + \mu w) = \lambda f(v) + \mu f(w).$$

2. *Ist f linear, dann gilt*
$$f(0) = 0$$
und
$$f(-v) = -f(v)$$
für alle $v \in V$.

3. *Ist f linear, dann gilt für alle $v_1, \dots, v_n \in V$ und alle $\lambda_1, \dots, \lambda_n \in k$:*
$$f\left(\sum_{i=1}^{n} \lambda_i v_i\right) = \sum_{i=1}^{n} \lambda_i f(v_i).$$

4. *Sind*
$$f : V \to W \quad \textit{und} \quad g : W \to U$$
linear, dann ist auch
$$g \circ f : V \to U$$
linear. Außerdem ist
$$\mathrm{Id}_V : V \to V$$
linear.

1. *Beweis.* Angenommen, f ist linear. Dann gilt
$$f(\lambda v + \mu w) = f(\lambda v) + f(\mu w) = \lambda f(v) + \mu f(w).$$
Umgekehrt nehmen wir an, dass
$$f(\lambda v + \mu w) = \lambda f(v) + \mu f(w)$$
für alle $v, w \in V$ und alle $\lambda, \mu \in k$ gilt. Mit $\lambda = \mu = 1$ erhalten wir
$$f(v + w) = f(v) + f(w).$$
Mit $\mu = 0$ erhalten wir
$$f(\lambda v) = \lambda f(v) + 0 f(w) = \lambda f(v).$$
Also ist f linear.

2. Ist f linear, dann ist insbesondere

$$f : (V, +) \to (W, +)$$

ein Gruppenhomomorphismus zwischen den additiven Gruppen. Nach den Grundregeln für Gruppenhomomorphismen erhalten Homomorphismen neutrale Elemente und Inverse. Also gilt

$$f(0) = 0$$

und

$$f(-v) = -f(v).$$

3. Die Idee ist: Wir ziehen f Schritt für Schritt durch die Summe.

Wir beweisen die Aussage per Induktion über n. Für $n = 1$ ist die Aussage genau

$$f(\lambda_1 v_1) = \lambda_1 f(v_1),$$

also die Verträglichkeit mit Skalarmultiplikation.

Sei die Aussage nun für ein $n \geq 1$ bewiesen. Dann gilt

$$\begin{aligned} f\left(\sum_{i=1}^{n+1} \lambda_i v_i\right) &= f\left(\left(\sum_{i=1}^{n} \lambda_i v_i\right) + \lambda_{n+1} v_{n+1}\right) \\ &= f\left(\sum_{i=1}^{n} \lambda_i v_i\right) + f(\lambda_{n+1} v_{n+1}) \\ &= \sum_{i=1}^{n} \lambda_i f(v_i) + \lambda_{n+1} f(v_{n+1}) \\ &= \sum_{i=1}^{n+1} \lambda_i f(v_i). \end{aligned}$$

Damit ist die Aussage für alle n bewiesen.

4. Seien $v, w \in V$ und $\lambda, \mu \in k$. Da f linear ist, gilt

$$f(\lambda v + \mu w) = \lambda f(v) + \mu f(w).$$

Da g linear ist, folgt

$$(g \circ f)(\lambda v + \mu w) = g(\lambda f(v) + \mu f(w)) = \lambda g(f(v)) + \mu g(f(w)).$$

Also ist $g \circ f$ linear.

Die Linearität von Id_V ist unmittelbar:

$$\mathrm{Id}_V(\lambda v + \mu w) = \lambda v + \mu w = \lambda \mathrm{Id}_V(v) + \mu \mathrm{Id}_V(w). \qquad \square$$

Definition 4.1.8 (Isomorphismus von Vektorräumen)**.** Seien V und W zwei k-Vektorräume. Eine Abbildung

$$f : V \to W$$

heißt ein *Isomorphismus*, wenn f bijektiv ist und sowohl

$$f : V \to W$$

als auch

$$f^{-1} : W \to V$$

linear sind.

Gibt es einen Isomorphismus $V \to W$, dann heißen V und W *isomorph*. Wir schreiben dann

$$V \cong W.$$

Lemma 4.1.9 (Bijektive lineare Abbildungen sind Isomorphismen)**.** *Seien V und W zwei k-Vektorräume. Ist*

$$f : V \to W$$

bijektiv und linear, dann ist f ein Isomorphismus.

Beweis. Nach Voraussetzung ist f bijektiv und linear. Es bleibt nur zu zeigen, dass

$$f^{-1} : W \to V$$

linear ist.

Seien $a, b \in W$ und $\lambda, \mu \in k$. Setze

$$v := f^{-1}(a) \quad \text{und} \quad w := f^{-1}(b).$$

Dann gilt

$$f(v) = a \quad \text{und} \quad f(w) = b.$$

Da f linear ist, erhalten wir

$$f(\lambda v + \mu w) = \lambda f(v) + \mu f(w) = \lambda a + \mu b.$$

Wir wenden f^{-1} an und erhalten

$$f^{-1}(\lambda a + \mu b) = \lambda v + \mu w.$$

Also gilt

$$f^{-1}(\lambda a + \mu b) = \lambda f^{-1}(a) + \mu f^{-1}(b).$$

Damit ist f^{-1} linear. □

4.2 Matrizen und die von ihnen induzierten linearen Abbildungen

Wir führen Matrizen nun als Rechenform für lineare Abbildungen ein.

Definition 4.2.1 (Matrix)**.** Seien $m, n \geq 1$. Eine *$m \times n$-Matrix* mit Einträgen in k ist ein rechteckiges Schema

$$A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1} & A_{m2} & \cdots & A_{mn} \end{pmatrix}$$

mit $A_{ij} \in k$.

Der Eintrag A_{ij} steht in der i-ten Zeile und in der j-ten Spalte. Die Menge aller $m \times n$-Matrizen mit Einträgen in k schreiben wir als

$$k^{m \times n}.$$

Definition 4.2.2 (Matrixaddition und Skalarmultiplikation)**.** Seien $A, B \in k^{m\times n}$ und $\lambda \in k$. Dann definieren wir

$$(A + B)_{ij} := A_{ij} + B_{ij}$$

und

$$(\lambda A)_{ij} := \lambda A_{ij}.$$

Also werden Matrizen gleicher Größe komponentenweise addiert und skaliert.

Definition 4.2.3 (Matrixmultiplikation)**.** Seien

$$A \in k^{m\times n} \quad \text{und} \quad B \in k^{n\times p}.$$

Dann ist das Produkt

$$AB \in k^{m\times p}$$

definiert durch

$$(AB)_{i\ell} := \sum_{j=1}^{n} A_{ij}B_{j\ell}.$$

Das Produkt ist also genau dann definiert, wenn die Anzahl der Spalten von A gleich der Anzahl der Zeilen von B ist.

Beispiel 4.2.4. Es gilt

$$\begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}\begin{pmatrix} 0 & 2 & 4 \\ 1 & 3 & 5 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 4 \\ 1 & 9 & 17 \end{pmatrix}.$$

Denn der Eintrag unten rechts ist zum Beispiel

$$3 \cdot 4 + 1 \cdot 5 = 17.$$

Theorem 4.2.5 (Rechenregeln für Matrizen)**.** *Matrixmultiplikation ist assoziativ, sobald alle Produkte definiert sind. Das heißt:*

$$(AB)C = A(BC).$$

Außerdem ist Matrixmultiplikation distributiv mit Matrixaddition:

$$A(B + C) = AB + AC$$

und

$$(A + B)C = AC + BC.$$

Die Beweise sind direkte Rechnungen mit der Definition der Einträge. Wir verwenden diese Regeln als Rechenregeln für Matrizen.

Bemerkung 4.2.6 (Vektoren als Spaltenmatrizen)**.** Ab jetzt betrachten wir Vektoren in k^n als Spaltenvektoren:

$$v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}.$$

Das ist eine $n \times 1$-Matrix. Ist

$$A \in k^{m\times n},$$

dann ist

$$Av$$

definiert und ist eine $m \times 1$-Matrix, also ein Vektor aus k^m.

Definition 4.2.7 (Die lineare Abbildung einer Matrix)**.** Sei

$$A \in k^{m \times n}.$$

Dann definieren wir

$$L_A : k^n \to k^m, \quad v \mapsto Av.$$

Lemma 4.2.8 (Matrizen definieren lineare Abbildungen)**.** *Sei*

$$A \in k^{m \times n}.$$

Dann ist

$$L_A : k^n \to k^m, \quad v \mapsto Av$$

linear.

Beweis. Seien $v, w \in k^n$ und $\lambda, \mu \in k$. Dann gilt nach den Distributivgesetzen für Matrizen

$$A(\lambda v + \mu w) = \lambda Av + \mu Aw.$$

Also gilt

$$L_A(\lambda v + \mu w) = \lambda L_A(v) + \mu L_A(w).$$

Damit ist L_A linear. □

4.3 Lineare Abbildungen sind durch Erzeuger bestimmt

Theorem 4.3.1 (Eindeutigkeit auf einem Erzeugendensystem)**.** *Seien*

$$f, g : V \to W$$

lineare Abbildungen. Sei außerdem

$$v_1, \dots, v_n$$

ein Erzeugendensystem von V. Gilt

$$f(v_i) = g(v_i)$$

für alle $i = 1, \dots, n$, dann gilt

$$f = g.$$

Beweis. Sei $v \in V$ beliebig. Da $v_1, \dots, v_n$ ein Erzeugendensystem von V ist, gibt es Skalare $\lambda_1, \dots, \lambda_n \in k$ mit

$$v = \sum_{i=1}^{n} \lambda_i v_i.$$

Da f linear ist, gilt

$$f(v) = \sum_{i=1}^{n} \lambda_i f(v_i).$$

Da g linear ist, gilt

$$g(v) = \sum_{i=1}^{n} \lambda_i g(v_i).$$

Wegen

$$f(v_i) = g(v_i)$$

für alle i sind diese beiden Summen gleich. Also gilt

$$f(v) = g(v).$$

Da v beliebig war, folgt

$$f = g.$$ □

Korollar 4.3.2 (Test auf einer Basis)**.** *Seien*

$$f, g : V \to W$$

lineare Abbildungen. Sei

$$b_1, \dots, b_n$$

eine Basis von V. Dann gilt:

$$f = g \quad \Longleftrightarrow \quad f(b_i) = g(b_i) \text{ für alle } i = 1, \dots, n.$$

Beweis. Eine Basis ist insbesondere ein Erzeugendensystem. Daher folgt die Richtung von rechts nach links aus dem vorherigen Satz. Die andere Richtung ist unmittelbar aus der Definition von Gleichheit von Abbildungen. □

Bemerkung 4.3.3. Dieses Korollar ist einer der wichtigsten praktischen Punkte dieses Abschnitts.

Um zwei lineare Abbildungen aus einem endlich dimensionalen Vektorraum zu vergleichen, muss man nicht alle Vektoren testen. Es reicht, die endlich vielen Basisvektoren zu testen.

Der Beweis ist sehr einfach, aber die Aussage ist sehr stark.

4.4 Jede lineare Abbildung zwischen Standardräumen entspricht einer Matrix

Sei

$$e_1, \dots, e_n$$

die Standardbasis von k^n. Also ist e_j der Spaltenvektor, dessen j-ter Eintrag 1 ist und dessen übrige Einträge 0 sind.

Lemma 4.4.1 (Spalten einer Matrix)**.** *Sei*

$$A \in k^{m \times n}.$$

Dann ist

$$Ae_j$$

die j-te Spalte von A.

Beweis. Der i-te Eintrag von Ae_j ist

$$(Ae_j)_i = \sum_{\ell=1}^{n} A_{i\ell}(e_j)_\ell.$$

Alle Einträge von e_j sind 0, außer der j-te Eintrag. Dort steht 1. Daher bleibt nur ein Summand übrig:

$$(Ae_j)_i = A_{ij}.$$

Das ist genau der i-te Eintrag der j-ten Spalte von A. □

Theorem 4.4.2 (Lineare Abbildungen $k^n \to k^m$ entsprechen Matrizen)**.** *Sei*

$$f : k^n \to k^m$$

linear. Dann gibt es genau eine Matrix

$$A \in k^{m \times n}$$

mit

$$f = L_A.$$

Die j-te Spalte von A ist dabei genau

$$f(e_j).$$

Beweis. Wir konstruieren die Matrix A durch ihre Spalten. Die j-te Spalte von A soll sein:

$$f(e_j).$$

Also setzen wir

$$A = \begin{pmatrix} | & | & & | \\ f(e_1) & f(e_2) & \cdots & f(e_n) \\ | & | & & | \end{pmatrix}.$$

Nach Lemma 4.4.1 gilt dann

$$L_A(e_j) = Ae_j = f(e_j)$$

für alle $j = 1, \dots, n$.

Die Vektoren

$$e_1, \dots, e_n$$

bilden ein Erzeugendensystem von k^n. Nach Theorem 4.3.1 folgt

$$L_A = f.$$

Die Matrix ist eindeutig. Denn wenn auch

$$f = L_B$$

gilt, dann muss für jedes j gelten:

$$Be_j = L_B(e_j) = f(e_j).$$

Also ist die j-te Spalte von B gleich $f(e_j)$. Damit sind alle Spalten von B festgelegt. Also ist $B = A$. □

Bemerkung 4.4.3 (Die Spalten sind die Bilder der Basisvektoren)**.** Die Matrix einer linearen Abbildung

$$f : k^n \to k^m$$

ist nicht geheimnisvoll.

Ihre Spalten sind einfach die Bilder der Standardbasisvektoren:

$$A = \begin{pmatrix} | & | & & | \\ f(e_1) & f(e_2) & \cdots & f(e_n) \\ | & | & & | \end{pmatrix}.$$

Wenn man eine Matrix anschaut, dann kann man also direkt ablesen, wohin die zugehörige lineare Abbildung die Basisvektoren schickt.

Beispiel 4.4.4 (Eine Rotation in der Ebene)**.** Wir betrachten die Rotation

$$R_\theta : \mathbb{R}^2 \to \mathbb{R}^2$$

um den Winkel θ gegen den Uhrzeigersinn.

Wir müssen nur wissen, wohin die Standardbasisvektoren gehen. Der erste Basisvektor wird zu

$$e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \longmapsto \quad \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}.$$

Der zweite Basisvektor wird zu

$$e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \longmapsto \quad \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix}.$$

Also ist die Matrix von R_θ

$$A_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Denn die Spalten sind genau die Bilder von e_1 und e_2.

Damit ist die Matrix einer Rotation nicht mysteriös. Sie hält nur fest, wohin die beiden Basisrichtungen gedreht werden.

Leitbeispiel 4.4.5 (Die Matrix des Schattenwurfs)**.** Auch das Leitbeispiel Leitbeispiel 4.1.5 bekommt jetzt seine Matrix. Wir lesen die Spalten als Schatten der drei Einheitspunkte ab:

$$P(e_1) = (1, 0, 0), \qquad P(e_2) = (0, 1, 0), \qquad P(e_3) = (1, 1, 0).$$

Ein Punkt auf dem Boden (e_1 und e_2) ist sein eigener Schatten; der Punkt e_3 in Höhe 1 wird von der schrägen Sonne auf $(1, 1, 0)$ verschoben. Also ist

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

Die letzte Zeile ist Null, weil jeder Schatten die Höhe 0 hat. In der dritten Spalte $(1, 1, 0)$ steckt die Sonnenrichtung: Ihre ersten beiden Einträge sind die waagrechten Komponenten von $d = (1, 1, -1)$ und sagen, um wie viel eine Höheneinheit den Schatten zur Seite schiebt. (Die ganze Richtung d kann in der Spalte nicht stehen — die dritte Komponente jedes Schattens ist ja 0.)

4.5 Isomorphismen, Kern und Bild

Theorem 4.5.1 (Isomorphismen bilden Basen auf Basen ab)**.** *Sei*

$$f : V \to W$$

ein Isomorphismus. Ist

$$b_1, \dots, b_n$$

eine Basis von V, dann ist

$$f(b_1), \dots, f(b_n)$$

eine Basis von W.

Beweis. Wir zeigen zuerst, dass $f(b_1), \dots, f(b_n)$ ein Erzeugendensystem von W ist.
Sei $w \in W$. Da f surjektiv ist, gibt es ein $v \in V$ mit

$$f(v) = w.$$

Da $b_1, \dots, b_n$ eine Basis von V ist, gibt es Skalare $\lambda_1, \dots, \lambda_n \in k$ mit

$$v = \sum_{i=1}^{n} \lambda_i b_i.$$

Wegen Linearität gilt

$$w = f(v) = f\left(\sum_{i=1}^{n} \lambda_i b_i\right) = \sum_{i=1}^{n} \lambda_i f(b_i).$$

Also erzeugen $f(b_1), \dots, f(b_n)$ den Vektorraum W.
Jetzt zeigen wir lineare Unabhängigkeit. Angenommen,

$$\sum_{i=1}^{n} \lambda_i f(b_i) = 0.$$

Dann gilt wegen Linearität

$$f\left(\sum_{i=1}^{n} \lambda_i b_i\right) = 0.$$

Außerdem ist

$$f(0) = 0.$$

Da f injektiv ist, folgt

$$\sum_{i=1}^{n} \lambda_i b_i = 0.$$

Da $b_1, \dots, b_n$ linear unabhängig sind, folgt

$$\lambda_1 = \dots = \lambda_n = 0.$$

Also sind $f(b_1), \dots, f(b_n)$ linear unabhängig.
Damit bilden $f(b_1), \dots, f(b_n)$ eine Basis von W. □

Korollar 4.5.2 (Isomorphe Vektorräume haben gleiche Dimension)**.** *Seien V und W endlich dimensionale k-Vektorräume. Ist*

$$V \cong W,$$

dann gilt

$$\dim(V) = \dim(W).$$

Beweis. Sei

$$f : V \to W$$

ein Isomorphismus. Sei

$$b_1, \dots, b_n$$

eine Basis von V. Dann ist nach Theorem 4.5.1

$$f(b_1), \dots, f(b_n)$$

eine Basis von W. Also haben V und W Basen gleicher Länge. Daher gilt

$$\dim(V) = \dim(W).$$ □

Definition 4.5.3 (Kern und Bild)**.** Sei

$$f : V \to W$$

eine lineare Abbildung.

Der *Kern* von f ist

$$\mathrm{Kern}(f) := \{v \in V \mid f(v) = 0\}.$$

Das *Bild* von f ist

$$\mathrm{Bild}(f) := \{f(v) \mid v \in V\} \subseteq W.$$

Leitbeispiel 4.5.4 (Der Schattenwurf: Kern und Bild)**.** Jetzt lösen wir die beiden Leitfragen aus Leitbeispiel 4.1.5.

Der Kern ist die Sonnenrichtung. Ein Punkt liegt im Kern, wenn sein Schatten der Ursprung ist:

$$P(x, y, z) = (x + z,\ y + z,\ 0) = (0, 0, 0) \iff x = -z \text{ und } y = -z.$$

Das sind genau die Vielfachen $(x, y, z) = z \cdot (-1, -1, 1)$, also

$$\mathrm{Kern}(P) = \mathrm{Span}(1, 1, -1) = \mathrm{Span}(d)$$

(es gilt $\mathrm{Span}(-1, -1, 1) = \mathrm{Span}(1, 1, -1)$, denn Vielfache — auch mit -1 — ändern den Spann nicht). Der Kern ist die Gerade der Sonnenstrahlen durch den Ursprung. Das ist anschaulich zwingend: Alle Punkte auf *einem* Strahl haben denselben Schatten, die Abbildung kann sie nicht auseinanderhalten. Was im Kern verschwindet, ist die Information „wie weit entlang des Strahls“ — genau die Information, die der Schatten wegwirft.

Das Bild ist der ganze Boden. Jeder Bodenpunkt $(u, v, 0)$ ist ein Schatten, etwa der von sich selbst: $P(u, v, 0) = (u, v, 0)$. Also

$$\mathrm{Bild}(P) = \{(u, v, 0) \mid u, v \in \mathbb{R}\},$$

die Bodenebene, ein zweidimensionaler Untervektorraum.

Insbesondere ist P *nicht* injektiv (der Kern ist größer als $\{0\}$) und *nicht* surjektiv als Abbildung nach $\mathbb{R}^3$ (das Bild ist nur eine Ebene). Beides sieht man dem Schatten sofort an.

Beispiel 4.5.5 (Die Messstation: ein riesiger Kern)**.** Ein zweites Beispiel zeigt, dass der Kern der eigentliche Ort des *Informationsverlusts* ist.

Wir besuchen die Messstation aus Leitbeispiel 3.3.6 wieder. Im Signalraum S (Leitbeispiel 3.1.5) der endlichen Überlagerungen reiner Sinuswellen liest die Station von jedem Signal genau drei Zahlen ab: die Stärken $\lambda_1, \lambda_2, \lambda_3$, mit denen ihre drei Detektorfrequenzen c_1, c_2, c_3 darin vertreten sind. Das Messen ist also die Abbildung

$$A : S \to \mathbb{R}^3, \qquad A(v) = (\lambda_1, \lambda_2, \lambda_3).$$

Kommt eine Detektorfrequenz im Signal gar nicht vor, so zeigt ihr Detektor 0 an — er schlägt einfach nicht aus. Damit ist A auf ganz S definiert, und man kann konkret rechnen: Ist etwa c_5 keine der drei Detektorfrequenzen, dann ist

$$A(7s_{c_1} - s_{c_5}) = (7,\ 0,\ 0).$$

Diese Abbildung ist *linear*: Überlagert man zwei Signale, so addieren sich ihre (eindeutigen) Frequenzanteile, also addieren sich die Anzeigen; verstärkt man ein Signal um einen Faktor, verstärkt sich die Anzeige um denselben Faktor.

A bildet einen riesigen Raum auf nur drei Zahlen ab — das lässt einen gewaltigen Kern erwarten, und wir können ihn genau angeben: Im Kern liegen genau die Signale, in denen keine der drei Detektorfrequenzen vorkommt, etwa jede reine Welle s_c mit $c \notin \{c_1, c_2, c_3\}$ und alle Überlagerungen solcher Wellen. Für die Station ist dieser ganze Teilraum *Stille*. Zwei Signale v_1, v_2 klingen für die Station *genau dann* gleich, wenn

$$A(v_1) = A(v_2), \quad \text{also} \quad v_1 - v_2 \in \operatorname{Kern}(A)$$

(denn $A(v_1) - A(v_2) = A(v_1 - v_2)$, weil A linear ist — genau diese Rechnung trägt gleich auch das Injektivitätslemma unten). Der Kern ist genau der Teil des Funkverkehrs, den die Station prinzipiell nicht hören kann.

Bemerkung 4.5.6 (Vom Detektor zum Auge)**.** Unser eigenes Farbensehen funktioniert nach demselben Muster. Licht ist ein Gemisch aus Wellenlängen, und das Auge misst dieses Gemisch mit nur drei Zapfensorten — eine lineare Abbildung in den $\mathbb{R}^3$. Echte Zapfen haben, wie echte Detektoren, eine Bandbreite: Jede Zapfensorte bildet ihre Zahl als gewichtetes Integral über das Spektrum. Auch hier ist der Kern gewaltig. Zwei physikalisch völlig verschiedene Spektren können exakt gleich aussehen, wenn ihre Differenz im Kern liegt — Physiker und Maler kennen das als *Metamerie*.

Das macht bspw. RGB Monitore überhaupt erst möglich. Ein solcher Monitor — RGB steht für Rot-Grün-Blau — sendet z. B. kein gelbes Licht. Dennoch hat der Monitor kein Problem damit in unseren Augen den selben Effekt wie gelbes Licht auszulösen. Wir sehen Farben als gleich, die als rein physikalische Wellen völlig verschieden sind.

Lemma 4.5.7 (Kern und Bild sind Untervektorräume)**.** *Sei*

$$f : V \to W$$

eine lineare Abbildung. Dann ist

$$\operatorname{Kern}(f)$$

ein Untervektorraum von V, und

$$\operatorname{Bild}(f)$$

ist ein Untervektorraum von W.

Beweis. Zuerst zum Kern. Da $f(0) = 0$ gilt, liegt 0 in $\mathrm{Kern}(f)$.
Seien nun $v, w \in \mathrm{Kern}(f)$ und $\lambda, \mu \in k$. Dann gilt

$$f(\lambda v + \mu w) = \lambda f(v) + \mu f(w) = \lambda 0 + \mu 0 = 0.$$

Also liegt

$$\lambda v + \mu w$$

wieder in $\mathrm{Kern}(f)$. Nach dem Untervektorraumkriterium ist $\mathrm{Kern}(f)$ ein Untervektorraum von V.
Jetzt zum Bild. Da $f(0) = 0$ gilt, liegt 0 in $\mathrm{Bild}(f)$.
Seien nun $x, y \in \mathrm{Bild}(f)$ und $\lambda, \mu \in k$. Dann gibt es $v, w \in V$ mit

$$x = f(v) \quad \text{und} \quad y = f(w).$$

Also gilt

$$\lambda x + \mu y = \lambda f(v) + \mu f(w) = f(\lambda v + \mu w).$$

Daher liegt

$$\lambda x + \mu y$$

wieder in $\mathrm{Bild}(f)$. Nach dem Untervektorraumkriterium ist $\mathrm{Bild}(f)$ ein Untervektorraum von W. □

Lemma 4.5.8 (Injektivität und Kern)**.** *Sei*

$$f : V \to W$$

eine lineare Abbildung. Dann gilt:

$$f \textit{ ist injektiv} \quad \Longleftrightarrow \quad \mathrm{Kern}(f) = \{0\}.$$

Beweis. Angenommen, f ist injektiv. Ist $v \in \mathrm{Kern}(f)$, dann gilt

$$f(v) = 0 = f(0).$$

Da f injektiv ist, folgt

$$v = 0.$$

Also gilt

$$\mathrm{Kern}(f) = \{0\}.$$

Umgekehrt gelte nun

$$\mathrm{Kern}(f) = \{0\}.$$

Seien $v, w \in V$ mit

$$f(v) = f(w).$$

Dann gilt

$$f(v - w) = f(v) - f(w) = 0.$$

Also liegt $v - w$ in $\mathrm{Kern}(f)$. Daher ist

$$v - w = 0.$$

Also ist

$$v = w.$$

Damit ist f injektiv. □

Definition 4.5.9 (Rang)**.** Sei

$$f : V \to W$$

eine lineare Abbildung. Der *Rang* von f ist

$$\mathrm{Rang}(f) := \dim\left(\mathrm{Bild}(f)\right).$$

Theorem 4.5.10 (Rangformel)**.** *Seien V und W zwei k-Vektorräume. Sei*

$$f : V \to W$$

eine lineare Abbildung. Ist V endlich dimensional, dann gilt

$$\dim(V) = \dim\left(\mathrm{Kern}(f)\right) + \mathrm{Rang}(f).$$

Beweis. Da V endlich dimensional ist, hat der Untervektorraum $\mathrm{Kern}(f) \subseteq V$ ein Komplement. Sei also $U \subseteq V$ ein Komplement von $\mathrm{Kern}(f)$. Dann gilt

$$V = \mathrm{Kern}(f) \oplus U.$$

Daher gilt

$$\dim(V) = \dim\left(\mathrm{Kern}(f)\right) + \dim(U).$$

Es bleibt zu zeigen, dass

$$\dim(U) = \dim\left(\mathrm{Bild}(f)\right).$$

Wir betrachten die Einschränkung

$$f|_U : U \to \mathrm{Bild}(f).$$

Diese Abbildung ist linear.

Sie ist injektiv: Ist $u \in U$ und

$$f(u) = 0,$$

dann liegt u in $\mathrm{Kern}(f)$. Also liegt u in

$$U \cap \mathrm{Kern}(f).$$

Da die Summe direkt ist, ist

$$U \cap \mathrm{Kern}(f) = \{0\}.$$

Also ist

$$u = 0.$$

Nach Lemma 4.5.8 ist $f|_U$ injektiv.

Sie ist surjektiv auf $\mathrm{Bild}(f)$: Sei $y \in \mathrm{Bild}(f)$. Dann gibt es ein $v \in V$ mit

$$f(v) = y.$$

Da $V = \mathrm{Kern}(f) \oplus U$ gilt, gibt es $z \in \mathrm{Kern}(f)$ und $u \in U$ mit

$$v = z + u.$$

Dann gilt

$$y = f(v) = f(z + u) = f(z) + f(u) = 0 + f(u) = f(u).$$

Also liegt y im Bild von $f|_U$.

Damit ist

$$f|_U : U \to \text{Bild}(f)$$

ein Isomorphismus. Nach Korollar 4.5.2 gilt

$$\dim(U) = \dim\left(\text{Bild}(f)\right).$$

Also folgt

$$\dim(V) = \dim\left(\text{Kern}(f)\right) + \dim\left(\text{Bild}(f)\right) = \dim\left(\text{Kern}(f)\right) + \text{Rang}(f). \qquad \square$$

Bemerkung 4.5.11 (Was die Rangformel misst)**.** Die Rangformel zerlegt die Dimension des Definitionsbereichs:

$$\dim(V) = \underbrace{\dim\left(\text{Kern}(f)\right)}_{\text{geht auf } 0} + \underbrace{\text{Rang}(f)}_{\text{kommt im Bild an}}.$$

Sie sagt nicht, dass

$$\dim(W)$$

zerlegt wird. Der Zielraum W kann größer sein als das Bild.

Leitbeispiel 4.5.12 (Der Schattenwurf: die Rangformel im Hof)**.** Für die Schattenabbildung $P : \mathbb{R}^3 \to \mathbb{R}^3$ aus Leitbeispiel 4.1.5 haben wir alles beisammen:

$$\text{Kern}(P) = \text{Span}(1, 1, -1), \qquad \text{Bild}(P) = \text{Bodenebene}.$$

Also $\dim \text{Kern}(P) = 1$ und $\text{Rang}(P) = 2$, und die Rangformel wird zur sichtbaren Aussage

$$\underbrace{3}_{\dim \mathbb{R}^3} = \underbrace{1}_{\substack{\text{Sonnenrichtung,} \\ \text{geht auf } 0}} + \underbrace{2}_{\substack{\text{Bodenebene,} \\ \text{kommt im Bild an}}}.$$

Die drei Freiheitsgrade des Raumes teilen sich sauber auf: Die eine Richtung entlang der Strahlen wird plattgedrückt, die beiden Richtungen des Bodens bleiben erhalten. Man sieht der Rangformel hier an, dass sie keine Buchhaltung ist, sondern eine geometrische Bilanz: *Was der Schatten wegwirft plus was er behält ergibt den ganzen Raum.*

Beachte auch die Warnung der vorigen Bemerkung: Der Zielraum ist $\mathbb{R}^3$, aber das Bild ist nur die Ebene. Die Rangformel zerlegt $\dim \mathbb{R}^3$ auf der *Startseite*, nicht den Zielraum.

4.6 Lineare Fortsetzung von Basiswerten

Theorem 4.6.1 (Lineare Fortsetzung von einer Basis)**.** *Sei V ein endlich dimensionaler k-Vektorraum mit Basis*

$$b_1, \dots, b_n.$$

Sei W ein weiterer k-Vektorraum. Seien

$$w_1, \dots, w_n \in W$$

beliebige Vektoren.

Dann gibt es genau eine lineare Abbildung

$$f : V \to W$$

mit

$$f(b_i) = w_i \quad \textit{für alle } i = 1, \dots, n.$$

Beweis. Jedes $v \in V$ hat genau eine Darstellung

$$v = \sum_{i=1}^{n} \lambda_i b_i.$$

Wir definieren

$$f(v) := \sum_{i=1}^{n} \lambda_i w_i.$$

Diese Definition ist wohldefiniert, weil die Koeffizienten $\lambda_1, \dots, \lambda_n$ eindeutig sind.

Die Abbildung ist linear: Seien

$$v = \sum_{i=1}^{n} \lambda_i b_i \quad \text{und} \quad u = \sum_{i=1}^{n} \mu_i b_i.$$

Dann ist

$$\alpha v + \beta u = \sum_{i=1}^{n} (\alpha\lambda_i + \beta\mu_i) b_i.$$

Also gilt

$$f(\alpha v + \beta u) = \sum_{i=1}^{n} (\alpha\lambda_i + \beta\mu_i) w_i = \alpha f(v) + \beta f(u).$$

Damit ist f linear.

Außerdem gilt für jedes j:

$$f(b_j) = w_j.$$

Die Eindeutigkeit folgt aus Theorem 4.3.1. Denn eine lineare Abbildung ist durch ihre Werte auf einer Basis eindeutig festgelegt. □

Korollar 4.6.2 (Endlich dimensionale Vektorräume gleicher Dimension sind isomorph)**.** *Seien V und W endlich dimensionale k-Vektorräume. Dann gilt:*

$$V \cong W \quad \Longleftrightarrow \quad \dim(V) = \dim(W).$$

Beweis. Die Richtung von links nach rechts ist genau Korollar 4.5.2.

Für die Rückrichtung gelte

$$\dim(V) = \dim(W) = n.$$

Sei

$$b_1, \dots, b_n$$

eine Basis von V, und sei

$$c_1, \dots, c_n$$

eine Basis von W.

Nach dem Satz über lineare Fortsetzung gibt es genau eine lineare Abbildung

$$f : V \to W$$

mit

$$f(b_i) = c_i \quad \text{für alle } i = 1, \dots, n.$$

Wir zeigen, dass f bijektiv ist.

Surjektivität: Da $c_1, \dots, c_n$ eine Basis von W ist, erzeugen diese Vektoren W. Da alle c_i im Bild von f liegen, gilt

$$\text{Bild}(f) = W.$$

Injektivität: Sei

$$v = \sum_{i=1}^{n} \lambda_i b_i$$

und gelte

$$f(v) = 0.$$

Dann ist

$$0 = f(v) = \sum_{i=1}^{n} \lambda_i c_i.$$

Da $c_1, \dots, c_n$ linear unabhängig sind, folgt

$$\lambda_1 = \cdots = \lambda_n = 0.$$

Also ist

$$v = 0.$$

Damit ist

$$\text{Kern}(f) = \{0\}.$$

Nach Lemma 4.5.8 ist f injektiv.

Somit ist f bijektiv und linear. Nach Lemma 4.1.9 ist f ein Isomorphismus. Also gilt

$$V \cong W.$$ □

Bemerkung 4.6.3 (Strategischer Punkt)**.** Sobald man zwei Basen gleicher Länge hat, kann man den einen Vektorraum isomorph auf den anderen abbilden, indem man die erste Basis auf die zweite schickt.

Damit ist die Dimension eine vollständige Klassifikation endlich dimensionaler Vektorräume über einem festen Körper. In diesem Sinne ist k^n der „einzige“ n-dimensional Vektorraum. Es ist aber oft sehr nützlich im originalen Vektorraum zu bleiben.

Kapitel 5

Koordinaten und Basiswechsel

5.1 Konjugation: umbenennen, anwenden, zurückbenennen

In diesem Kapitel geht es um eine einzige Frage:

Was ändert sich, wenn wir dieselbe Sache in einer anderen Sprache beschreiben — und was bleibt gleich?

Diese Frage ist uns schon mehrfach begegnet. Die Symmetrien des Dreiecks und die Permutationen seiner Ecken sind „dasselbe in zwei Sprachen“ (Leitbeispiel 2.1.50). Die Anzeige der Messstation beschreibt ein Signal durch drei Zahlen (Leitbeispiel 3.3.6). Und im Kapitel über lineare Abbildungen haben wir gesehen, dass jeder n-dimensionale Vektorraum isomorph zu k^n ist — aber auf viele verschiedene Weisen.

Solange wir nur *Objekte* übersetzen, ist das alles harmlos. Interessant wird es, wenn wir *Abbildungen* übersetzen: Wie sieht eine Drehung aus, wenn man das Koordinatensystem wechselt? Wie sieht eine Permutation aus, wenn man die Objekte umnummeriert? Die Antwort der Algebra auf diese Frage ist immer dieselbe Formel, und sie hat einen Namen: *Konjugation*. Wir haben sie in Definition 2.1.53 bereits kennengelernt: Das Konjugat von h mit g ist

$$g \circ h \circ g^{-1},$$

gelesen von rechts nach links:

erst mit g^{-1} zurückübersetzen, dann h anwenden, dann mit g wieder vorübersetzen.

Das Konjugat ist die Handlung h, verpflanzt in eine andere Darstellung, an einen anderen Ort, in eine andere Sprache. In diesem Abschnitt üben wir diese Denkfigur an Gruppen — und lösen dabei ein offenes Versprechen aus dem Kapitel über das Vorzeichen ein. Ab dem nächsten Abschnitt bauen wir dann die lineare Version auf: Koordinaten, Matrizen und schließlich den Basiswechsel.

Dieser erste Abschnitt vertieft Stoff über Gruppen, Permutationen und das Vorzeichen. Wer nur die lineare Algebra braucht, kann die Kernidee („umbenennen, anwenden, zurückbenennen“) mitnehmen und ab dem nächsten Abschnitt einsteigen.

Leitbeispiel 5.1.1 (Der Roboter und die Kiste)**.** In einer Lagerhalle arbeitet ein Roboter. In der Halle steht eine Kiste, und der Roboter beherrscht einige Handlungen: Er kann die Kiste verschieben, ihren Deckel umklappen, und an der *Packstation* steht eine Anlage, die eine dort stehende offene Kiste mit drei Paketen befüllt. Handlungen werden nacheinander ausgeführt, und jede Handlung soll sich rückgängig machen lassen — die Handlungen verhalten sich also wie Elemente einer Gruppe, verknüpft durch Hintereinanderausführung.

Erste Szene: die Kiste steht im Lager, nicht an der Packstation. Die Befüllanlage kann nur an der Packstation arbeiten. Der Roboter löst das Problem so:

1. T: schiebe die Kiste vom Lager zur Packstation,
2. F: lasse die Anlage die Kiste befüllen,
3. T^{-1}: schiebe die Kiste zurück ins Lager.

Als Verkettung gelesen (rechts steht, was zuerst passiert) ist das

$$T^{-1} \circ F \circ T,$$

ein *Konjugat* von F (in der Rolle des g aus $g \circ h \circ g^{-1}$ steht hier $g = T^{-1}$ — welche Seite das Inverse trägt, hängt also davon ab, was man g nennt; entscheidend ist die *Leserichtung* „rechts zuerst“, nicht die Position des Strichs). Die Formel listet die drei Schritte damit in *umgekehrter* Reihenfolge zur Aufzählung oben. Sein Gesamteffekt: Die Kiste steht wieder an ihrem alten Platz — aber befüllt. Das Konjugat verhält sich im Lager exakt so, wie sich F an der Packstation verhält: Es ist F, an einen anderen Schauplatz verpflanzt. Man beachte dabei: Verpflanzt heißt *verändert* — das Konjugat ist eine andere Handlung als F selbst. F befüllt Kisten an der Packstation; das Konjugat befüllt, unterm Strich, Kisten im Lager, wo der Roboter gar keine Befüllanlage besitzt.

Zweite Szene: der Deckel. Dieselbe Figur, noch eine Spur verblüffender. Sei K die Handlung „klappe den Deckel um“ (aus offen wird zu, aus zu wird offen; insbesondere ist $K^{-1} = K$) und F wie oben das Befüllen der *offenen* Kiste. Das Konjugat

$$K \circ F \circ K$$

liest sich von rechts nach links: Deckel aufklappen, Pakete hineinlegen, Deckel wieder zuklappen. Der Gesamteffekt: *Die Pakete sind in der geschlossenen Kiste gelandet.* Kein einzelner Handgriff des Roboters kann das — durch einen geschlossenen Deckel kann man nichts legen. Das Konjugat ist F, verpflanzt in die Welt der zugeklappten Kisten.

In beiden Szenen ist das Konjugat also etwas Neues, verschieden von F. Nach Lemma 2.1.56 — „$g \circ h \circ g^{-1} = h$ gilt genau dann, wenn g und h kommutieren“ — *muss* das so sein, denn die beteiligten Handlungen kommutieren jeweils nicht mit F: „Erst befüllen, dann zur Packstation schieben“ lässt die Kiste leer (im Lager arbeitet keine Anlage), „erst schieben, dann befüllen“ nicht. Und „erst zuklappen, dann befüllen“ scheitert am Deckel, „erst befüllen, dann zuklappen“ nicht.

Dritte Szene: das Foto. Wann ändert Konjugieren ausnahmsweise *nichts*? Sei D die Handlung „drehe die Kiste um eine Vierteldrehung um ihre Hochachse“ und F' die Handlung „fotografiere die Kiste von oben und lege das Foto ins Archiv“. Das Konjugat

$$D^{-1} \circ F' \circ D$$

— drehen, fotografieren, zurückdrehen — lässt die Kiste am Ende exakt so stehen wie zuvor und legt ein Foto der *gedrehten* Kiste ins Archiv. Die Handlung F' allein legt ein Foto der ungedrehten Kiste ab. Die beiden Abläufe hinterlassen also genau dann ununterscheidbare Spuren — wir gehen idealisiert davon aus, dass das Drehen der Kiste selber beispielsweise keine Schleifspuren hinterlässt, und dass die Handlungen des Roboters nicht mitgeschrieben werden — wenn die Kiste von oben betrachtet nach der Vierteldrehung genauso aussieht wie vorher — wenn sie *symmetrisch* ist. Und das ist nach Lemma 2.1.56 genau die Aussage, dass Drehen und Fotografieren *kommutieren*: Bei einer symmetrischen Kiste ist es egal, ob man erst dreht und dann fotografiert oder umgekehrt. Die Symmetrie eines Objekts ist also keine Zusatzidee, sondern exakt die Bedingung, unter der ein Konjugat mit dem Original zusammenfällt. Diese Lesart kehrt am Ende des Abschnitts als physikalischer Symmetriebegriff wieder.

Eine ehrliche Fußnote zur Modellierung: Wer die Handlungen wirklich als Gruppe fassen will, nimmt die Menge Z aller Lagerzustände (Position und Ausrichtung der Kiste, Deckel offen oder zu,

Inhalt — und für die dritte Szene das Fotoarchiv) und modelliert Handlungen als Permutationen von Z, also als Elemente der *symmetrischen Gruppe* $\mathrm{Sym}(Z)$ — der Gruppe aller Permutationen (umkehrbaren Selbstabbildungen) von Z. Dazu muss man idealisieren: Jede Handlung muss auf jedem Zustand erklärt und umkehrbar sein — „befülle die offene Kiste“ etwa erklären wir auf geschlossenen Kisten als „tue nichts“, ihre Umkehrung nimmt die drei Pakete wieder heraus, und die Umkehrung des Fotografierens entfernt das oberste Foto wieder aus dem Archiv. Für die Anschauung braucht man diese Buchhaltung nicht, aber es ist gut zu wissen, dass sie möglich ist.

Nun das angekündigte allgemeine Prinzip. Es ist fast schon eine Trivialität — und genau deshalb so nützlich.

Lemma 5.1.2 (In abelschen Zielgruppen verschwindet die Konjugation)**.** *Seien G und H Gruppen und sei*

$$\varphi : G \to H$$

ein Gruppenhomomorphismus. Ist H abelsch (das heißt kommutativ) — zur Erinnerung: dass φ ein Homomorphismus *ist, heißt $\varphi(xy) = \varphi(x)\varphi(y)$ —, dann gilt für alle $g, h \in G$:*

$$\varphi\left(ghg^{-1}\right) = \varphi(h).$$

Ein Homomorphismus in eine abelsche Gruppe kann konjugierte Elemente nicht unterscheiden.

Beweis. Da φ ein Homomorphismus ist und Homomorphismen Inverse erhalten, gilt

$$\varphi\left(ghg^{-1}\right) = \varphi(g)\,\varphi(h)\,\varphi(g)^{-1}.$$

Da H abelsch ist, dürfen wir die Faktoren vertauschen:

$$\varphi(g)\,\varphi(h)\,\varphi(g)^{-1} = \varphi(g)\,\varphi(g)^{-1}\,\varphi(h) = \varphi(h). \qquad \square$$

Bemerkung 5.1.3 (Warum das bemerkenswert ist)**.** In G selbst kann Konjugation viel verändern — der Roboter aus Leitbeispiel 5.1.1 hat mit einem Konjugat Pakete in eine geschlossene Kiste gezaubert, und im Dreieck dreht Konjugation die Spiegelachsen weiter. Das Lemma sagt: Sobald man durch die Brille eines Homomorphismus in eine *abelsche* Gruppe schaut, wird all diese Bewegung unsichtbar. Abelsche Messwerte sind *konjugationsblind*. Wer also eine Größe sucht, die nicht von der Darstellung abhängt, sollte nach Homomorphismen in abelsche Gruppen Ausschau halten. Genau eine solche Größe kennen wir schon: das Vorzeichen.

Das Vorzeichen hängt nicht von der Nummerierung ab

Im Kapitel über das Vorzeichen blieb ein Unbehagen zurück. Die Definition

$$\operatorname{signum}\sigma = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

rechnet mit den *Zahlenwerten* der Elemente $1, \ldots, n$. Aber Permutationen gibt es von jeder n-elementigen Menge X: von den Ecken eines Dreiecks, von den Teilnehmern eines Turniers. Um die Formel anzuwenden, muss man die Elemente von X erst durchnummerieren — und niemand hat uns garantiert, dass verschiedene Nummerierungen dasselbe Vorzeichen liefern. Jetzt können wir diese Garantie beweisen.

Definition 5.1.4 (Nummerierung)**.** Sei X eine Menge mit n Elementen. Eine *Nummerierung* von X ist eine bijektive Abbildung

$$A : X \to \{1, \dots, n\}.$$

Lemma 5.1.5 (Umnummerieren ist ein Isomorphismus)**.** *Sei X eine Menge mit n Elementen und sei $A : X \to \{1, \dots, n\}$ eine Nummerierung. Dann ist*

$$c_A : \mathrm{Sym}(X) \to S_n, \quad \sigma \mapsto A \circ \sigma \circ A^{-1}$$

ein Isomorphismus von Gruppen.

Beweis. Zuerst prüfen wir, dass c_A überhaupt in S_n landet: $A \circ \sigma \circ A^{-1}$ ist eine Verkettung bijektiver Abbildungen $\{1, \dots, n\} \to X \to X \to \{1, \dots, n\}$, also eine Permutation von $\{1, \dots, n\}$.

c_A ist ein Homomorphismus: Für $\sigma, \tau \in \mathrm{Sym}(X)$ gilt

$$c_A(\sigma) \circ c_A(\tau) = A \circ \sigma \circ \underbrace{A^{-1} \circ A}_{=\mathrm{Id}_X} \circ \tau \circ A^{-1} = A \circ \sigma \circ \tau \circ A^{-1} = c_A(\sigma \circ \tau).$$

c_A ist bijektiv, denn

$$S_n \to \mathrm{Sym}(X), \quad \rho \mapsto A^{-1} \circ \rho \circ A$$

ist eine Umkehrabbildung (einsetzen und kürzen wie eben). Nach Lemma 2.1.45 ist c_A ein Isomorphismus. □

Bemerkung 5.1.6. Die Formel $A \circ \sigma \circ A^{-1}$ hat dieselbe Gestalt wie die Konjugationsformel aus Definition 2.1.53 — nur dass A hier zwischen zwei *verschiedenen* Mengen übersetzt — streng genommen also keine Konjugation *innerhalb* einer Gruppe, sondern der Transport der Struktur längs des Isomorphismus A; für den Beweis unten brauchen wir ohnehin nur die echte Konjugation in S_n. Die Lesart ist dieselbe: Nimm eine Nummer, übersetze sie zurück in ein Element von X, wende σ an, und übersetze das Ergebnis wieder in eine Nummer. $c_A(\sigma)$ ist „σ, erzählt in Nummern“.

Theorem 5.1.7 (Homomorphismen in abelsche Gruppen sind nummerierungsblind)**.** *Sei X eine Menge mit n Elementen, und seien*

$$A, B : X \to \{1, \dots, n\}$$

zwei Nummerierungen von X. Sei H eine abelsche Gruppe und

$$\varphi : S_n \to H$$

ein Gruppenhomomorphismus. Dann gilt

$$\varphi \circ c_A = \varphi \circ c_B.$$

Das heißt: Für jede Permutation $\sigma \in \mathrm{Sym}(X)$ liefert φ, angewendet auf die durchnummerierte Version von σ, dasselbe Ergebnis — ganz gleich, mit welcher Nummerierung man arbeitet.

Beweis. Die beiden Nummerierungen unterscheiden sich nur um eine Permutation der Nummern: Setze

$$\tau := A \circ B^{-1}.$$

Das ist eine bijektive Abbildung $\{1, \dots, n\} \to \{1, \dots, n\}$, also ein Element von S_n.

Sei nun $\sigma \in \mathrm{Sym}(X)$ beliebig. Dann gilt

$$c_A(\sigma) = A \circ \sigma \circ A^{-1} = (A \circ B^{-1}) \circ (B \circ \sigma \circ B^{-1}) \circ (B \circ A^{-1}) = \tau \circ c_B(\sigma) \circ \tau^{-1}.$$

Wir haben nur $B^{-1} \circ B = \mathrm{Id}_X$ eingeschoben. Die beiden durchnummerierten Versionen von σ sind also *konjugiert* in S_n. Nach Lemma 5.1.2 folgt

$$\varphi(c_A(\sigma)) = \varphi\left(\tau \circ c_B(\sigma) \circ \tau^{-1}\right) = \varphi(c_B(\sigma)).$$ □

Korollar 5.1.8 (Das Vorzeichen einer Permutation beliebiger Objekte)**.** *Sei X eine Menge mit n Elementen und $\sigma \in \mathrm{Sym}(X)$. Dann hat*

$$\mathrm{signum}\left(A \circ \sigma \circ A^{-1}\right)$$

für jede Nummerierung A von X denselben Wert. Wir dürfen diesen Wert das Vorzeichen von σ *nennen und* $\mathrm{signum}\,\sigma$ *schreiben. Da c_A ein Isomorphismus ist, ist das so erklärte* $\mathrm{signum} : \mathrm{Sym}(X) \to (\{-1,+1\},\cdot)$ *selbst ein Gruppenhomomorphismus — insbesondere multiplikativ:* $\mathrm{signum}(\sigma \circ \tau) = \mathrm{signum}(\sigma)\,\mathrm{signum}(\tau)$.

Beweis. Das Vorzeichen

$$\mathrm{signum} : S_n \to (\{-1,+1\},\cdot)$$

ist ein Gruppenhomomorphismus, und die zweielementige Gruppe $\{-1,+1\}$ ist abelsch. Nach Theorem 5.1.7 ist $\mathrm{signum} \circ c_A$ unabhängig von A. □

Beispiel 5.1.9 (Das Dreieck, ohne Beschriftung)**.** Für die Symmetrien des Dreiecks hatten wir das Vorzeichen geometrisch gedeutet: $\mathrm{signum} = +1$ für die Drehungen, $\mathrm{signum} = -1$ für das Umklappen. Ob ein Dreieck umgeklappt wird, sieht man ihm an — dazu muss niemand die Ecken mit 1, 2, 3 beschriften. Die geometrische Deutung *erzwingt* also, dass das Vorzeichen von der Beschriftung unabhängig ist. Das Korollar bestätigt das und erklärt zugleich den Mechanismus dahinter: Zwei Beschriftungen unterscheiden sich um eine Konjugation, und in der abelschen Zielgruppe $\{-1,+1\}$ kürzt sich jede Konjugation weg. Achtung: Der Isomorphismus $c_A : \mathrm{Sym}(X) \to S_3$ selbst hängt sehr wohl von der Beschriftung ab — *welcher* Dreierzykel eine gegebene Drehung ist, entscheidet die Nummerierung. Nur das Vorzeichen ist blind dafür.

Bemerkung 5.1.10 (Symmetrie in der Physik ist eine Konjugationsaussage)**.** Die Denkfigur „umbenennen, anwenden, zurückbenennen“ ist auch die algebraische Form des physikalischen Symmetriebegriffs. Die Foto-Szene aus Leitbeispiel 5.1.1 hat ihn im Kleinen schon vorgeführt: Symmetrisch ist, was man folgenlos drehen darf — Konjugat gleich Original, Drehen kommutiert mit Fotografieren. Jetzt dasselbe im Großformat.

Stellen wir uns die Zeitentwicklung als Handlung vor: U bedeutet „lasse die Physik eine Sekunde lang laufen“, aufgefasst als *Bijektion* auf den Zuständen der Welt — dieselbe Modellierungs-Idealisierung wie in der Fußnote zu Leitbeispiel 5.1.1, jetzt im Großformat (dass die Dynamik überhaupt umkehrbar ist, ist selbst eine physikalische Annahme). Sei C die Umbenennung „ersetze überall positive durch negative Ladungen und umgekehrt“. *Ladungssymmetrie* ist dann die Behauptung

$$C \circ U \circ C^{-1} = U :$$

Alle Ladungen tauschen, die Physik laufen lassen, und wieder zurücktauschen — das soll von „einfach laufen lassen“ nicht zu unterscheiden sein. Nach Lemma 2.1.56 ist das gleichbedeutend mit $C \circ U = U \circ C$: Es ist egal, ob man erst umbenennt und dann die Zeit laufen lässt oder umgekehrt.

Genauso ist *Translationssymmetrie* die Aussage $V \circ U \circ V^{-1} = U$ für die Umbenennung V, die die ganze Welt um einen festen Vektor verschiebt: Die Naturgesetze sind hier dieselben wie einen Meter weiter links.

Zwei Dinge sind daran bemerkenswert. Erstens: Eine Symmetrie ist keine Eigenschaft der Umbenennung allein, sondern eine Aussage über das *Zusammenspiel* von Umbenennung und Dynamik — nämlich dass die Konjugation die Dynamik nicht ändert. Zweitens: Solche Aussagen können falsch sein. Die Ladungssymmetrie galt lange als selbstverständlich, wird aber von der schwachen Wechselwirkung tatsächlich verletzt — ob $C \circ U \circ C^{-1} = U$ gilt, ist eine experimentelle Frage, keine Formsache. Die Algebra stellt hier nur die Sprache bereit, in der man die Frage präzise stellen kann.

Damit ist die Denkfigur dieses Kapitels aufgebaut: Konjugation transportiert Verhalten von einer Darstellung in eine andere, und konjugationsblinde Größen sind Eigenschaften der Sache selbst, nicht ihrer Beschreibung. In der linearen Algebra heißt „eine Darstellung wählen“: *eine Basis wählen*. Der Rest des Kapitels führt das aus — erst für Vektoren (Koordinaten), dann für lineare Abbildungen (Matrizen), und schließlich für den Wechsel zwischen zwei Basen.

5.2 Koordinatenvektoren

Sei k ein Körper und sei V ein endlich dimensionaler k-Vektorraum.

Eine Basis von V haben wir bisher als System $b_1, \dots, b_n$ geschrieben. Ab jetzt spielt zusätzlich die *Reihenfolge* eine Rolle: Wer Koordinaten als Zahlenspalte notiert, muss wissen, welche Zahl zu welchem Basisvektor gehört. Wir schreiben Basen darum als Tupel

$$B = (b_1, \dots, b_n)$$

und meinen damit eine Basis mit festgelegter Reihenfolge. Als Menge betrachtet ist B dieselbe Basis wie zuvor; alle bisherigen Sätze über Basen — insbesondere die Existenz und Eindeutigkeit der Darstellung (Lemma 3.3.3) — gelten unverändert. Neu ist allein, dass die Reihenfolge festliegt: erst dadurch wird der Koordinatenvektor eine wohlbestimmte Zahlen*spalte*.

Definition 5.2.1 (Koordinatenvektor)**.** Sei V ein endlich-dimensionaler k-Vektorraum, und sei $B = (b_1, \dots, b_n)$ eine Basis von V. Ist $v \in V$, dann gibt es eindeutige Skalare $\lambda_1, \dots, \lambda_n \in k$ mit

$$v = \lambda_1 b_1 + \cdots + \lambda_n b_n \,.$$

Der Spaltenvektor

$$[v]_B := \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \in k^n$$

heißt der *Koordinatenvektor* von v bezüglich der Basis B.

Bemerkung 5.2.2. Die Existenz und Eindeutigkeit der Skalare ist genau Lemma 3.3.3: Jeder Vektor hat bezüglich einer Basis genau eine Darstellung als Linearkombination. Ohne die Eindeutigkeit wäre „der“ Koordinatenvektor gar nicht definiert. Man beachte die Notation: Die Basis steht als Index am Koordinatenvektor. Koordinaten sind immer Koordinaten *bezüglich einer Basis*, und die Notation zwingt uns, die gewählte Sprache dazuzusagen.

Beispiel 5.2.3 (Die Standardbasis: nichts Neues im k^n)**.** Sei $E = (e_1, \dots, e_n)$ die Standardbasis von k^n. Für

$$v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in k^n$$

gilt

$$v = v_1 e_1 + \cdots + v_n e_n,$$

also

$$[v]_E = v.$$

Im k^n mit der Standardbasis ist jeder Vektor sein eigener Koordinatenvektor. Genau deshalb übersieht man leicht, dass auch hier schon eine Basiswahl im Spiel ist: Die Einträge von v *sind* Koordinaten — bezüglich der Standardbasis.

Beispiel 5.2.4 (Eine schiefe Basis in der Ebene — und wie man Koordinaten ausrechnet)**.** In $\mathbb{R}^2$ betrachten wir die Basis

$$B = (b_1, b_2) \quad \text{mit} \quad b_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix},\ b_2 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

(b_1, b_2 sind keine Vielfachen voneinander, also linear unabhängig; zwei linear unabhängige Vektoren in einem zweidimensionalen Raum sind eine Basis.)

Was ist der Koordinatenvektor von

$$v = \begin{pmatrix} 5 \\ 1 \end{pmatrix}$$

bezüglich B? Wir suchen λ_1, λ_2 mit

$$\lambda_1 \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 5 \\ 1 \end{pmatrix}.$$

Komponentenweise gelesen ist das ein Gleichungssystem:

$$\lambda_1 + \lambda_2 = 5, \qquad \lambda_1 - \lambda_2 = 1.$$

Addieren liefert $2\lambda_1 = 6$, also $\lambda_1 = 3$ und $\lambda_2 = 2$. Also

$$[v]_B = \begin{pmatrix} 3 \\ 2 \end{pmatrix}.$$

Merke: *Koordinaten ausrechnen heißt, ein lineares Gleichungssystem lösen* — die Basisvektoren stehen (als Standardkoordinaten) in den Spalten, der Vektor auf der rechten Seite. Und zur Erinnerung: $v = \begin{pmatrix} 5 \\ 1 \end{pmatrix}$ selbst ist bereits $[v]_E$ — derselbe Vektor, nur in einer anderen Sprache als $[v]_B = \begin{pmatrix} 3 \\ 2 \end{pmatrix}$. Hier ging es mit bloßem Hinsehen; ein systematisches Verfahren für große Systeme entwickeln wir im nächsten Kapitel.

Beispiel 5.2.5 (Polynome: dieselbe Funktion, zwei Befragungen)**.** Sei P_2 der Vektorraum der reellen Polynome vom Grad höchstens 2. Die *Monombasis* ist

$$B = (1,\ x,\ x^2).$$

Für $p = 4 + 3x - x^2$ liest man die Koordinaten direkt ab:

$$[p]_B = \begin{pmatrix} 4 \\ 3 \\ -1 \end{pmatrix}.$$

Nun eine zweite Basis, die um die Stelle 1 herum gebaut ist:

$$B' = \big(1,\ (x-1),\ (x-1)^2\big).$$

(Auch das ist eine Basis: Substituiert man $y = x - 1$, wird aus B' die Monombasis in y — jedes Polynom vom Grad höchstens 2 hat also genau eine Darstellung.) Wir suchen a, b, c mit

$$4 + 3x - x^2 = a + b(x-1) + c(x-1)^2.$$

Ausmultiplizieren der rechten Seite ergibt

$$(a - b + c) + (b - 2c)\,x + c\,x^2.$$

Koeffizientenvergleich:

$$c = -1, \qquad b - 2c = 3 \implies b = 1, \qquad a - b + c = 4 \implies a = 6.$$

Also

$$[p]_{B'} = \begin{pmatrix} 6 \\ 1 \\ -1 \end{pmatrix}.$$

Die neuen Koordinaten sind keine willkürlichen Zahlen — sie beantworten Fragen über das Verhalten von p an der Stelle 1:

$$a = p(1) = 6, \qquad b = p'(1) = 3 - 2 \cdot 1 = 1, \qquad c = \tfrac{1}{2}p''(1) = -1.$$

Das ist kein Zufall, sondern der Anfang der *Taylorentwicklung* aus der Analysis. Die Moral: Eine Basis ist eine *Befragung* des Vektors. Die Monombasis fragt nach den Koeffizienten, die verschobene Basis fragt nach Wert, Steigung und Krümmung bei 1. Derselbe Vektor, zwei Antworten — je nachdem, welche Fragen man stellt.

Leitbeispiel 5.2.6 (Die Messstation liest Koordinaten ab)**.** Jetzt können wir aussprechen, was in Leitbeispiel 3.3.6 schon die ganze Zeit passiert ist. Die Station lauscht mit drei Detektoren auf die Frequenzen c_1, c_2, c_3 und lebt im Raum

$$W = \operatorname{Span}(s_{c_1}, s_{c_2}, s_{c_3})$$

mit der Basis

$$B = (s_{c_1}, s_{c_2}, s_{c_3}).$$

Empfängt sie ein Signal $v \in W$, dann zeigt sie das Tripel $(\lambda_1, \lambda_2, \lambda_3)$ seiner eindeutigen Darstellung an — in unserer neuen Sprache:

$$\text{Anzeige der Station} = [v]_B.$$

Die Messstation ist eine Koordinatenabbildung.

Das ist ein allgemeines Muster, das man nicht mehr vergisst, wenn man es einmal gesehen hat: *Ein Messgerät gibt niemals „den Vektor selbst" aus, sondern immer Zahlen — Koordinaten bezüglich einer Basis, die im Gerät fest verbaut ist.* Beim Signalraum sind das die drei Detektorfrequenzen. Beim übernächsten Leitbeispiel wird es dramatischer: Dort verstellt sich die verbaute Basis.

Leitbeispiel 5.2.7 (Das Kristallgitter: Labormeter und Gitterschritte)**.** Ein Kristall ist aus lauter gleichen Zellen aufgebaut, die von drei *Gittervektoren* $a_1, a_2, a_3 \in \mathbb{R}^3$ aufgespannt werden. Für ein konkretes Zahlenbeispiel nehmen wir (gemessen in einer Laboreinheit entlang der Standardachsen)

$$a_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \qquad a_2 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \qquad a_3 = \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix}.$$

Die drei Vektoren sind linear unabhängig, also ist $G = (a_1, a_2, a_3)$ eine Basis des $\mathbb{R}^3$. Nun beschreibt dieselbe Person zweierlei Sprachen für denselben Ort v im Kristall:

- Die *Laborantin* misst mit dem Maßstab entlang der Standardachsen:

$$[v]_E = \begin{pmatrix} 3 \\ 2 \\ 4 \end{pmatrix}.$$

- Der *Kristallograph* zählt Gitterschritte: erst wie oft a_1, dann wie oft a_2, dann wie oft a_3. Er findet

$$[v]_G = \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix},$$

denn

$$1 \cdot a_1 + 2 \cdot a_2 + 2 \cdot a_3 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 2 \\ 2 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 4 \end{pmatrix} = \begin{pmatrix} 3 \\ 2 \\ 4 \end{pmatrix} = v.$$

Beide beschreiben denselben Punkt. Warum tut sich der Kristallograph die schiefe Basis an? Weil in *seiner* Sprache der Kristall einfach wird: Die Atome sitzen genau an den Stellen mit *ganzzahligen* Gitterkoordinaten. Was im Labor wie ein schiefes Muster aussieht, ist in Gitterkoordinaten schlicht $\mathbb{Z}^3$. (Die Kristallographie treibt das systematisch: Richtungen und Ebenen im Kristall werden traditionell durch kleine ganze Zahlen in Gitterkoordinaten angegeben.) Die Lehre ist dieselbe wie beim Taylor-Beispiel: *Man wählt die Basis so, dass das eigene Problem einfache Koordinaten bekommt.* Wie man zwischen Labor- und Gittersprache *umrechnet*, klären wir im letzten Abschnitt dieses Kapitels.

Leitbeispiel 5.2.8 (Der Schiffsmast: verdrehte Messgeräte)**.** Ein Schiff trägt an seinem Mast zwei Ortungsgeräte: ein Radar und eine optische Kamera. Jedes Gerät ortet andere Schiffe und meldet deren Position relativ zum Mast — als Zahlenpaar in der (horizontalen) Ebene: so viele Meilen in Richtung des *eigenen* „Voraus“, so viele in Richtung des *eigenen* „Steuerbord“. In unserer Sprache: Im Radar ist eine Basis $R = (r_1, r_2)$ der Ebene verbaut (r_1 zeigt entlang der Radar-Nullrichtung, r_2 senkrecht dazu), in der Kamera eine Basis $K = (k_1, k_2)$, und gemeldet werden die Koordinatenvektoren

$$[v]_R \qquad \text{beziehungsweise} \qquad [v]_K$$

des Ortsvektors v eines georteten Schiffs. Solange alle Geräte exakt gleich ausgerichtet sind, stimmen die Zahlen überein und niemand denkt über Basen nach.

Dann kommt der Sturm. Die Montageringe am Mast verrutschen, die Geräte sind nun gegeneinander *verdreht* — um Winkel, die niemand kennt. Ab sofort melden Radar und Kamera für dasselbe Schiff verschiedene Zahlenpaare:

$$[v]_R \neq [v]_K,$$

obwohl beide denselben Vektor v orten. Kein Gerät ist kaputt — sie sprechen nur verschiedene Sprachen. An den Mast kommt auf See niemand heran. Die Frage dieses Kapitels, in ihrer praktischsten Form:

Kann man die Verdrehung rein rechnerisch rückgängig machen — also die Radardaten in Kamerasprache umrechnen, ohne ein einziges Gerät anzufassen?

Die Antwort ist ja, und sie besteht aus einer einzigen Matrix. Wir lösen das im letzten Abschnitt dieses Kapitels auf.

Die Zuordnung $v \mapsto [v]_B$ verdient einen genaueren Blick. Sie ist nicht irgendeine Buchhaltung, sondern selbst eine lineare Abbildung — und zwar eine besonders gute.

Lemma 5.2.9 (Die Koordinatenabbildung ist ein Isomorphismus)**.** *Sei V ein k-Vektorraum mit Basis $B = (b_1, \dots, b_n)$. Dann ist die* Koordinatenabbildung

$$\Phi_B : V \to k^n, \quad v \mapsto [v]_B$$

ein Isomorphismus von Vektorräumen. Insbesondere gilt

$$[v + w]_B = [v]_B + [w]_B \quad \textit{und} \quad [\lambda v]_B = \lambda [v]_B$$

für alle $v, w \in V$ und $\lambda \in k$, sowie

$$\Phi_B(b_j) = e_j \quad \textit{für } j = 1, \dots, n.$$

Beweis. Wir betrachten die Abbildung in die andere Richtung:

$$\Psi_B : k^n \to V, \quad \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \mapsto \lambda_1 b_1 + \cdots + \lambda_n b_n.$$

Diese Abbildung ist linear (Addieren und Skalieren von Koeffizienten verträgt sich mit Addieren und Skalieren von Linearkombinationen). Nach Lemma 3.3.3 hat jedes $v \in V$ *genau eine* Darstellung als Linearkombination der b_i. Das heißt: Ψ_B ist surjektiv (mindestens eine Darstellung) und injektiv (höchstens eine Darstellung), also bijektiv. Nach Lemma 4.1.9 ist Ψ_B ein Isomorphismus.

Die Koordinatenabbildung Φ_B ist genau die Umkehrabbildung von Ψ_B: Sie schickt v auf das eindeutige Koeffiziententupel seiner Darstellung. Als Umkehrabbildung eines Isomorphismus ist Φ_B selbst linear und ein Isomorphismus.

Schließlich ist

$$b_j = 0 \cdot b_1 + \cdots + 1 \cdot b_j + \cdots + 0 \cdot b_n,$$

also $[b_j]_B = e_j$. □

Bemerkung 5.2.10 (Der Vektor ist das Ding — die Koordinaten sind seine Beschreibung)**.** Das Lemma präzisiert den „strategischen Punkt“ vom Ende des Kapitels über lineare Abbildungen: Jeder n-dimensionale k-Vektorraum ist isomorph zu k^n — aber nicht auf eine einzige, gottgegebene Weise. *Jede Basis B liefert ihren eigenen Isomorphismus Φ_B.* Eine Basis wählen heißt also: eine Übersetzung in die Zahlenwelt k^n wählen.

Daraus folgt die wichtigste Warnung dieses Kapitels: Koordinaten sind nie absolut. Der Vektor v existiert ohne jede Basis — der Pfeil im Raum, das Signal im Äther, das Polynom als Funktion.

Seine Koordinaten dagegen sind eine Beschreibung *relativ zu einer gewählten Sprache*, und in verschiedenen Sprachen sehen sie verschieden aus:

$$[p]_B = \begin{pmatrix} 4 \\ 3 \\ -1 \end{pmatrix}, \qquad [p]_{B'} = \begin{pmatrix} 6 \\ 1 \\ -1 \end{pmatrix}$$

beschreiben dasselbe Polynom. Wer Koordinaten notiert, ohne die Basis dazuzusagen, produziert genau die Verwirrung, die auf dem Schiffsmast aus Leitbeispiel 5.2.8 herrscht.

5.3 Die Matrix einer linearen Abbildung bezüglich Basen

Im Kapitel über lineare Abbildungen haben wir bewiesen: Jede lineare Abbildung $f : k^n \to k^m$ ist von der Form L_A für genau eine Matrix A, und die Spalten von A sind die Bilder der Standardbasisvektoren (Theorem 4.4.2). Dieser Satz hat zwei Lücken:

- Er redet nur über die Standardräume k^n. Was ist mit einer linearen Abbildung zwischen *beliebigen* endlich dimensionalen Vektorräumen — etwa der Ableitung auf Polynomen? Dort gibt es keine „Standardbasis“ vom Himmel.
- Selbst im k^n gibt es viele Basen — und wir werden sehen, dass eine gut gewählte Basis dieselbe Abbildung *dramatisch* einfacher beschreibt.

Die Koordinatenabbildungen aus dem letzten Abschnitt schließen beide Lücken: Wir beschreiben eine Abbildung $F : V \to W$, indem wir sagen, was sie *in Koordinaten* tut.

Seien im Folgenden V und W endlich-dimensionale k-Vektorräume.

Definition 5.3.1 (Matrixdarstellung zu Basen)**.** Sei $B = (b_1, \dots, b_n)$ eine Basis von V, und sei $C = (c_1, \dots, c_m)$ eine Basis von W. Ist $F : V \to W$ linear, dann ist die *Matrix von F bezüglich der Basen B und C* die Matrix

$$M_{C \leftarrow B}(F) \in k^{m \times n},$$

deren j-te Spalte der Koordinatenvektor $[F(b_j)]_C$ ist:

$$M_{C \leftarrow B}(F) = \begin{pmatrix} | & & | \\ [F(b_1)]_C & \cdots & [F(b_n)]_C \\ | & & | \end{pmatrix}.$$

Bemerkung 5.3.2 (Wie man das Symbol liest)**.** Man liest $M_{C \leftarrow B}$ als $M_{C \leftarrow B}$: rechts die Start- (Eingabe-)Basis B, links die Ziel- (Ausgabe-)Basis C; der Pfeil läuft, wie Matrix-mal-Vektor, von rechts nach links.

Bemerkung 5.3.3 (Warum die Basis in der Matrix steht)**.** Die Definition ist dasselbe Rezept wie im Standardfall, nur konsequent in Koordinaten übersetzt:

Schicke jeden Basisvektor durch F und schreibe das Ergebnis — in der Sprache der Zielbasis — als Spalte auf.

Die Matrix ist also ein Protokoll: Spalte j protokolliert das Schicksal von b_j. Mehr muss man nicht festhalten, denn eine lineare Abbildung ist durch ihre Werte auf einer Basis vollständig bestimmt (Korollar 4.3.2). In der Notation $M_{C \leftarrow B}$ steht der Pfeil für die Richtung der Übersetzung: Die Matrix nimmt B-Koordinaten entgegen und liefert C-Koordinaten. Das macht der folgende Satz präzise.

Theorem 5.3.4 (Die Matrixdarstellung rechnet in Koordinaten)**.** *Seien B, C und F wie in Definition 5.3.1. Dann gilt für jedes $v \in V$:*

$$[F(v)]_C = M_{C\leftarrow B}(F)\,[v]_B\,. \tag{†}$$

Außerdem ist $M_{C\leftarrow B}(F)$ die einzige *Matrix mit dieser Eigenschaft.*

Beweis. Sei $v \in V$ mit Basisdarstellung

$$v = \lambda_1 b_1 + \cdots + \lambda_n b_n, \qquad \text{also} \qquad [v]_B = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}.$$

Da F linear ist, gilt

$$F(v) = \lambda_1 F(b_1) + \cdots + \lambda_n F(b_n).$$

Da die Koordinatenabbildung Φ_C linear ist (Lemma 5.2.9), folgt

$$[F(v)]_C = \lambda_1 [F(b_1)]_C + \cdots + \lambda_n [F(b_n)]_C.$$

Rechts steht eine Linearkombination der Spalten von $M := M_{C\leftarrow B}(F)$ mit den Koeffizienten λ_j. Genau das ist das Matrixprodukt: Nach Lemma 4.4.1 ist Me_j die j-te Spalte von M, und da L_M linear ist (Lemma 4.2.8), gilt

$$M[v]_B = M(\lambda_1 e_1 + \cdots + \lambda_n e_n) = \lambda_1 Me_1 + \cdots + \lambda_n Me_n.$$

Beide Seiten stimmen also überein, und (†) ist bewiesen.

Zur Eindeutigkeit: Erfüllt eine Matrix M' ebenfalls $[F(v)]_C = M'[v]_B$ für alle v, dann setzen wir $v = b_j$ ein. Wegen $[b_j]_B = e_j$ folgt

$$M'e_j = [F(b_j)]_C,$$

die j-te Spalte von M' ist also $[F(b_j)]_C$. Damit sind alle Spalten von M' festgelegt, und es gilt $M' = M_{C\leftarrow B}(F)$. □

Bemerkung 5.3.5 (Was diese Matrix tut: eine Konjugation)**.** Die Matrix $M_{C\leftarrow B}(F)$ ist nicht die Abbildung F selbst. Sie ist die Beschreibung von F in Koordinaten. Man startet mit Koordinaten bezüglich B, wendet die Matrix an, und erhält Koordinaten bezüglich C. Als Diagramm, mit den Koordinatenabbildungen Φ_B und Φ_C aus Lemma 5.2.9:

$$\begin{array}{ccc} V & \xrightarrow{F} & W \\ {\scriptstyle\Phi_B}\downarrow & & \downarrow{\scriptstyle\Phi_C} \\ k^n & \xrightarrow[L_{M_{C\leftarrow B}(F)}]{} & k^m \end{array}$$

Es sagt: Erst abbilden und dann Koordinaten nehmen ist dasselbe wie erst Koordinaten nehmen und dann mit der Matrix multiplizieren. Als Gleichung geschrieben:

$$L_{M_{C\leftarrow B}(F)} = \Phi_C \circ F \circ \Phi_B^{-1}.$$

Von rechts nach links gelesen ist das die Denkfigur aus dem ersten Abschnitt: *Übersetze die Koordinaten zurück in einen Vektor (Φ_B^{-1}), wende F an, übersetze das Ergebnis wieder in Koordinaten (Φ_C).*

Angenommen nun $G : V \to V$ ist eine *lineare* Abbildung von einem Vektorraum V in sich selber. Und wir wählen auf dem Definitions- und Wertebereich dieselbe Basis D. Dann gilt

$$L_{M_{D\leftarrow D}(G)} = \Phi_D \circ G \circ \Phi_D^{-1}.$$

Die Matrixdarstellung ist ein *echtes* Konjugat von G — anders als im allgemeinen Fall $F : V \to W$, wo vorne und hinten *verschiedene* Koordinatenabbildungen stehen und wir nur von einer „Denkfigur“ sprachen, steht hier vorne und hinten dasselbe Φ_D — dieselbe Abbildung, verpflanzt in die Koordinatenwelt.

Beispiel 5.3.6 (Konsistenz-Check: die Standardbasen)**.** Sei $f : k^n \to k^m$ linear. Sei E die Standardbasis von k^n und E' die Standardbasis von k^m. Wegen $[w]_{E'} = w$ für alle $w \in k^m$ ist die j-te Spalte von $M_{E'\leftarrow E}(f)$ einfach $f(e_j)$ — also genau die Matrix aus Theorem 4.4.2. Die alte Theorie ist der Spezialfall „beide Basen sind die Standardbasen“ der neuen.

Beispiel 5.3.7 (Ableiten ist Matrixmultiplikation)**.** Sei P_2 der Raum der Polynome vom Grad höchstens 2 und P_1 der vom Grad höchstens 1. Die Ableitung

$$D : P_2 \to P_1, \quad p \mapsto p'$$

ist linear. Wir wählen die Monombasen $B = (1, x, x^2)$ von P_2 und $C = (1, x)$ von P_1 und protokollieren die Basisvektoren:

$$D(1) = 0, \qquad D(x) = 1, \qquad D(x^2) = 2x.$$

In C-Koordinaten sind das die Spalten $\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\2\end{pmatrix}$, also

$$M_{C\leftarrow B}(D) = \begin{pmatrix}0 & 1 & 0\\ 0 & 0 & 2\end{pmatrix}.$$

Probe mit $p = 4 + 3x - x^2$, also $[p]_B = (4, 3, -1)$ als Spalte:

$$\begin{pmatrix}0 & 1 & 0\\ 0 & 0 & 2\end{pmatrix}\begin{pmatrix}4\\3\\-1\end{pmatrix} = \begin{pmatrix}3\\-2\end{pmatrix},$$

und tatsächlich ist $p' = 3 - 2x$. Das Ableiten von Polynomen ist also — sobald man Basen gewählt hat — eine Matrixmultiplikation. Genau so behandeln Computeralgebrasysteme solche Operationen: Sie speichern Koordinatenvektoren und multiplizieren Matrizen.

Beispiel 5.3.8 (Dieselbe Drehung, zwei Matrizen)**.** Die Vierteldrehung

$$R : \mathbb{R}^2 \to \mathbb{R}^2, \quad \begin{pmatrix}x\\y\end{pmatrix} \mapsto \begin{pmatrix}-y\\x\end{pmatrix}$$

hat bezüglich der Standardbasis E die Matrix

$$M_{E\leftarrow E}(R) = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}.$$

Nun nehmen wir die schiefe Basis $B = (b_1, b_2)$ mit $b_1 = \begin{pmatrix}1\\1\end{pmatrix}$, $b_2 = \begin{pmatrix}1\\-1\end{pmatrix}$ aus Beispiel 5.2.4 und protokollieren neu:

$$R(b_1) = \begin{pmatrix}-1\\1\end{pmatrix} = 0 \cdot b_1 + (-1) \cdot b_2, \qquad R(b_2) = \begin{pmatrix}1\\1\end{pmatrix} = 1 \cdot b_1 + 0 \cdot b_2.$$

Also

$$M_{B\leftarrow B}(R) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Dieselbe Abbildung, zwei verschiedene Matrizen — die Einträge einer Matrixdarstellung sind also *keine* Eigenschaften der Abbildung allein, sondern hängen an der gewählten Basis. (Dass sich die beiden Matrizen hier nur um Vorzeichen unterscheiden, liegt daran, dass B gegenüber E gedreht *und gespiegelt* ist — in der B-Sprache dreht R „andersherum“.) Welche Größen von der Basis *unabhängig* sind, ist damit eine echte Frage — wir kommen am Ende des Kapitels darauf zurück.

Leitbeispiel 5.3.9 (Der Schattenwurf in angepasster Basis)**.** Jetzt der versprochene Grund, überhaupt fremde Basen anzufassen. Wir holen die Schattenabbildung aus Leitbeispiel 4.1.5 zurück:

$$P : \mathbb{R}^3 \to \mathbb{R}^3, \qquad P(x, y, z) = (x + z,\ y + z,\ 0),$$

mit Sonnenrichtung $d = (1, 1, -1)$. Bezüglich der Standardbasis war ihre Matrix

$$M_{E\leftarrow E}(P) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Man sieht ihr wenig an.

Nun wählen wir eine Basis, die zur *Geometrie des Schattenwurfs* passt: zwei Richtungen im Boden und die Sonnenrichtung,

$$B = (e_1,\ e_2,\ d).$$

(Das ist eine Basis: Eine Linearkombination $\lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 d = 0$ hat als dritte Komponente $-\lambda_3 = 0$, und dann folgt sofort $\lambda_1 = \lambda_2 = 0$.) Das Protokoll ist jetzt reine Anschauung:

$$P(e_1) = e_1, \qquad P(e_2) = e_2, \qquad P(d) = 0,$$

denn Bodenpunkte sind ihr eigener Schatten, und die Sonnenrichtung ist genau der Kern. In B-Koordinaten heißt das $[P(e_1)]_B = e_1$, $[P(e_2)]_B = e_2$, $[P(d)]_B = 0$, also

$$M_{B\leftarrow B}(P) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Diese Matrix ist eine *Inhaltsangabe* der Abbildung: „behalte die erste Richtung, behalte die zweite, drücke die dritte platt.“ Kern und Bild kann man ablesen, und auch $P \circ P = P$ ist keine Rechnung mehr wert — für Diagonalmatrizen quadriert man einfach die Diagonale, und $1^2 = 1$, $0^2 = 0$.

Merke: *Der Vektorraum wird durch einen Basiswechsel nicht einfacher — aber die Beschreibung der Abbildung kann es werden.* Die Kunst besteht darin, die Basis aus den geometrisch bedeutsamen Richtungen der Abbildung selbst zusammenzusetzen. Diese Kunst systematisch zu betreiben ist das Thema des Kapitels über Eigenwerte und Eigenvektoren.

Ein ehrlicher Vorbehalt: Nicht jede Abbildung lässt sich so weit vereinfachen. Dass überhaupt eine Basis aus geometrisch bedeutsamen Richtungen *existiert*, ist selbst eine Bedingung, keine Selbstverständlichkeit — die Scherung $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ etwa ist zu keiner Diagonalmatrix ähnlich. Das Kapitel über Eigenwerte zeigt, wann die Vereinfachung gelingt und wann nicht.

Zum Abschluss dieses Abschnitts klären wir, wie sich Matrixdarstellungen mit dem Verketten von Abbildungen vertragen. Die Antwort ist der eigentliche Grund, warum die Matrixmultiplikation so definiert ist, wie sie definiert ist.

Lemma 5.3.10 (Matrix einer Verkettung). *Seien $F : V \to W$ und $G : W \to U$ lineare Abbildungen zwischen endlich-dimensionalen k-Vektorräumen. Sei B eine Basis von V, sei C eine Basis von W, und sei D eine Basis von U. Dann gilt*

$$M_{D\leftarrow C}(G) \cdot M_{C\leftarrow B}(F) = M_{D\leftarrow B}(G \circ F)\,.$$

Beweis. Sei $v \in V$. Dann gilt nach Theorem 5.3.4 zuerst

$$[F(v)]_C = M_{C\leftarrow B}(F)\,[v]_B$$

und danach

$$[G(F(v))]_D = M_{D\leftarrow C}(G)\,[F(v)]_C\,.$$

Zusammen ergibt das

$$[(G \circ F)(v)]_D = M_{D\leftarrow C}(G)\,M_{C\leftarrow B}(F)\,[v]_B\,.$$

Die Matrix $M_{D\leftarrow C}(G)M_{C\leftarrow B}(F)$ rechnet also für $G \circ F$ in Koordinaten. Nach der Eindeutigkeit in Theorem 5.3.4 ist sie damit *die* Matrix von $G \circ F$ bezüglich B und D. □

Bemerkung 5.3.11 (Merkregel: die Basen docken aneinander an). In der Schreibweise mit Pfeilen liest sich das Lemma wie Dominosteine:

$$M_{D\leftarrow C}(G) \cdot M_{C\leftarrow B}(F) = M_{D\leftarrow B}(G \circ F).$$

Innen treffen sich zweimal dieselbe Basis C — die Ausgabesprache von F muss die Eingabesprache von G sein, sonst ergibt das Produkt keinen Sinn. Wer diese Regel im Kopf hat, setzt Basiswechselformeln später fehlerfrei zusammen.

Und noch eine Einsicht steckt im Lemma: Im Kapitel über lineare Abbildungen fiel die Formel für das Matrixprodukt scheinbar vom Himmel. Jetzt sehen wir ihren Sinn: *Matrixmultiplikation ist Verkettung von Abbildungen, aufgeschrieben in Koordinaten.*

Definition 5.3.12 (Einheitsmatrix). Die *Einheitsmatrix* $E_n \in k^{n\times n}$ ist die Matrix, deren j-te Spalte der Standardbasisvektor e_j ist:

$$E_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}.$$

Sie erfüllt $E_n v = v$ für alle $v \in k^n$ sowie $AE_n = A$ und $E_n M = M$, wann immer die Produkte definiert sind — sie ist das neutrale Element der Matrixmultiplikation. (Nicht zu verwechseln mit der Standardbasis E: E ohne Index bezeichnet stets die Standard*basis*, E_n mit Index stets die Einheits*matrix*.)

Beispiel 5.3.13 (Die Matrix des Nichtstuns). Sei $B = (b_1, \dots, b_n)$ eine Basis von V. Welche Matrix hat die Identität Id_V bezüglich B — *zweimal derselben* Basis B? Die Spalten sind

$$[\mathrm{Id}_V(b_j)]_B = [b_j]_B = e_j,$$

also

$$M_{B\leftarrow B}(\mathrm{Id}_V) = E_n.$$

Nichtstun, in ein und derselben Sprache protokolliert, ist die Einheitsmatrix. Der ganze nächste Abschnitt beruht auf der Beobachtung, dass dieser Satz *falsch* wird, sobald man vorne und hinten *verschiedene* Basen einsetzt.

5.4 Basiswechsel

Jetzt sind alle Werkzeuge beisammen für die Frage, die diesem Kapitel den Namen gibt:

Derselbe Vektor, dieselbe Abbildung — aber eine andere Basis. Wie rechnet man um?

Die Antwort ist verblüffend sparsam: Wir brauchen keinen einzigen neuen Begriff. Es genügt, die Matrixdarstellung aus dem letzten Abschnitt auf die *Identitätsabbildung* loszulassen.

Definition 5.4.1 (Basiswechselmatrix)**.** Sei V ein endlich-dimensionaler k-Vektorraum, und seien $B = (b_1, \dots, b_n)$ und $B' = (b'_1, \dots, b'_n)$ zwei Basen von V. Die *Basiswechselmatrix von B nach B'* ist

$$M_{B' \leftarrow B}(\mathrm{Id}_V) \in k^{n \times n},$$

die Matrix der Identität mit Startbasis B und Zielbasis B'.

Bemerkung 5.4.2 (Was diese Matrix tut — und warum die Basis in ihr drinsteht)**.** Setzt man $F = \mathrm{Id}_V$ in Theorem 5.3.4 ein, wird aus (†):

$$[v]_{B'} = M_{B' \leftarrow B}(\mathrm{Id}_V)\,[v]_B \qquad \text{für alle } v \in V.$$

Die Basiswechselmatrix ist also ein reiner *Übersetzer*: B-Koordinaten hinein, B'-Koordinaten heraus — am Vektor selbst geschieht *nichts*. Sie ist die Matrix des Nichtstuns, protokolliert in zwei verschiedenen Sprachen. (Mit *derselben* Basis vorne und hinten war das Protokoll des Nichtstuns die Einheitsmatrix, Beispiel 5.3.13. Der ganze Witz entsteht durch die zwei Sprachen.)

Und ihre Spalten kennen wir nach Definition 5.3.1 auch: Die j-te Spalte ist

$$[\mathrm{Id}_V(b_j)]_{B'} = [b_j]_{B'},$$

der j-te alte Basisvektor, geschrieben in der neuen Sprache. Deshalb „steht die Basis in der Matrix drin“. Besonders durchsichtig wird das im k^n mit $B' = E$ (Standardbasis): Wegen $[w]_E = w$ ist dann

$$M_{E \leftarrow B}(\mathrm{Id}) = \begin{pmatrix} | & & | \\ b_1 & \cdots & b_n \\ | & & | \end{pmatrix}$$

— man schreibt schlicht die Basisvektoren als Spalten nebeneinander. *Achtung:* nur weil hier $B' = E$ ist, sind es die Basisvektoren selbst; bei beliebiger Zielbasis stehen in den Spalten ihre *Koordinaten $[b_j]_{B'}$ in der neuen Basis*.

Beispiel 5.4.3 (Die schiefe Basis in der Ebene, Teil 2)**.** Für $B = (b_1, b_2)$ mit $b_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $b_2 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ aus Beispiel 5.2.4 ist

$$M_{E \leftarrow B}(\mathrm{Id}) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Probe mit dem dort berechneten $[v]_B = \begin{pmatrix} 3 \\ 2 \end{pmatrix}$:

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 5 \\ 1 \end{pmatrix} = [v]_E,$$

wie es sein muss. Diese Richtung — von der schiefen Basis in die Standardbasis — ist geschenkt. Die *nützliche* Richtung ist aber meist die andere: Gegeben ein Vektor in Standardkoordinaten, was sind seine B-Koordinaten? Dazu müssen wir die Übersetzung *umkehren*.

Invertierbare Matrizen

Übersetzen kann man in beide Richtungen. Auf Matrixebene braucht das einen Begriff, den wir hier nur so weit einführen, wie dieses Kapitel ihn benötigt — das systematische Rechnen folgt im nächsten Kapitel.

Definition 5.4.4 (Invertierbare Matrix)**.** Eine quadratische Matrix $A \in k^{n\times n}$ heißt *invertierbar*, wenn es eine Matrix $X \in k^{n\times n}$ gibt mit

$$AX = E_n \quad \text{und} \quad XA = E_n.$$

Lemma 5.4.5 (Die Inverse ist eindeutig)**.** *Sei $A \in k^{n\times n}$ invertierbar. Dann gibt es genau eine Matrix B mit $AB = BA = E_n$. Wir nennen sie* die inverse Matrix *von A und schreiben*

$$A^{-1} := B.$$

Beweis. Seien B und B' zwei solche Matrizen. Dann gilt mit der Assoziativität der Matrixmultiplikation

$$B' = B'E_n = B'(AB) = (B'A)B = E_nB = B.$$ □

Bemerkung 5.4.6. Wie man eine inverse Matrix *ausrechnet*, ist eine eigene Geschichte — sie braucht das Gaußverfahren und wird im Kapitel über lineare Gleichungssysteme erzählt. In diesem Kapitel sind alle Matrizen so klein oder so speziell, dass wir Inverse durch Hinsehen und eine Probe finden. Die Probe genügt dabei völlig: Wer ein B mit $AB = BA = E_n$ vorweist, hat die Inverse gefunden.

Der erste Ertrag des Begriffs: Basiswechselmatrizen sind *immer* invertierbar — und ihre Inversen sind genau die Übersetzungen in die Gegenrichtung.

Korollar 5.4.7 (Basiswechselmatrizen sind invers zueinander)**.** *Seien B und B' zwei Basen eines endlich-dimensionalen k-Vektorraums V. Dann sind die beiden Basiswechselmatrizen $M_{B'\leftarrow B}(\mathrm{Id}_V)$ und $M_{B\leftarrow B'}(\mathrm{Id}_V)$ invertierbar, und es gilt*

$$M_{B\leftarrow B'}(\mathrm{Id}_V) = M_{B'\leftarrow B}(\mathrm{Id}_V)^{-1}.$$

Beweis. Wir wenden Lemma 5.3.10 zweimal auf $\mathrm{Id}_V = \mathrm{Id}_V \circ \mathrm{Id}_V$ an. Einerseits gilt

$$M_{B\leftarrow B'}(\mathrm{Id}_V)\, M_{B'\leftarrow B}(\mathrm{Id}_V) = M_{B\leftarrow B}(\mathrm{Id}_V) = E_n$$

nach Beispiel 5.3.13. Andererseits gilt ebenso

$$M_{B'\leftarrow B}(\mathrm{Id}_V)\, M_{B\leftarrow B'}(\mathrm{Id}_V) = M_{B'\leftarrow B'}(\mathrm{Id}_V) = E_n.$$

Also sind beide Matrizen invertierbar und nach Lemma 5.4.5 invers zueinander. □

Bemerkung 5.4.8 (Hin- und Rückübersetzung)**.** Inhaltlich ist das Korollar keine Überraschung: Erst von B nach B' übersetzen und dann von B' zurück nach B muss jede Koordinatenspalte unverändert lassen — und die Matrix, die nichts verändert, ist E_n. Beachte, wie die Dominoregel aus dem letzten Abschnitt die Reihenfolge kontrolliert: Innen docken zweimal dieselbe Basis an.

Beispiel 5.4.9 (Die schiefe Basis in der Ebene, Teil 3)**.** Für die Matrix aus Beispiel 5.4.3 prüft man

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = E_2$$

(und ebenso in der anderen Reihenfolge). Also ist

$$M_{B \leftarrow E}(\mathrm{Id}) = M_{E \leftarrow B}(\mathrm{Id})^{-1} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

und für unser $v = \begin{pmatrix} 5 \\ 1 \end{pmatrix}$ liefert die Matrix

$$[v]_B = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 5 \\ 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 6 \\ 4 \end{pmatrix} = \begin{pmatrix} 3 \\ 2 \end{pmatrix}$$

— dasselbe Ergebnis wie das Gleichungssystem in Beispiel 5.2.4. Das ist kein Zufall, sondern der Normalfall: *Koordinaten bestimmen heißt ein Gleichungssystem lösen; die inverse Basiswechselmatrix löst alle diese Gleichungssysteme auf einen Schlag.*

Die Basiswechselformel

Nun zum Hauptsatz des Kapitels: Wie ändert sich die *Matrix einer Abbildung*, wenn man die Basen wechselt?

Korollar 5.4.10 (Basiswechselformel)**.** *Sei $F : V \to W$ linear. Seien B, B' Basen von V, und seien C, C' Basen von W. Dann gilt*

$$M_{C' \leftarrow B'}(F) = M_{C' \leftarrow C}(\mathrm{Id}_W) \cdot M_{C \leftarrow B}(F) \cdot M_{B \leftarrow B'}(\mathrm{Id}_V)\,.$$

Beweis. Wir schreiben die Abbildung als Verkettung mit zwei Identitäten:

$$F = \mathrm{Id}_W \circ F \circ \mathrm{Id}_V\,.$$

Nun wenden wir zweimal Lemma 5.3.10 an und wählen die Basen so, dass sie innen aneinander andocken: rechts die Identität mit Basen B' und B, in der Mitte F mit den Basen B und C, links die Identität mit Basen C und C'. Das ergibt genau die behauptete Gleichung. □

Bemerkung 5.4.11 (Warum die Formel erwartbar ist)**.** Eine Basiswechselmatrix ist kein neuer Operator, sondern ein Übersetzer. Liest man die rechte Seite der Formel von rechts nach links, steht dort ein vollkommen vernünftiger Arbeitsablauf:

1. $M_{B \leftarrow B'}(\mathrm{Id}_V)$: übersetze die neuen Eingabekoordinaten in die alte Sprache,
2. $M_{C \leftarrow B}(F)$: wende die *bekannte* Matrix von F an,
3. $M_{C' \leftarrow C}(\mathrm{Id}_W)$: übersetze das Ergebnis in die neue Zielsprache.

Umbenennen, anwenden, zurückbenennen — die Basiswechselformel ist die Konjugationsfigur aus dem ersten Abschnitt, nur dass Eingabe- und Ausgabesprache unabhängig voneinander gewechselt werden dürfen.

Am wichtigsten ist der Spezialfall der Endomorphismen, also $F : V \to V$ mit *einer* Basis pro Seite. Dort wird aus der Formel wortwörtlich eine Konjugation.

Korollar 5.4.12 (Basiswechsel für Endomorphismen ist Konjugation). *Sei $F : V \to V$ linear und seien B, B' Basen von V. Setze*

$$P := M_{B \leftarrow B'}(\mathrm{Id}_V).$$

Dann ist P invertierbar mit $P^{-1} = M_{B' \leftarrow B}(\mathrm{Id}_V)$, und es gilt

$$M_{B' \leftarrow B'}(F) = P^{-1} \cdot M_{B \leftarrow B}(F) \cdot P.$$

Beweis. Die Invertierbarkeit ist Korollar 5.4.7. Die Basiswechselformel mit $C = B$ und $C' = B'$ liefert

$$M_{B' \leftarrow B'}(F) = M_{B' \leftarrow B}(\mathrm{Id}_V) \cdot M_{B \leftarrow B}(F) \cdot M_{B \leftarrow B'}(\mathrm{Id}_V) = P^{-1} \cdot M_{B \leftarrow B}(F) \cdot P. \qquad \square$$

Bemerkung 5.4.13 (Achtung, Richtung von P). $P = M_{B \leftarrow B'}(\mathrm{Id}_V)$ ist die *Rück*übersetzung: sie nimmt neue Koordinaten (bezüglich B') entgegen und liefert alte (bezüglich B) — die *Gegenrichtung* zu der in Definition 5.4.1 benannten „Basiswechselmatrix von B nach B'“. Deshalb sitzt der *un*-invertierte Faktor P hier in der Rolle des g^{-1} aus der Konjugationsformel $g \circ h \circ g^{-1}$ und steht *rechts*, obwohl dort der un-invertierte Faktor links stand. Merke die Leserichtung, nicht die Position des Strichs: von rechts nach links wird die Eingabe zuerst in die bekannte alte Sprache übersetzt.

Leitbeispiel 5.4.14 (Der Schattenwurf: die Rechnung hinter der schönen Matrix). In Leitbeispiel 5.3.9 haben wir für die Schattenabbildung P die Basis $B = (e_1, e_2, d)$ mit $d = (1, 1, -1)$ gewählt und die Diagonalmatrix erhalten. Jetzt rechnen wir dasselbe noch einmal — diesmal mit der Basiswechselformel, als Probe aufs Exempel. (Um Verwechslungen zu vermeiden, nennen wir die Matrizen in diesem Beispiel A und T; der Buchstabe P gehört hier der Schattenabbildung.)

Die Übersetzungsmatrix von B in die Standardbasis hat die Basisvektoren als Spalten:

$$T := M_{E \leftarrow B}(\mathrm{Id}) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & -1 \end{pmatrix}.$$

Ein Glücksfall dieser Basis: T ist zu sich selbst invers,

$$T \cdot T = E_3,$$

wie man spaltenweise nachrechnet ($Te_1 = e_1$, $Te_2 = e_2$ und $T(1, 1, -1) = (1 + 0 - 1,\ 0 + 1 - 1,\ 0 + 0 + 1) = e_3$). Also ist $M_{B \leftarrow E}(\mathrm{Id}) = T^{-1} = T$.

Nach Korollar 5.4.12 gilt mit $A := M_{E \leftarrow E}(P)$:

$$M_{B \leftarrow B}(P) = T^{-1} A T = T A T.$$

Wir rechnen in zwei Schritten. Zuerst

$$AT = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

denn die dritte Spalte ist $Ad = P(d) = 0$. Dann

$$T(AT) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Dieselbe Diagonalmatrix wie beim direkten Protokollieren — die Basiswechselformel und die Anschauung greifen ineinander.

Der praktische Gewinn solcher Rechnungen: Man kann in der bequemen Basis *arbeiten* und am Ende zurückübersetzen. Mit der Diagonalmatrix $D := M_{B\leftarrow B}(P)$: Wer etwa A^{100} braucht, rechnet

$$A^{100} = (TDT)^{100} = TD^{100}T = TDT = A \qquad \text{(mit } D \text{ von eben)},$$

denn im Inneren heben sich alle Paare $TT = E_3$ auf und $D^{100} = D$ für unsere Diagonalmatrix. Allgemein stünde hier $TD^{100}T^{-1}$; dass zweimal *dasselbe* T auftaucht, liegt allein an der Selbstinversität $T = T^{-1}$ dieser Basis. Hundertmal Schatten werfen ist einmal Schatten werfen — was anschaulich klar war, wird in der richtigen Basis auch rechnerisch trivial.

Leitbeispiel 5.4.15 (Das Kristallgitter: eine Matrix übersetzt das Labor)**.** Wir setzen das Zahlenbeispiel aus Leitbeispiel 5.2.7 fort: Gitterbasis $G = (a_1, a_2, a_3)$ mit $a_1 = (1,0,0)$, $a_2 = (1,1,0)$, $a_3 = (0,0,2)$. Die Übersetzung von Gitter- in Laborkoordinaten hat die Gittervektoren als Spalten:

$$M_{E\leftarrow G}(\mathrm{Id}) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Für die Gegenrichtung raten wir und machen die Probe:

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{2} \end{pmatrix} = E_3$$

(und ebenso umgekehrt), also

$$M_{G\leftarrow E}(\mathrm{Id}) = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{2} \end{pmatrix}.$$

Damit wird jede Labormessung mit einer einzigen Multiplikation zur Gitterbeschreibung:

$$[v]_G = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 3 \\ 2 \\ 4 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix},$$

genau die Gitterschritte, die der Kristallograph in Leitbeispiel 5.2.7 gezählt hat. In der Praxis programmiert man diese eine Matrix — und der gesamte Messdatenstrom des Labors läuft automatisch in Kristallsprache ein.

Ein Ausblick, der sich lohnt: Die Spalten von $M_{E\leftarrow G}(\mathrm{Id})$ spannen die Elementarzelle des Gitters auf. Im Kapitel über Determinanten werden wir einer Matrix eine Zahl zuordnen, die genau das (vorzeichenbehaftete) Volumen dieser Zelle misst — und das Kristallgitter wird uns dort als Leitbeispiel wieder begegnen.

Leitbeispiel 5.4.16 (Der Schiffsmast: Kalibrierung statt Kletterei)**.** Zurück auf See (Leitbeispiel 5.2.8). Radar und Kamera sind gegeneinander verdreht, niemand kommt an den Mast, und niemand kennt den Verdrehwinkel. Gesucht ist die Übersetzung

$$M_{K\leftarrow R}(\mathrm{Id}) \qquad \text{mit} \qquad [v]_K = M_{K\leftarrow R}(\mathrm{Id})\,[v]_R.$$

Die Kalibrierung. Woher soll die Matrix kommen, wenn wir die Gerätebasen nicht sehen können? Die Antwort: aus *gemeinsamen Messungen*. Eine Matrix ist durch ihre Werte auf einer

Basis festgelegt — wir brauchen also nur zwei Schiffe, die (in Radarsprache) in unabhängige Richtungen liegen und von *beiden* Geräten gleichzeitig geortet werden. An einem klaren Morgen bieten sich zwei Frachter an:

$$\text{Frachter } u: \quad [u]_R = \begin{pmatrix} 5 \\ 0 \end{pmatrix}, \quad [u]_K = \begin{pmatrix} 3 \\ -4 \end{pmatrix},$$
$$\text{Frachter } w: \quad [w]_R = \begin{pmatrix} 0 \\ 5 \end{pmatrix}, \quad [w]_K = \begin{pmatrix} 4 \\ 3 \end{pmatrix}.$$

Frachter u liegt genau auf der ersten Radarachse: $[u]_R = 5e_1$. Aus $[u]_K = M_{K\leftarrow R}(\mathrm{Id}) \cdot 5e_1$ folgt, dass die *erste Spalte* der gesuchten Matrix gleich $\frac{1}{5}[u]_K$ ist; genauso liefert w die zweite Spalte. Also

$$M_{K\leftarrow R}(\mathrm{Id}) = \frac{1}{5}\begin{pmatrix} 3 & 4 \\ -4 & 3 \end{pmatrix}.$$

(Liegen die Kalibrierschiffe nicht so bequem auf den Radarachsen, ist es kaum schlimmer: Die Bedingungen $[u]_K = M[u]_R$ und $[w]_K = M[w]_R$ sind dann ein lineares Gleichungssystem für die Einträge von M; wie man diese löst studieren wir im nächsten Kapitel)

Der Betrieb. Ab jetzt ist die Verdrehung Software. Meldet das Radar einen neuen Kontakt bei $[v]_R = \begin{pmatrix} 10 \\ 5 \end{pmatrix}$, dann schwenkt die Kamera nach

$$[v]_K = \frac{1}{5}\begin{pmatrix} 3 & 4 \\ -4 & 3 \end{pmatrix}\begin{pmatrix} 10 \\ 5 \end{pmatrix} = \begin{pmatrix} 10 \\ -5 \end{pmatrix}$$

— und findet dort das Schiff. Beachte, was wir alles *nicht* gebraucht haben: den Verdrehwinkel nicht, die Richtung der Mastachsen nicht, keinen Schraubenschlüssel. Zwei gemeinsame Peilungen enthalten die vollständige Übersetzung. (Wer mag, liest den Winkel trotzdem ab: Die Matrix hat die Form einer Drehmatrix mit $\cos\theta = \frac{3}{5}$, $\sin\theta = -\frac{4}{5}$ — die Kamera ist um etwa 53° verdreht. Dass eine reine Drehung herauskommt, ist eine stille Konsistenzprüfung: Der Sturm hat die Geräte verdreht, aber nicht verbogen.)

Und die Konjugation? Bisher haben wir nur *Vektoren* übersetzt. Sobald ein Gerät auch *Operationen* ausführt, braucht man die volle Konjugationsfigur. Die Kamerasoftware kennt etwa den Befehl S: „spiegle das Suchmuster an der eigenen Vorausachse“ (Steuerbord und Backbord tauschen). Soll das Radar *dasselbe* Manöver in seiner Sprache ausführen, lautet der Befehl

$$M^{-1}SM \qquad \text{mit } M = M_{K\leftarrow R}(\mathrm{Id}):$$

übersetze nach Kamerasprache, spiegle dort, übersetze zurück. Das Ergebnis ist *nicht* die Spiegelung an der Radar-Vorausachse, sondern die an der mitverdrehten Kameraachse — genau wie beim Dreieck, wo das Konjugat einer Spiegelung die Spiegelung an der mitgedrehten Achse war. Drehbefehle dagegen sind hier immun: Drehungen der Ebene kommutieren miteinander, und nach Lemma 2.1.56 lässt Konjugation mit der Matrix M jede Drehung unverändert — entscheidend ist, dass M hier *selbst* eine Drehung ist; mit einer Scherung oder Spiegelung als M änderte sich eine Drehung sehr wohl. „Schwenke um 10° nach links“ heißt in beiden Gerätesprachen wörtlich dasselbe — ein kleines Echo des Prinzips, dass in abelschen Situationen die Konjugation verschwindet.

Ähnliche Matrizen

Die Konjugationsformel aus Korollar 5.4.12 verdient einen eigenen Begriff auf der Matrixseite.

Definition 5.4.17 (Ähnliche Matrizen)**.** Zwei Matrizen $A, A' \in k^{n\times n}$ heißen *ähnlich* (oder *konjugiert*), wenn es eine invertierbare Matrix $S \in k^{n\times n}$ gibt mit

$$A' = S^{-1} A S.$$

Bemerkung 5.4.18. In der Sprache des ersten Abschnitts ist A' das Konjugat von A mit S^{-1}; der *un*-invertierte Faktor S steht rechts.

Theorem 5.4.19 (Ähnlich heißt: dieselbe Abbildung in zwei Basen)**.** *Seien $A, A' \in k^{n\times n}$. Dann sind äquivalent:*

1. *A und A' sind ähnlich.*
2. *Es gibt einen n-dimensionalen k-Vektorraum V, einen Endomorphismus $F : V \to V$ und Basen B, B' von V mit*
$$A = M_{B\leftarrow B}(F) \quad \textit{und} \quad A' = M_{B'\leftarrow B'}(F).$$

Ähnliche Matrizen sind also zwei Protokolle derselben *linearen Abbildung — und umgekehrt sind zwei Protokolle derselben Abbildung stets ähnlich.*

Beweis. „(b) ⇒ (a)“: Das ist genau Korollar 5.4.12 mit $S = M_{B\leftarrow B'}(\mathrm{Id}_V)$.

„(a) ⇒ (b)“: Sei $A' = S^{-1}AS$ mit S invertierbar. Wir bauen die Situation aus (b) explizit. Als Vektorraum nehmen wir $V = k^n$, als Abbildung $F = L_A$, als erste Basis die Standardbasis $B = E$. Dann ist $M_{E\leftarrow E}(L_A) = A$ (Beispiel 5.3.6 zusammen mit Theorem 4.4.2).

Als zweite Basis nehmen wir die Spalten von S:

$$b'_j := Se_j \qquad (j = 1, \dots, n).$$

Das ist tatsächlich eine Basis: Die Abbildung L_S ist ein Isomorphismus, denn $L_{S^{-1}}$ ist ihre Umkehrabbildung — nach der Assoziativität der Matrixmultiplikation gilt ja

$$L_S(L_{S^{-1}}(v)) = S(S^{-1}v) = (SS^{-1})v = v$$

und genauso in der anderen Reihenfolge. Isomorphismen bilden Basen auf Basen ab (Theorem 4.5.1), also ist $B' = (b'_1, \dots, b'_n)$ als Bild der Standardbasis eine Basis von k^n.

Die Basiswechselmatrix von B' zur Standardbasis hat die Vektoren b'_j als Spalten, ist also genau S:

$$M_{E\leftarrow B'}(\mathrm{Id}) = S.$$

Nach Korollar 5.4.12 (mit $B = E$ und $P = S$) folgt

$$M_{B'\leftarrow B'}(L_A) = S^{-1}\, M_{E\leftarrow E}(L_A)\, S = S^{-1} A S = A'. \qquad \square$$

Proposition 5.4.20 (Ähnlichkeit ist eine Äquivalenzrelation)**.** *Auf $k^{n\times n}$ ist*

$$A \sim A' \quad :\Longleftrightarrow \quad A \textit{ und } A' \textit{ sind ähnlich}$$

eine Äquivalenzrelation.

Beweis. *Reflexivität:* $A = E_n^{-1} A\, E_n$, und E_n ist invertierbar (zu sich selbst invers).

Symmetrie: Sei $A' = S^{-1}AS$. Die Matrix S^{-1} ist invertierbar mit $(S^{-1})^{-1} = S$ (die definierenden Gleichungen $SS^{-1} = S^{-1}S = E_n$ sind symmetrisch in S und S^{-1}). Multipliziert man $A' = S^{-1}AS$ von links mit S und von rechts mit S^{-1}, erhält man

$$SA'S^{-1} = A, \qquad \text{also} \qquad A = (S^{-1})^{-1} A'\, (S^{-1}).$$

Transitivität: Sei $A' = S^{-1}AS$ und $A'' = T^{-1}A'T$. Das Produkt ST ist invertierbar mit $(ST)^{-1} = T^{-1}S^{-1}$, denn

$$(ST)(T^{-1}S^{-1}) = S(TT^{-1})S^{-1} = SS^{-1} = E_n$$

und ebenso in der anderen Reihenfolge. Einsetzen liefert

$$A'' = T^{-1}S^{-1} A\, ST = (ST)^{-1} A\, (ST). \qquad \square$$

Bemerkung 5.4.21 (Ähnlichkeitsinvarianten: das Forschungsprogramm)**.** Jetzt schließt sich der Kreis zum ersten Abschnitt. Dort war die Frage: Welche Größen einer Permutation hängen nicht von der Nummerierung ab? Antwort: alle Größen, die von Konjugation nichts merken — wie das Vorzeichen. Hier ist die Frage: Welche Größen einer Matrix hängen nicht von der Basis ab? Antwort: die *Ähnlichkeitsinvarianten* — Größen, die auf ähnlichen Matrizen denselben Wert haben. Nach Theorem 5.4.19 gilt:

Eine Ähnlichkeitsinvariante ist in Wahrheit keine Größe der Matrix, sondern eine Größe der linearen Abbildung selbst.

Solche Größen zu finden ist ein Programm, das uns durch den Rest der Vorlesung trägt: Im Kapitel über Determinanten werden wir eine Zahl $\det(A)$ konstruieren und zeigen, dass sie eine Ähnlichkeitsinvariante ist — erst dadurch dürfen wir von der Determinante *eines Endomorphismus* sprechen. Im Kapitel über Eigenwerte kommen weitere Invarianten hinzu. Und jedes Mal ist das Argument dasselbe kleine Wunder wie in Lemma 5.1.2: Irgendwo kürzt sich $S^{-1} \cdots S$ weg. (Für die Determinante ist es genau genommen kein wörtlicher Sonderfall jenes Lemmas: Auf ganz $k^{n\times n}$ ist det kein Gruppenhomomorphismus, denn $(k^{n\times n}, \cdot)$ ist keine Gruppe. Es genügt aber die Multiplikativität $\det(XY) = \det(X)\det(Y)$ zusammen mit der Invertierbarkeit von S, und deshalb gilt die Invarianz sogar für singuläre A.)

Bemerkung 5.4.22 (Rückblick: ein Begriff, viele Kostüme)**.** Zum Abschluss stellen wir die Fäden des Kapitels nebeneinander. Viermal dieselbe Figur „umbenennen, anwenden, zurückbenennen“:

- *Im Lager:* Der Roboter verpflanzt das Befüllen an einen anderen Ort — $T^{-1} \circ F \circ T$ (Leitbeispiel 5.1.1).
- *Bei Permutationen:* Zwei Nummerierungen derselben Menge unterscheiden sich um eine Konjugation in S_n; Homomorphismen in abelsche Gruppen — wie das Vorzeichen — sind dafür blind (Theorem 5.1.7).
- *In der Physik:* Eine Symmetrie ist die Aussage, dass die Konjugation der Dynamik mit einer Umbenennung (Ladungen tauschen, alles verschieben) die Dynamik nicht ändert.
- *In der linearen Algebra:* Ein Basiswechsel konjugiert die Matrix eines Endomorphismus, $M_{B'\leftarrow B'}(F) = P^{-1}\, M_{B\leftarrow B}(F)\, P$; basisunabhängige Größen sind genau die Ähnlichkeitsinvarianten.

Wer eine gute Basis wählt, macht die Matrix zur Inhaltsangabe der Abbildung — beim Schattenwurf war das eine Diagonalmatrix. Die systematische Suche nach solchen Basen beginnt im Kapitel über Eigenwerte und Eigenvektoren.

Kapitel 6

Lineare Gleichungssysteme

6.1 Definition und Darstellung

Sei k ein Körper. Ein lineares Gleichungssystem über k besteht aus Gleichungen der Form

$$\begin{aligned} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &= b_1, \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n &= b_2, \\ &\vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n &= b_m. \end{aligned}$$

Dabei sind die Skalare

$$a_{i,j} \in k \quad \text{und} \quad b_i \in k$$

bekannt. Gesucht sind die unbekannten Skalare

$$x_1, \ldots, x_n \in k.$$

Bemerkung 6.1.1. Ein lineares Gleichungssystem hat zwei Arten von Daten:

1. Die Koeffizienten $a_{i,j}$ vor den unbekannten Variablen.
2. Die rechten Seiten b_i.

Die Koeffizienten schreiben wir in eine Matrix. Die unbekannten Variablen und die rechten Seiten schreiben wir als Spaltenvektoren.

Zu dem Gleichungssystem

$$\begin{aligned} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &= b_1, \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n &= b_2, \\ &\vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n &= b_m \end{aligned}$$

gehören also die Matrix

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix} \in k^{m \times n},$$

der Vektor der Unbekannten

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in k^n$$

und der rechte Seitenvektor

$$b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \in k^m.$$

Bemerke, dass dann das lineare Gleichungssystem genau die Matrixgleichung

$$Ax = b$$

ist.

Definition 6.1.2 (Lineares Gleichungssystem)**.** Seien

$$A \in k^{m \times n} \quad \text{und} \quad b \in k^m.$$

Die Gleichung

$$Ax = b$$

heißt ein *lineares Gleichungssystem*.

Die *Lösungsmenge* dieses Gleichungssystems ist

$$LR(A, b) := \{x \in k^n \mid Ax = b\}.$$

Ist

$$b = 0,$$

dann heißt das Gleichungssystem *homogen*.

Lemma 6.1.3 (Homogene Lösungsmenge als Kern)**.** *Sei*

$$A \in k^{m \times n}.$$

Dann gilt

$$LR(A, 0) = \text{Kern}(L_A).$$

Insbesondere ist

$$LR(A, 0)$$

ein Untervektorraum von k^n.

Beweis. Nach Definition gilt

$$LR(A, 0) = \{x \in k^n \mid Ax = 0\}.$$

Die zu A gehörige lineare Abbildung ist

$$L_A : k^n \to k^m, \quad x \mapsto Ax.$$

Also ist

$$\text{Kern}(L_A) = \{x \in k^n \mid L_A(x) = 0\} = \{x \in k^n \mid Ax = 0\}.$$

Daher gilt

$$LR(A, 0) = \text{Kern}(L_A).$$

Da Kerne linearer Abbildungen Untervektorräume sind, ist $LR(A, 0)$ ein Untervektorraum von k^n. □

Bemerkung 6.1.4. Im homogenen Fall suchen wir also nicht irgendeine beliebige Menge. Wir suchen einen Untervektorraum.

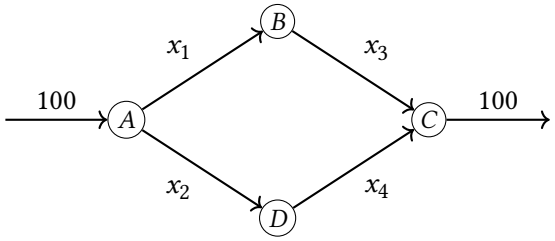
Das ist wichtig: Einen Untervektorraum können wir durch eine Basis beschreiben. Unser Ziel im homogenen Fall ist daher:

$$\text{Bestimme eine Basis von } LR(A, 0).$$

Leitbeispiel 6.1.5 (Das Straßennetz)**.** Als Leitbeispiel für dieses Kapitel begleitet uns ein kleines Netz von Einbahnstraßen. Pro Stunde strömen 100 Autos in den Knoten A hinein und verlassen das Netz wieder am Knoten C.

Wir nehmen an, dass kein Auto am Knoten C hineinfährt oder aus A hinausfährt. Die entsprechenden Straßen sind also Einbahnstraßen. Diese Annahme können wir weglassen, wenn wir die entgegen der Pfeilrichtung fahrenden Fahrzeuge negativ zählen. Das werden wir später auf den internen Wegen auf jeden Fall tun müssen.

Von A nach C führen zwei Wege: der obere über B und der untere über D.



Unbekannt sind die vier stündlichen Verkehrsstärken

$$x_1 \text{ auf } A \to B, \quad x_2 \text{ auf } A \to D, \quad x_3 \text{ auf } B \to C, \quad x_4 \text{ auf } D \to C.$$

Diese werden wie folgt gezählt: Autos, die entlang der Straße x_i in Pfeilrichtung fahren, zählen positiv. Fährt ein Auto entlang x_i, aber entgegen der Pfeilrichtung, so zählt es negativ. Die Zahl x_i ist also eine *Nettogröße*.

Die einzige Annahme ist eine Erhaltungsgröße: An jedem Knoten fließt genauso viel hinein wie hinaus — kein Auto verschwindet, keines entsteht. Das ist eine *lineare* Bedingung und liefert an den vier Knoten vier Gleichungen:

$$\begin{aligned} I: &\quad x_1 + x_2 = 100, & II: &\quad x_1 = x_3, \\ III: &\quad x_2 = x_4, & IV: &\quad x_3 + x_4 = 100. \end{aligned}$$

Das negative Zählen der Fahrten entgegen der Pfeilrichtung ist dabei notwendig: Ein Autofahrer könnte dreimal zwischen A und B hin und her pendeln, ehe er das Straßennetz wieder verlässt. Würden wir jede dieser Fahrten positiv zählen, wäre die Erhaltungsgröße I verletzt; mit Vorzeichen gezählt heben sich Hin- und Rückfahrt dagegen auf, und die Bilanz stimmt.

Um daraus eine Matrixgleichung zu machen, bringen wir zuerst alle Unbekannten auf die linke Seite (aus $x_1 = x_3$ wird $x_1 - x_3 = 0$ — daher gleich die Minuszeichen) und schreiben die Gleichungen in der Reihenfolge I, II, III, IV untereinander:

$$\begin{aligned} x_1 + x_2 \qquad\quad &= 100 \\ x_1 \qquad - x_3 \qquad &= 0 \\ x_2 \qquad\quad - x_4 &= 0 \\ x_3 + x_4 &= 100 \end{aligned}$$

Als Matrixgleichung $Mx = b$ geschrieben:

$$M = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \qquad x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}, \qquad b = \begin{pmatrix} 100 \\ 0 \\ 0 \\ 100 \end{pmatrix}.$$

Zwei Fragen tragen uns durch das Kapitel. Ist der Verkehr im Inneren durch die Randmessungen schon eindeutig festgelegt? Und wenn nicht — wie viel Freiheit bleibt?

Den homogenen Fall sehen wir dabei schon in Reinform. Setzt man alle äußeren Zu- und Abflüsse auf null, also $b = 0$, so beschreibt das System den *geschlossenen* Verkehr: Autos, die nur im Kreis fahren. Nach Lemma 6.1.3 bilden diese Kreisflüsse einen Untervektorraum, keine bloße Ansammlung von Lösungen. Dessen Basis suchen wir als Nächstes.

6.2 Homogener Fall

Wir studieren nun wie man homogene lineare Gleichungssysteme löst. Da $Ax = 0$ für $x = 0$ immer gilt, so haben wir stets eine triviale Lösung. Im homogenen Fall geht es also immer darum eine Basis des ganzen Lösungsraumes zu finden.

6.2.1 Homogene Gleichungssysteme in Zeilenstufenform

Wir beginnen mit dem Teilproblem:

Wie löst man ein homogenes Gleichungssystem, wenn die Matrix schon eine besonders einfache Form hat?

Eine besonders einfache Form ist die „Zeilenstufenform“:

Definition 6.2.1 (Zeilenstufenform)**.** Eine Matrix

$$A \in k^{m \times n}$$

ist in *Zeilenstufenform*, wenn es ein r mit

$$0 \leq r \leq m$$

und Spaltenindizes

$$1 \leq j_1 < j_2 < \cdots < j_r \leq n$$

gibt, so dass gilt:

1. Für jedes $i = 1, \ldots, r$ gilt
$$A_{i,j_i} \neq 0.$$
2. Für jedes $i = 1, \ldots, r$ und jedes $j < j_i$ gilt
$$A_{i,j} = 0.$$
3. Für jedes $i > r$ ist die i-te Zeile eine Nullzeile.

Die Einträge

$$A_{1,j_1}, \dots, A_{r,j_r}$$

heißen *Pivotstellen*. Die Spalten

$$j_1, \dots, j_r$$

heißen *Pivotspalten*.

Bemerkung 6.2.2. Anschaulich bedeutet Zeilenstufenform: In jeder neuen Nicht-Nullzeile beginnt der erste von Null verschiedene Eintrag weiter rechts als in der Zeile davor.

Die Pivotstellen bilden also eine Treppe. Die Treppe darf breite Stufen haben, aber sie geht immer nach unten und nach rechts.

Beispiel 6.2.3. Die Matrix

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

hat Zeilenstufenform. Die Pivotstellen liegen in den Spalten 1 und 3.

Definition 6.2.4 (Gebundene und freie Variablen)**.** Sei

$$A \in k^{m \times n}$$

in Zeilenstufenform. Die Variablen

$$x_{j_1}, \dots, x_{j_r}$$

zu den Pivotspalten heißen *gebundene Variablen*. Die übrigen Variablen heißen *freie Variablen*.

Bemerkung 6.2.5. Die Idee ist: Die freien Variablen dürfen wir wählen. Danach bestimmen die Gleichungen von unten nach oben eindeutig die gebundenen Variablen.

Das ist der zentrale Lesemechanismus bei Zeilenstufenform.

Beispiel 6.2.6 (Ein homogenes System in Zeilenstufenform lösen)**.** Wir betrachten

$$A = \begin{pmatrix} 1 & 2 & -1 & 0 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \in \mathbb{R}^{3 \times 4}$$

und lösen

$$Ax = 0.$$

Das zugehörige Gleichungssystem ist

$$\begin{aligned} x_1 + 2x_2 - x_3 &= 0, \\ x_3 + 3x_4 &= 0, \\ 0 &= 0. \end{aligned}$$

Die Pivotspalten sind 1 und 3. Also sind x_1 und x_3 gebunden, und x_2 und x_4 sind frei.

Wir setzen

$$x_2 = s \quad \text{und} \quad x_4 = t.$$

Dann folgt aus der zweiten Gleichung

$$x_3 = -3t.$$

Aus der ersten Gleichung folgt

$$x_1 = -2s + x_3 = -2s - 3t.$$

Also ist

$$x = \begin{pmatrix} -2s - 3t \\ s \\ -3t \\ t \end{pmatrix} = s \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \end{pmatrix} + t \begin{pmatrix} -3 \\ 0 \\ -3 \\ 1 \end{pmatrix}.$$

Daher ist

$$\begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -3 \\ 0 \\ -3 \\ 1 \end{pmatrix}$$

eine Basis von $LR(A, 0)$.

Definition 6.2.7 (Basislösungen)**.** Sei $A \in k^{m \times n}$ in Zeilenstufenform.

Zu jeder freien Variablen x_j erhalten wir eine Lösung von $Ax = 0$ wie folgt:

1. Setze
$$x_j = 1.$$
2. Setze alle anderen freien Variablen gleich 0.
3. Bestimme die gebundenen Variablen von unten nach oben.

Die so entstehenden Lösungen heißen *Basislösungen*.

Theorem 6.2.8 (Lösung eines homogenen Systems in Zeilenstufenform)**.** *Sei*

$$A \in k^{m \times n}$$

in Zeilenstufenform. Dann bilden die Basislösungen eine Basis von

$$LR(A, 0).$$

Insbesondere gilt: Ist r die Anzahl der Pivotstellen, dann gilt

$$\dim(LR(A, 0)) = n - r.$$

Beweis. Seien

$$j_1 < \cdots < j_r$$

die Pivotspalten. Die zugehörigen Variablen

$$x_{j_1}, \ldots, x_{j_r}$$

sind gebunden. Die übrigen Variablen sind frei.

Wir zeigen zuerst, dass jede Belegung der freien Variablen tatsächlich eine Lösung von $Ax = 0$ liefert, wenn man die gebundenen Variablen von unten nach oben bestimmt.

Wähle also beliebige Werte für alle freien Variablen. Nun bestimmen wir die gebundenen Variablen rückwärts. Für $i = r, r-1, \dots, 1$ setzen wir

$$x_{j_i} := -\frac{1}{A_{i,j_i}} \sum_{\ell > j_i} A_{i,\ell} x_\ell.$$

Diese Definition ist sinnvoll: Der Pivot-Eintrag A_{i,j_i} ist ungleich 0, also dürfen wir durch ihn teilen. Außerdem sind alle Variablen x_ℓ mit $\ell > j_i$ bereits bekannt. Denn entweder ist x_ℓ frei und wurde am Anfang gewählt, oder x_ℓ ist eine spätere gebundene Variable, die in einem vorherigen Rückwärtsschritt schon bestimmt wurde.

Wir prüfen nun, dass der so konstruierte Vektor x wirklich $Ax = 0$ erfüllt. Für eine Nullzeile ist die zugehörige Gleichung automatisch erfüllt. Sei also $i \leq r$. Da A in Zeilenstufenform ist, stehen vor der Pivotstelle in der i-ten Zeile nur Nullen. Daher ist die i-te Gleichung gleich

$$A_{i,j_i} x_{j_i} + \sum_{\ell > j_i} A_{i,\ell} x_\ell = 0.$$

Genau diese Gleichung wird durch die Definition von x_{j_i} erfüllt. Also erfüllt x jede Zeile von A. Damit gilt

$$Ax = 0.$$

Insbesondere sind die Basislösungen wirklich Lösungen von $Ax = 0$, denn sie entstehen aus speziellen Belegungen der freien Variablen.

Nun zeigen wir, dass die Basislösungen linear unabhängig sind. Jede Basislösung gehört zu genau einer freien Variablen. An der Stelle dieser freien Variablen hat sie den Eintrag 1. An den Stellen der anderen freien Variablen hat sie den Eintrag 0. Ein Komponentenvergleich in den freien Variablen zeigt daher, dass eine Linearkombination der Basislösungen nur dann 0 sein kann, wenn alle Koeffizienten 0 sind. Also sind die Basislösungen linear unabhängig.

Jetzt zeigen wir, dass sie den ganzen Lösungsraum erzeugen. Sei

$$x \in LR(A, 0)$$

eine beliebige Lösung. Wir lesen an x die Werte der freien Variablen ab. Sei y die Linearkombination der Basislösungen mit genau diesen Koeffizienten. Dann ist y eine Lösung von $Ay = 0$, und x und y haben dieselben Werte in allen freien Variablen.

Also ist

$$z := x - y$$

eine Lösung von $Az = 0$, bei der alle freien Variablen gleich 0 sind.

Wir zeigen, dass dann schon $z = 0$ gilt. In der letzten Nicht-Nullzeile hängt die letzte gebundene Variable nur von späteren Variablen ab. Diese späteren Variablen sind frei, also gleich 0. Daher ist auch die letzte gebundene Variable gleich 0.

Geht man nun Zeile für Zeile nach oben, sind jeweils alle späteren Variablen bereits als 0 bekannt. Die jeweilige Pivotvariable muss daher ebenfalls 0 sein. Also sind alle gebundenen Variablen gleich 0. Da auch alle freien Variablen gleich 0 sind, gilt

$$z = 0.$$

Damit ist

$$x = y.$$

Also ist x eine Linearkombination der Basislösungen.

Die Basislösungen sind also linear unabhängig und erzeugen $LR(A, 0)$. Sie bilden damit eine Basis von $LR(A, 0)$.

Es gibt genau eine Basislösung pro freier Variable. Da es $n - r$ freie Variablen gibt, gilt

$$\dim(LR(A, 0)) = n - r. \qquad \square$$

6.2.2 Elementare Zeilenoperationen

Wir wissen jetzt: Wenn eine Matrix in Zeilenstufenform ist, können wir das homogene Gleichungssystem vollständig lösen.

Die nächste Frage ist:

Wie dürfen wir ein Gleichungssystem umformen, ohne die Lösungsmenge zu verändern?

Definition 6.2.9 (Elementare Zeilenoperationen)**.** Sei

$$A \in k^{m \times n}.$$

Die folgenden Umformungen heißen *elementare Zeilenoperationen*:

1. Zwei Zeilen werden vertauscht.
2. Eine Zeile wird mit einem Skalar
$$\lambda \neq 0$$
multipliziert.
3. Zu einer Zeile wird ein Vielfaches einer anderen Zeile addiert.

Bemerkung 6.2.10 (Gleichungsebene)**.** Auf der Ebene des Gleichungssystems bedeuten diese Operationen:

1. Man vertauscht zwei Gleichungen.
2. Man multipliziert eine Gleichung mit einem Skalar $\lambda \neq 0$.
3. Man addiert ein Vielfaches einer Gleichung zu einer anderen Gleichung.

Alle drei Operationen sind vertraute Umformungen von Gleichungssystemen. Der wichtige Punkt ist: Sie verändern die Lösungsmenge nicht.

Lemma 6.2.11 (Elementare Zeilenoperationen erhalten den homogenen Lösungsraum)**.** *Sei*

$$A \in k^{m \times n}.$$

Entsteht A' aus A durch eine elementare Zeilenoperation, dann gilt

$$LR(A, 0) = LR(A', 0).$$

Auch das Streichen von Nullzeilen verändert $LR(A, 0)$ nicht.

Beweis. Wir argumentieren auf der Ebene der Gleichungen.

Das Vertauschen zweier Zeilen vertauscht nur zwei Gleichungen. Die Menge der Lösungen ändert sich dadurch nicht.

Das Multiplizieren einer Zeile mit einem Skalar $\lambda \neq 0$ verändert die Lösungsmenge ebenfalls nicht. Denn die Gleichung

$$g(x) = 0$$

ist äquivalent zu

$$\lambda g(x) = 0,$$

weil $\lambda \neq 0$ ist.

Beim dritten Typ ersetzen wir eine Gleichung durch die Summe dieser Gleichung mit einem Vielfachen einer anderen Gleichung. Wenn ein Vektor x beide ursprünglichen Gleichungen erfüllt, dann erfüllt er auch die neue Gleichung. Umgekehrt kann man diese Operation rückgängig machen, indem man das entgegengesetzte Vielfache addiert. Daher entstehen keine neuen Lösungen, und es gehen keine alten Lösungen verloren.

Eine Nullzeile entspricht der Gleichung

$$0 = 0.$$

Diese Gleichung ist immer erfüllt. Man kann sie daher streichen, ohne die Lösungsmenge zu verändern. □

Bemerkung 6.2.12. Dieses Lemma ist die Rechtfertigung für das Rechnen.

Wir dürfen elementare Zeilenoperationen explorativ benutzen. Solange wir nur diese Operationen verwenden, bleibt der homogene Lösungsraum derselbe.

6.2.3 Das Gaußsche Eliminationsverfahren

Die letzte Frage ist:

Wie bringt man eine Matrix zuverlässig in Zeilenstufenform?

Die Antwort ist das Gaußsche Eliminationsverfahren.

Theorem 6.2.13 (Gaußsches Eliminationsverfahren)**.** *Jede Matrix*

$$A \in k^{m \times n}$$

lässt sich durch elementare Zeilenoperationen in Zeilenstufenform bringen.

Beweis. Wir beschreiben ein Verfahren.

Ist A die Nullmatrix, dann ist A bereits in Zeilenstufenform.

Andernfalls gibt es mindestens einen Eintrag ungleich 0. Wähle die erste Spalte, in der ein Eintrag ungleich 0 vorkommt. Sei diese Spalte die j-te Spalte.

Durch Vertauschen von Zeilen können wir erreichen, dass in der ersten Zeile in Spalte j ein Eintrag ungleich 0 steht. Wir haben also

$$A_{1,j} \neq 0.$$

Nun eliminieren wir alle Einträge unterhalb von $A_{1,j}$. Dazu ziehen wir für jede Zeile $i > 1$ ein geeignetes Vielfaches der ersten Zeile von der i-ten Zeile ab. Danach sind alle Einträge unterhalb von $A_{1,j}$ gleich 0.

Jetzt betrachten wir die Matrix, die aus den Zeilen $2, \dots, m$ besteht. Auf diese Restmatrix wenden wir dasselbe Verfahren an.

Bei jedem Schritt verlieren wir eine Zeile. Deshalb endet das Verfahren nach endlich vielen Schritten.

Außerdem liegen die neuen Pivotstellen immer weiter rechts. Denn in den Zeilen unterhalb der ersten Pivotstelle sind alle Einträge in der Pivotspalte und in allen früheren Spalten gleich 0.

Also ist die entstehende Matrix in Zeilenstufenform. □

Bemerkung 6.2.14 (Das Backrezept)**.** Zusammengefasst funktioniert das Verfahren so:

1. Suche möglichst weit links einen Eintrag ungleich 0.

2. Bringe ihn durch Zeilentausch nach oben.
3. Eliminiere mit dieser Zeile alle Einträge darunter.
4. Wiederhole das Verfahren mit der Restmatrix.

Dies ist ein sicheres Verfahren. Man muss keinen Trick sehen. Man muss nur das Rezept ausführen.

Korollar 6.2.15 (Homogene lineare Gleichungssysteme sind lösbar durch Gauß)**.** *Sei*

$$A \in k^{m \times n}.$$

Dann kann man eine Basis von

$$LR(A, 0)$$

wie folgt bestimmen:

1. *Bringe A durch elementare Zeilenoperationen in Zeilenstufenform.*
2. *Bestimme die Pivotspalten und die freien Variablen.*
3. *Bilde die Basislösungen, indem du jeweils eine freie Variable gleich 1 und alle anderen freien Variablen gleich 0 setzt.*
4. *Lies die gebundenen Variablen von unten nach oben ab.*

Die so erhaltenen Basislösungen bilden eine Basis von $LR(A, 0)$.

Beweis. Nach Theorem 6.2.13 können wir A durch elementare Zeilenoperationen in eine Matrix A' in Zeilenstufenform bringen. Nach Lemma 6.2.11 gilt

$$LR(A, 0) = LR(A', 0).$$

Nach Theorem 6.2.8 bilden die Basislösungen von A' eine Basis von $LR(A', 0)$. Also bilden sie auch eine Basis von $LR(A, 0)$. □

Leitbeispiel 6.2.16 (Das Straßennetz: die Kreisflüsse)**.** Wir lösen das geschlossene Netz aus Leitbeispiel 6.1.5, also $b = 0$:

$$x_1 + x_2 = 0, \quad x_1 = x_3, \quad x_2 = x_4, \quad x_3 + x_4 = 0.$$

Setzt man $x_1 = x_3$ und $x_2 = x_4$ ein, so wird die erste Gleichung zu $x_1 + x_2 = 0$ und die vierte zu $x_3 + x_4 = x_1 + x_2 = 0$ — dieselbe Bedingung. Eine Gleichung ist also überflüssig; es bleibt genau eine freie Variable. Wählen wir $x_1 = t$, so folgt $x_3 = t$, $x_2 = -t$, $x_4 = -t$, insgesamt

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = t \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}.$$

Der Lösungsraum $LR(M, 0)$ ist also eindimensional mit Basislösung $(1, -1, 1, -1)$. (Wer das Netz stattdessen brav mit dem Gaußverfahren löst, erhält die freie Variable x_4 und die Basislösung $(-1, 1, -1, 1)$ — denselben Umlauf in Gegenrichtung. Beides ist richtig: Eine Basis ist nicht eindeutig, und jedes Vielfache $\neq 0$ der Basislösung erzeugt denselben Lösungsraum.) Dank der Zählkonvention aus Leitbeispiel 6.1.5 hat diese Basislösung eine wörtliche Bedeutung: positiver Fluss auf $A \to B$ und $B \to C$, dazu *negativer* auf $A \to D$ und $D \to C$ — das ist ein Auto, das den

Umlauf $A \to B \to C \to D \to A$ fährt. Auf den beiden unteren Straßen fährt es entgegen der Pfeilrichtung und wird deshalb negativ gezählt. Die Dimension des Kerns zählt hier die unabhängigen Kreise des Netzes: einen.

An dieser Stelle zahlt sich die Zählkonvention richtig aus. Wären die inneren Straßen Einbahnstraßen, dann könnte niemand den Umlauf fahren — der einzige *reale* geschlossene Verkehr wäre $t = 0$. Um das im Modell abzubilden, müssten wir die Forderungen $x_i \geq 0$ in das System aufnehmen. Aber eine Ungleichung ist *keine* lineare Gleichung mehr: Die Lösungsmenge wäre kein Untervektorraum, und die Theorie dieses Kapitels würde nicht greifen. Mit der Vorzeichen-Zählung auf Zweirichtungsstraßen bleibt dagegen alles linear, und die Basislösung ist ein echtes Fahrmanöver statt eines bloßen Rechenobjekts.

Im inhomogenen Fall kommt für den Kreisfluss noch eine zweite Lesart hinzu: Dort wird das negative Vorzeichen nicht nur „rückwärts fahren“ heißen, sondern auch „so viel Verkehr weniger auf diesem Weg“ — der Kreisfluss lässt sich dann auch als *Verlagerung* des Verkehrs vom unteren auf den oberen Weg deuten.

Bemerkung 6.2.17 (Der rote Faden)**.** Für homogene lineare Gleichungssysteme ist der Weg nun klar:

1. Matrix auf Zeilenstufenform bringen!
2. Lösen!

Der inhomogene Fall

$$Ax = b$$

kommt jetzt. Dort muss man die rechten Seiten bei den Zeilenoperationen mitführen. Außerdem ist der Lösungsraum kein Untervektorraum mehr. Weiterhin gibt es nicht immer eine Lösung.

6.3 Inhomogener Fall

Wir haben für homogene lineare Gleichungssysteme

$$Ax = 0$$

eine Lösungstheorie entwickelt. Wir betrachten daher den homogenen Fall für gelöst.

Nun betrachten wir wieder allgemeine lineare Gleichungssysteme

$$Ax = b.$$

Hier ist

$$A \in k^{m \times n} \quad \text{und} \quad b \in k^m.$$

Der wichtigste Unterschied zum homogenen Fall ist: Die Lösungsmenge ist für $b \neq 0$ kein Untervektorraum mehr. Denn wenn

$$Ax = b$$

gilt, dann ist

$$A0 = 0 \neq b.$$

Also liegt der Nullvektor für $b \neq 0$ nicht in der Lösungsmenge.

Trotzdem bleibt die Strategie fast dieselbe wie im homogenen Fall.

Wir bringen das Gleichungssystem durch erlaubte Zeilenoperationen in eine Form, die man von unten nach oben lesen kann.

Der einzige neue Punkt ist: Die rechte Seite muss bei allen Zeilenoperationen mitgeführt werden.

Definition 6.3.1 (Erweiterte Matrix)**.** Seien

$$A \in k^{m \times n} \quad \text{und} \quad b \in k^m.$$

Die *erweiterte Matrix* des linearen Gleichungssystems

$$Ax = b$$

ist die Matrix

$$(A|b) \in k^{m \times (n+1)},$$

die entsteht, indem man b als zusätzliche letzte Spalte an A anhängt.

Bemerkung 6.3.2. Die letzte Spalte der erweiterten Matrix ist keine Variablenspalte. Sie enthält die rechte Seite.

Die Variablen sind weiterhin

$$x_1, \dots, x_n.$$

Sie entsprechen den ersten n Spalten.

Beispiel 6.3.3. Das Gleichungssystem

$$\begin{aligned} x_1 + 2x_2 - x_3 &= 3, \\ 2x_1 + x_2 + x_3 &= 1 \end{aligned}$$

hat die Matrixdarstellung

$$Ax = b$$

mit

$$A = \begin{pmatrix} 1 & 2 & -1 \\ 2 & 1 & 1 \end{pmatrix} \quad \text{und} \quad b = \begin{pmatrix} 3 \\ 1 \end{pmatrix}.$$

Die erweiterte Matrix ist

$$(A|b) = \begin{pmatrix} 1 & 2 & -1 & 3 \\ 2 & 1 & 1 & 1 \end{pmatrix}.$$

Lemma 6.3.4 (Elementare Zeilenoperationen im inhomogenen Fall)**.** *Seien*

$$A \in k^{m \times n} \quad \textit{und} \quad b \in k^m.$$

Entsteht

$$(A'|b')$$

aus

$$(A|b)$$

durch elementare Zeilenoperationen, dann gilt

$$LR(A, b) = LR(A', b').$$

Beweis. Wir argumentieren wie im homogenen Fall auf der Ebene der Gleichungen.

Ein Zeilentausch vertauscht nur zwei Gleichungen. Die Lösungsmenge ändert sich dadurch nicht.

Das Multiplizieren einer Zeile mit einem Skalar $\lambda \neq 0$ verändert die Lösungsmenge ebenfalls nicht. Denn die Gleichung

$$g(x) = c$$

ist äquivalent zu

$$\lambda g(x) = \lambda c.$$

Beim dritten Typ addiert man ein Vielfaches einer Gleichung zu einer anderen Gleichung. Erfüllt ein Vektor x beide ursprünglichen Gleichungen, dann erfüllt er auch die neue Gleichung. Umgekehrt kann man diese Operation rückgängig machen, indem man das entgegengesetzte Vielfache addiert.

Also entstehen keine neuen Lösungen, und es gehen keine alten Lösungen verloren. □

Bemerkung 6.3.5 (Was ist gleich, was ist anders?)**.** Gleich wie im homogenen Fall:

1. Wir benutzen elementare Zeilenoperationen.
2. Wir bringen eine Matrix in Zeilenstufenform.
3. Wir lesen die gebundenen Variablen von unten nach oben ab.

Anders als im homogenen Fall:

1. Wir arbeiten mit der erweiterten Matrix $(A|b)$.
2. Die letzte Spalte ist die rechte Seite und keine Variable.
3. Es kann Widerspruchszeilen geben.

6.3.1 Das erweiterte Gaußverfahren

Wir lösen nun

$$Ax = b$$

mit demselben Verfahren wie im homogenen Fall, aber angewendet auf die erweiterte Matrix

$$(A|b).$$

Definition 6.3.6 (Widerspruchszeile)**.** Eine Zeile der erweiterten Matrix heißt *Widerspruchszeile*, wenn sie von der Form

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & c \end{pmatrix}$$

mit

$$c \neq 0$$

ist.

Auf Gleichungsebene bedeutet das

$$0 = c.$$

Bemerkung 6.3.7. Eine Widerspruchszeile zeigt sofort: Das Gleichungssystem hat keine Lösung. Denn die Gleichung

$$0 = c$$

kann für $c \neq 0$ von keinem Vektor erfüllt werden.

Theorem 6.3.8 (Erweitertes Gaußverfahren)**.** *Seien*

$$A \in k^{m \times n} \quad \textit{und} \quad b \in k^m.$$

Bringe die erweiterte Matrix

$$(A|b)$$

durch elementare Zeilenoperationen in Zeilenstufenform. Dann gilt:

1. *Tritt eine Widerspruchszeile auf, dann ist*

$$LR(A, b) = \emptyset.$$

2. *Tritt keine Widerspruchszeile auf, dann erhält man Lösungen wie im homogenen Fall: Die freien Variablen werden frei gewählt, und die gebundenen Variablen werden von unten nach oben bestimmt.*

Beweis. Nach Lemma 6.3.4 verändern die elementaren Zeilenoperationen die Lösungsmenge nicht. Es genügt also, das Gleichungssystem zu betrachten, das zu einer Zeilenstufenform der erweiterten Matrix gehört.

Tritt eine Widerspruchszeile auf, dann enthält das Gleichungssystem eine Gleichung der Form

$$0 = c$$

mit $c \neq 0$. Diese Gleichung kann keine Lösung haben. Also hat das gesamte Gleichungssystem keine Lösung.

Nun nehmen wir an, dass keine Widerspruchszeile auftritt. Wir betrachten nur die ersten n Spalten als Variablenspalten. Die letzte Spalte ist die rechte Seite.

Wie im homogenen Fall heißen die Variablen zu den Pivotspalten gebunden. Die übrigen Variablen heißen frei.

Wähle beliebige Werte für alle freien Variablen. Nun bestimmen wir die gebundenen Variablen von unten nach oben. Sei die Pivotstelle in Zeile i in der Spalte j_i. Dann hat die i-te Gleichung die Form

$$A_{i,j_i} x_{j_i} + \sum_{\ell > j_i} A_{i,\ell} x_\ell = b_i.$$

Der Pivot-Eintrag A_{i,j_i} ist ungleich 0. Also können wir setzen

$$x_{j_i} = \frac{1}{A_{i,j_i}} \left(b_i - \sum_{\ell > j_i} A_{i,\ell} x_\ell \right).$$

Die Variablen x_ℓ mit $\ell > j_i$ sind zu diesem Zeitpunkt bereits bekannt: Sie sind entweder frei gewählt oder wurden in einem vorherigen Rückwärtsschritt bestimmt.

Damit erfüllt der so konstruierte Vektor jede Zeile des Gleichungssystems. Also ist er eine Lösung. □

Bemerkung 6.3.9 (Speziallösung)**.** Wenn keine Widerspruchszeile auftritt, erhält man besonders leicht eine einzelne Lösung: Man setzt alle freien Variablen gleich 0 und bestimmt dann die gebundenen Variablen von unten nach oben.

Eine solche einzelne Lösung nennt man eine *Speziallösung*.

Beispiel 6.3.10. Wir betrachten das Gleichungssystem

$$\begin{aligned} x_1 + x_2 + x_3 &= 1, \\ x_2 + x_3 &= 2, \\ x_1 + 2x_2 + 2x_3 &= 3. \end{aligned}$$

Die erweiterte Matrix ist

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 2 \\ 1 & 2 & 2 & 3 \end{pmatrix}.$$

Ziehen wir die erste Zeile von der dritten Zeile ab, so erhalten wir

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

Ziehen wir nun die zweite Zeile von der dritten Zeile ab, so erhalten wir

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

Es tritt keine Widerspruchszeile auf. Die Pivotspalten sind 1 und 2. Also ist x_3 frei.
Setzen wir

$$x_3 = t,$$

dann folgt aus der zweiten Zeile

$$x_2 = 2 - t.$$

Aus der ersten Zeile folgt

$$x_1 = 1 - x_2 - x_3 = 1 - (2 - t) - t = -1.$$

Also ist

$$LR(A, b) = \left\{ \begin{pmatrix} -1 \\ 2 - t \\ t \end{pmatrix} \middle| \, t \in \mathbb{R} \right\}.$$

Beispiel 6.3.11 (Keine Lösung)**.** Wir betrachten

$$\begin{aligned} x_1 + x_2 + x_3 &= 1, \\ x_2 + x_3 &= 2, \\ x_1 + 2x_2 + 2x_3 &= 2. \end{aligned}$$

Die erweiterte Matrix ist

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

Ziehen wir die erste Zeile von der dritten Zeile ab, so erhalten wir

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

Ziehen wir nun die zweite Zeile von der dritten Zeile ab, so erhalten wir

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

Die letzte Zeile bedeutet

$$0 = -1.$$

Das ist unmöglich. Also gilt

$$LR(A, b) = \emptyset.$$

6.3.2 Die Form der Lösungsmenge

Wenn ein inhomogenes lineares Gleichungssystem lösbar ist, dann besteht seine Lösungsmenge aus einer Speziallösung plus allen Lösungen des zugehörigen homogenen Systems.

Definition 6.3.12 (Affine Verschiebung eines Untervektorraums)**.** Sei V ein k-Vektorraum, sei $U \subseteq V$ ein Untervektorraum und sei $x_0 \in V$. Dann schreiben wir

$$x_0 + U := \{x_0 + u \mid u \in U\}.$$

Eine solche Menge heißt ein *affiner Unterraum* von V. Der Untervektorraum U heißt der *Richtungsraum* dieses affinen Unterraums.

Bemerkung 6.3.13. Ein affiner Unterraum muss selbst kein Untervektorraum sein. Er ist eine verschobene Version eines Untervektorraums.

Das ist genau das, was bei inhomogenen linearen Gleichungssystemen passiert.

Theorem 6.3.14 (Speziallösung plus homogener Lösungsraum)**.** *Seien*

$$A \in k^{m \times n} \quad \textit{und} \quad b \in k^m.$$

Sei $x_0 \in k^n$ eine Lösung von $Ax = b$, es gelte also

$$Ax_0 = b.$$

Dann gilt

$$LR(A, b) = x_0 + LR(A, 0).$$

Beweis. Sei zunächst

$$x \in LR(A, b).$$

Dann gilt

$$Ax = b \quad \text{und} \quad Ax_0 = b.$$

Also ist

$$A(x - x_0) = Ax - Ax_0 = b - b = 0.$$

Daher gilt

$$x - x_0 \in LR(A, 0).$$

Also ist

$$x \in x_0 + LR(A, 0).$$

Sei umgekehrt

$$x \in x_0 + LR(A, 0).$$

Dann gibt es ein $u \in LR(A, 0)$ mit

$$x = x_0 + u.$$

Also gilt

$$Ax = A(x_0 + u) = Ax_0 + Au = b + 0 = b.$$

Daher ist

$$x \in LR(A, b).$$

Zusammen folgt

$$LR(A, b) = x_0 + LR(A, 0).$$ □

Korollar 6.3.15 (Vollständiges Lösungsverfahren im lösbaren Fall)**.** *Sei*

$$Ax = b$$

ein lösbares lineares Gleichungssystem. Dann erhält man alle Lösungen wie folgt:

1. *Bestimme mit dem erweiterten Gaußverfahren eine Speziallösung x_0.*
2. *Bestimme mit dem homogenen Gaußverfahren eine Basis von $LR(A, 0)$.*
3. *Addiere zu x_0 alle Linearkombinationen dieser Basis.*

Wenn

$$u_1, \dots, u_s$$

eine Basis von $LR(A, 0)$ ist, dann ist

$$LR(A, b) = \{x_0 + \lambda_1 u_1 + \cdots + \lambda_s u_s \mid \lambda_1, \dots, \lambda_s \in k\}.$$

Bemerkung 6.3.16 (Parallelität zum homogenen Fall)**.** Im homogenen Fall war die Lösungsmenge ein Untervektorraum:

$$LR(A, 0).$$

Im inhomogenen lösbaren Fall ist die Lösungsmenge eine Verschiebung dieses Untervektorraums:

$$x_0 + LR(A, 0).$$

Die Richtungen der Lösungsmenge kommen also weiterhin aus dem homogenen System. Neu ist nur der Aufpunkt x_0.

Leitbeispiel 6.3.17 (Das Straßennetz: eine Lösung plus alle Kreise)**.** Jetzt das volle System aus Leitbeispiel 6.1.5 mit $b = (100, 0, 0, 100)^\top$. Eine Speziallösung liest man direkt ab: Schickt man allen Verkehr über den unteren Weg, also $x_2 = x_4 = 100$ und $x_1 = x_3 = 0$, so sind alle vier Knotenbilanzen erfüllt. Das ist unser Aufpunkt

$$x_0 = (0, 100, 0, 100)^\top.$$

(Das Rezept „freie Variable null setzen“ aus dem Gaußverfahren hätte stattdessen $(100, 0, 100, 0)^\top$ geliefert — allen Verkehr über den oberen Weg. Auch das ist richtig: *Jede* Lösung taugt als Aufpunkt, die beschriebene Gerade ist dieselbe.) Nach Theorem 6.3.14 ist damit

$$LR(M, b) = x_0 + LR(M, 0) = \begin{pmatrix} 0 \\ 100 \\ 0 \\ 100 \end{pmatrix} + s \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}, \qquad s \in \mathbb{R}.$$

Der Aufpunkt ist *eine* zulässige Verkehrsführung, der Richtungsraum sind die Kreisflüsse aus Leitbeispiel 6.2.16. Anschaulich: Stehen die Zahlen an den Rändern fest, so ist die Aufteilung im Inneren keineswegs eindeutig — man darf jederzeit einen Umlauf dazuaddieren, ohne die Bilanz an irgendeinem Knoten zu stören. Der Parameter s ist dabei genau die Verkehrsstärke, die man vom unteren auf den oberen Weg verlagert:

$$x = (s,\ 100 - s,\ s,\ 100 - s)^\top.$$

Hier zeigt sich, dass die Mathematik in manchen Fällen mehr Lösungen liefert, als die Wirklichkeit zulässt. Nicht-ganzzahlige Verkehrsstärken sind über „Autos zählen“ natürlich nicht interpretierbar. Bemerke aber, dass es Lösungen gibt, die nur ganze Zahlen enthalten — das ist bei weitem nicht für jedes lineare Gleichungssystem so, hier aber durch die Interpretation wenig überraschend. Die ganzzahligen Lösungen entsprechen genau den Parametern $s \in \mathbb{Z}$.

Sind manche der inneren Straßen Einbahnstraßen, gibt es ein weiteres Problem: Dann dürfen die betroffenen Verkehrsstärken nicht negativ werden, also muss $0 \leq s \leq 100$ gelten (und zusammen mit der Ganzzahligkeit sogar $s \in \{0, \dots, 100\}$). Die volle Lösungsgerade $x_0 + LR(M, 0)$ ist unendlich lang; die bei Einbahnstraßen physikalisch sinnvollen Führungen bilden darauf nur ein beschränktes Stück — ganzzahlig gezählt sogar nur endlich viele Punkte. Die lineare Algebra bestimmt die *Richtungen* der Freiheit, die Sachfrage grenzt den zulässigen Bereich ein.

6.3.3 Das Rang-Kriterium für Lösbarkeit

Wir geben nun ein begriffliches Kriterium dafür, wann ein inhomogenes lineares Gleichungssystem überhaupt lösbar ist.

Definition 6.3.18 (Rang einer Matrix)**.** Sei

$$A \in k^{m \times n}.$$

Der *Rang* von A ist der Rang der zugehörigen linearen Abbildung

$$L_A : k^n \to k^m, \quad x \mapsto Ax.$$

Also ist

$$\operatorname{Rang}(A) := \operatorname{Rang}(L_A) = \dim\left(\operatorname{Bild}(L_A)\right).$$

Bemerkung 6.3.19. Das Bild von L_A ist genau der von den Spalten von A erzeugte Untervektorraum von k^m. Denn für

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

gilt

$$Ax = x_1 S_1 + \cdots + x_n S_n,$$

wobei

$$S_1, \ldots, S_n$$

die Spalten von A sind.

Der Rang von A ist also die Dimension des Spaltenraums von A.

Lemma 6.3.20 (Pivotstellen berechnen den Rang)**.** *Sei*

$$A \in k^{m \times n}.$$

Entsteht aus A durch elementare Zeilenoperationen eine Zeilenstufenform mit r Pivotstellen, dann gilt

$$\mathrm{Rang}(A) = r.$$

Beweis. Sei A' eine Zeilenstufenform von A mit r Pivotstellen. Elementare Zeilenoperationen erhalten den homogenen Lösungsraum. Also gilt

$$LR(A, 0) = LR(A', 0).$$

Nach dem Satz über homogene Systeme in Zeilenstufenform gilt

$$\dim\left(LR(A', 0)\right) = n - r.$$

Also ist auch

$$\dim\left(LR(A, 0)\right) = n - r.$$

Da

$$LR(A, 0) = \mathrm{Kern}(L_A)$$

gilt, folgt aus der Rangformel

$$\mathrm{Rang}(A) = n - \dim\left(\mathrm{Kern}(L_A)\right) = n - \dim\left(LR(A, 0)\right) = n - (n - r) = r. \qquad \square$$

Bemerkung 6.3.21 (Zeilenrang und Spaltenrang)**.** Die Anzahl der Pivotstellen ist genau die Anzahl der Nicht-Nullzeilen der Matrix. Aufgrund der Zeilenstufenform sind diese, wenn man sie als Vektoren interpretiert, alle auch linear unabhängig. In Zeilenstufenform ist also die Dimension des von den Spalten aufgespannten Raumes (Spaltenraums) und die Dimension des von den Zeilen aufgespannten Raumes (Zeilenraum) gleich. Der Spaltenraum ist genau das Bild der Matrix also entspricht die Dimension des Spaltenraums dem Rang.

Wegen dem Rangsatz ändert sich die Dimension des Bildes nicht, solange sich der Kern nicht ändert. Die elementaren Zeilenumformungen erhalten aber den Kern. Also, ist die Dimension des Spaltenraums einer Matrix gleich der Dimension des Spaltenraums einer zugehörigen Zeilenstufenform. Die elementaren Zeilenumformungen erhalten sogar den Zeilenraum selber (und nicht nur seine Dimension), der von den Zeilen aufgespannt wird. Also, ist die Dimension des Zeilenraums einer Matrix gleich der Dimension des Zeilenraums einer zugehörigen Zeilenstufenform.

Man sieht also, dass der Zeilenraum und der Spaltenraum einer beliebigen Matrix die gleiche Dimension haben. Dieser Fakt ist unter dem Slogan „Zeilenrang gleich Spaltenrang“ bekannt.

Theorem 6.3.22 (Rang-Kriterium für Lösbarkeit)**.** *Seien*

$$A \in k^{m \times n} \quad \textit{und} \quad b \in k^m.$$

Dann ist das lineare Gleichungssystem

$$Ax = b$$

genau dann lösbar, wenn

$$\operatorname{Rang}(A) = \operatorname{Rang}(A|b)$$

gilt.

Beweis. Seien

$$S_1, \dots, S_n$$

die Spalten von A. Dann gilt

$$Ax = x_1 S_1 + \cdots + x_n S_n.$$

Also ist

$$Ax = b$$

genau dann lösbar, wenn

$$b \in \operatorname{Span}(S_1, \dots, S_n)$$

gilt.

Der Spaltenraum von A ist

$$\operatorname{Span}(S_1, \dots, S_n).$$

Der Spaltenraum von $(A|b)$ ist

$$\operatorname{Span}(S_1, \dots, S_n, b).$$

Ist $b \in \operatorname{Span}(S_1, \dots, S_n)$, dann ändert das Hinzufügen von b das Erzeugnis nicht. Also gilt

$$\operatorname{Rang}(A) = \operatorname{Rang}(A|b).$$

Gilt umgekehrt

$$\operatorname{Rang}(A) = \operatorname{Rang}(A|b),$$

dann haben der Spaltenraum von A und der Spaltenraum von $(A|b)$ dieselbe Dimension. Da der Spaltenraum von A ein Untervektorraum des Spaltenraums von $(A|b)$ ist, folgt aus der Effektivität der Dimension (Korollar 3.3.21), dass beide Spaltenräume gleich sind. Also liegt insbesondere

$$b$$

im Spaltenraum von A. Daher ist

$$Ax = b$$

lösbar. □

Bemerkung 6.3.23. Beim Hinzufügen der Spalte b kann der Rang nicht kleiner werden. Er bleibt gleich oder wird größer.

Das Rang-Kriterium sagt: Das Gleichungssystem ist genau dann lösbar, wenn die zusätzliche Spalte b den Rang nicht größer macht.

Korollar 6.3.24 (Rang-Kriterium per Gauß)**.** *Das Gleichungssystem*

$$Ax = b$$

ist genau dann lösbar, wenn beim Gaußverfahren auf der erweiterten Matrix

$$(A|b)$$

keine Widerspruchszeile auftritt.

Beweis. Nach Lemma 6.3.20 berechnet die Anzahl der Pivotstellen den Rang. In der erweiterten Matrix $(A|b)$ gibt es genau dann eine zusätzliche Pivotstelle in der letzten Spalte, wenn eine Widerspruchszeile auftritt.

Also gilt genau dann

$$\text{Rang}(A) < \text{Rang}(A|b),$$

wenn eine Widerspruchszeile auftritt. Nach Theorem 6.3.22 ist das Gleichungssystem genau dann nicht lösbar.

Also ist es genau dann lösbar, wenn keine Widerspruchszeile auftritt. □

Bemerkung 6.3.25 (Zusammenfassung)**.** Für inhomogene lineare Gleichungssysteme gilt:

$$Ax = b \quad \longrightarrow \quad (A|b) \quad \longrightarrow \quad \text{erweitertes Gaußverfahren.}$$

Dann gibt es zwei Fälle:

$$\text{Widerspruchszeile} \quad \Longrightarrow \quad LR(A, b) = \emptyset.$$

Keine Widerspruchszeile:

$$LR(A, b) = x_0 + LR(A, 0).$$

Die Richtungen der Lösungsmenge kommen also aus dem homogenen Gleichungssystem. Die rechte Seite b entscheidet nur, ob es überhaupt Lösungen gibt, und wo die affine Lösungsmenge liegt.

6.4 Invertieren von Matrizen

Wir wenden das erweiterte Gaußverfahren nun auf eine wichtige Frage an:

Wie berechnet man die inverse Matrix?

Invertierbare Matrizen kennen wir aus Kapitel 5 (Definition 5.4.4): Eine quadratische Matrix $A \in k^{n\times n}$ heißt invertierbar, wenn es eine Matrix B mit

$$AB = E_n \quad \text{und} \quad BA = E_n$$

gibt; diese Matrix ist dann eindeutig (Lemma 5.4.5) und heißt die *inverse Matrix* A^{-1}. Dort haben wir Inverse allerdings nur durch Hinsehen und eine Probe gefunden. In diesem Abschnitt bauen wir das systematische Rechenverfahren.

Zuerst übersetzen wir den Begriff in die Sprache der linearen Abbildungen.

Lemma 6.4.1 (Invertierbar heißt: die Abbildung ist ein Isomorphismus)**.** *Sei $A \in k^{n\times n}$. Dann gilt: A ist genau dann invertierbar, wenn*

$$L_A : k^n \to k^n$$

ein Isomorphismus ist.

Beweis. Vorbereitend halten wir fest, dass für Matrizen M und N mit passenden Größen stets

$$L_M \circ L_N = L_{MN}$$

gilt, denn nach der Assoziativität der Matrixmultiplikation ist

$$M(Nv) = (MN)v$$

für alle v.

Sei zuerst A invertierbar. Dann gilt

$$L_A \circ L_{A^{-1}} = L_{AA^{-1}} = L_{E_n} = \mathrm{Id}_{k^n}$$

und ebenso

$$L_{A^{-1}} \circ L_A = \mathrm{Id}_{k^n}.$$

Also ist L_A bijektiv mit Umkehrabbildung $L_{A^{-1}}$. Als bijektive lineare Abbildung ist L_A ein Isomorphismus (Lemma 4.1.9).

Sei umgekehrt L_A ein Isomorphismus. Dann ist die Umkehrabbildung

$$(L_A)^{-1} : k^n \to k^n$$

linear. Nach Theorem 4.4.2 gibt es eine Matrix B mit

$$L_B = (L_A)^{-1}.$$

Dann gilt

$$L_{AB} = L_A \circ L_B = \mathrm{Id}_{k^n} = L_{E_n}.$$

Da die Matrix zu einer linearen Abbildung eindeutig ist, folgt

$$AB = E_n.$$

Genauso folgt $BA = E_n$. Also ist A invertierbar. □

Bemerkung 6.4.2 (Warum nur quadratische Matrizen?)**.** Für nicht-quadratische Matrizen gibt es keine beidseitigen Inversen. Gäbe es nämlich $A \in k^{m\times n}$ und $B \in k^{n\times m}$ mit

$$AB = E_m \quad \text{und} \quad BA = E_n,$$

dann wäre wie im Beweis eben L_B die Umkehrabbildung von

$$L_A : k^n \to k^m,$$

also L_A ein Isomorphismus. Isomorphe endlich dimensionale Vektorräume haben aber die gleiche Dimension. Also folgt $m = n$.

Wir schreiben ab jetzt kurz $M_n(k) := k^{n\times n}$ für die quadratischen Matrizen.

Lemma 6.4.3. *Seien V und W endlich-dimensionale k-Vektorräume. Sei $\dim(V) = \dim(W)$ und $L : V \to W$ linear und surjektiv. Dann ist L ein Isomorphismus.*

Beweis. Sei $n = \dim(V) = \dim(W)$ und $b_1, \dots, b_n$ eine Basis von V. Dann ist $L(b_1), \dots, L(b_n)$ ein Erzeugendensystem von W. Weil die Länge der Dimension entspricht ist es eine Basis. Sei G die eindeutige lineare Fortsetzung von $G(L(b_i)) = b_i$ für $i \in \{1, \dots, n\}$. Dann ist $G \circ L = \mathrm{Id}$ auf einer Basis und daher überall. Also ist G eine Linksinverse und damit ist L injektiv. Nach Voraussetzung ist L surjektiv, also insgesamt bijektiv. Eine bijektive lineare Abbildung ist ein Isomorphismus, denn ihre Umkehrabbildung ist wieder linear. □

Lemma 6.4.4 (Rechtsinverse und Linksinverse stimmen überein)**.** *Seien*

$$A, B \in M_n(k).$$

Gilt

$$AB = E_n,$$

dann gilt auch

$$BA = E_n.$$

Ebenso gilt, dass aus

$$BA = E_n$$

folgt

$$AB = E_n.$$

Beweis. Wir zeigen die erste Aussage. Die zweite folgt durch Tauschen von A und B.

Angenommen, es gilt

$$AB = E_n.$$

Dann gilt für die zugehörigen linearen Abbildungen

$$L_A \circ L_B = \mathrm{Id}_{k^n}.$$

Also ist L_A surjektiv: Zu jedem $y \in k^n$ gilt nämlich

$$y = \mathrm{Id}_{k^n}(y) = L_A(L_B(y)).$$

Da

$$L_A : k^n \to k^n$$

eine lineare Abbildung zwischen zwei endlich dimensionalen Vektorräumen gleicher Dimension ist, folgt aus der Surjektivität nach Lemma 6.4.3 bereits, dass L_A ein Isomorphismus ist.

Die Umkehrabbildung von L_A ist eindeutig. Aus

$$L_A \circ L_B = \mathrm{Id}_{k^n}$$

folgt daher

$$L_B = L_A^{-1}.$$

Also gilt auch

$$L_B \circ L_A = \mathrm{Id}_{k^n}.$$

In Matrixsprache heißt das

$$BA = E_n.$$

□

Korollar 6.4.5. *Seien*

$$A, B \in M_n(k).$$

Dann gilt:

$$B = A^{-1} \quad \Longleftrightarrow \quad AB = E_n.$$

Insbesondere reicht es, eine Rechtsinverse zu finden.

Beweis. Ist $B = A^{-1}$, dann gilt nach Definition

$$AB = E_n.$$

Gilt umgekehrt

$$AB = E_n,$$

dann gilt nach Lemma 6.4.4 auch

$$BA = E_n.$$

Also ist B eine inverse Matrix zu A. □

6.4.1 Wie findet man eine Rechtsinverse?

Sei

$$A \in M_n(k).$$

Wir suchen eine Matrix

$$B \in M_n(k)$$

mit

$$AB = E_n.$$

Schreiben wir die Spalten von B als

$$B = \begin{pmatrix} | & & | \\ y_1 & \cdots & y_n \\ | & & | \end{pmatrix},$$

dann sind die Spalten von AB genau

$$Ay_1, \ldots, Ay_n.$$

Lemma 6.4.6 (Spalten eines Matrixprodukts)**.** *Seien*

$$A \in k^{m \times n} \quad \text{und} \quad B \in k^{n \times r}.$$

Schreiben wir die Spalten von B als

$$B = \begin{pmatrix} | & & | \\ b_1 & \cdots & b_r \\ | & & | \end{pmatrix},$$

dann gilt

$$AB = \begin{pmatrix} | & & | \\ Ab_1 & \cdots & Ab_r \\ | & & | \end{pmatrix}.$$

Beweis. Die j-te Spalte von B ist

$$b_j = Be_j.$$

Daher ist die j-te Spalte von AB gleich

$$(AB)e_j = A(Be_j) = Ab_j.$$

□

Korollar 6.4.7. *Seien*

$$A, B \in M_n(k).$$

Schreiben wir die Spalten von B als

$$B = \begin{pmatrix} | & & | \\ y_1 & \cdots & y_n \\ | & & | \end{pmatrix},$$

dann gilt

$$AB = E_n$$

genau dann, wenn

$$Ay_i = e_i$$

für alle

$$i \in \{1, \dots, n\}$$

gilt.

Beweis. Nach Lemma 6.4.6 sind die Spalten von AB genau

$$Ay_1, \dots, Ay_n.$$

Die Spalten von E_n sind

$$e_1, \dots, e_n.$$

Also gilt

$$AB = E_n$$

genau dann, wenn

$$Ay_i = e_i$$

für alle $i \in \{1, \dots, n\}$ gilt. □

Bemerkung 6.4.8. Um A^{-1} zu finden, müssen wir also die n linearen Gleichungssysteme

$$Ay_1 = e_1, \quad Ay_2 = e_2, \quad \dots, \quad Ay_n = e_n$$

lösen.

Alle diese Gleichungssysteme haben dieselbe Koeffizientenmatrix A. Deshalb lösen wir sie gleichzeitig.

6.4.2 Invertieren mit dem erweiterten Gaußverfahren

Wir schreiben die rechten Seiten

$$e_1, \dots, e_n$$

nebeneinander. So entsteht die mehrfach erweiterte Matrix

$$(A|E_n).$$

Definition 6.4.9 (Strenge Zeilenstufenform)**.** Sei

$$A \in k^{m \times n}$$

eine Matrix in Zeilenstufenform. Seien

$$j_1 < \cdots < j_r$$

die Pivotspalten.

Die Matrix A heißt in *strenger Zeilenstufenform*, wenn zusätzlich gilt:

1. Alle Pivotstellen sind gleich 1, das heißt

   $$A_{i,j_i} = 1$$

   für alle $i \in \{1, \dots, r\}$.

2. In jeder Pivotspalte sind alle anderen Einträge gleich 0, das heißt

   $$A_{a,j_i} = 0$$

   für alle $i \in \{1, \dots, r\}$ und alle $a \neq i$.

Bemerkung 6.4.10. In gewöhnlicher Zeilenstufenform stehen unterhalb jeder Pivotstelle bereits Nullen. In strenger Zeilenstufenform stehen zusätzlich auch oberhalb jeder Pivotstelle Nullen, und jede Pivotstelle ist zu 1 normiert.

Diese Form ist besonders angenehm, weil man die Lösungen direkt ablesen kann.

Theorem 6.4.11 (Existenz der strengen Zeilenstufenform)**.** *Jede Matrix*

$$A \in k^{m \times n}$$

lässt sich durch elementare Zeilenoperationen in strenge Zeilenstufenform bringen.

Beweis. Nach dem Gaußschen Eliminationsverfahren lässt sich A durch elementare Zeilenoperationen zunächst in Zeilenstufenform bringen. Wir dürfen also annehmen, dass A bereits in Zeilenstufenform ist.

Seien

$$j_1 < \cdots < j_r$$

die Pivotspalten. Die Pivotstellen

$$A_{1,j_1}, \dots, A_{r,j_r}$$

sind alle ungleich 0.

Zuerst normieren wir die Pivotstellen. Für jedes $i \in \{1, \dots, r\}$ multiplizieren wir die i-te Zeile mit

$$A_{i,j_i}^{-1}.$$

Danach gilt

$$A_{i,j_i} = 1$$

für alle $i \in \{1, \dots, r\}$.

Nun eliminieren wir die Einträge oberhalb der Pivotstellen. Dazu gehen wir von unten nach oben vor. Wir lassen i die folgende Folge ablaufen

$$(r, r-1, \dots, 1)\,.$$

Iterativ ziehen wir für jede Zeile $a < i$ das A_{a,j_i}-fache der i-ten Zeile von der a-ten Zeile ab. Danach ist der Eintrag in Zeile a und Spalte j_i gleich 0.

Diese Operationen zerstören die bereits erreichten Pivotspalten nicht. Denn die i-te Zeile hat vor ihrer Pivotstelle nur Nullen. Insbesondere hat sie in allen früheren Pivotspalten

$$j_1, \dots, j_{i-1}$$

den Eintrag 0. Wenn wir also ein Vielfaches der i-ten Zeile zu einer oberen Zeile addieren, ändern sich die früheren Pivotspalten nicht.

Außerdem bleiben die Einträge unterhalb der Pivotstellen gleich 0, denn wir verändern nur Zeilen oberhalb der jeweiligen Pivotzeile.

Am Ende sind alle Pivotstellen gleich 1, und in jeder Pivotspalte stehen außerhalb der Pivotstelle nur Nullen. Also liegt eine strenge Zeilenstufenform vor. □

Theorem 6.4.12 (Matrixinvertierung durch Gauß)**.** *Sei*

$$A \in M_n(k).$$

Wir bilden die mehrfach erweiterte Matrix

$$(A|E_n).$$

Bringen wir sie durch elementare Zeilenoperationen in die (strenge Zeilenstufen-)Form

$$(E_n|C),$$

dann ist A invertierbar und

$$A^{-1} = C.$$

Wenn sich der linke Block nicht zu E_n umformen lässt, dann ist A nicht invertierbar.

Beweis. Wir betrachten die Spalten von C. Schreibe

$$C = \begin{pmatrix} | & & | \\ c_1 & \cdots & c_n \\ | & & | \end{pmatrix}.$$

Die Zeilenoperationen auf

$$(A|E_n)$$

sind genau dieselben Zeilenoperationen, die wir auf jedes der linearen Gleichungssysteme

$$Ay_i = e_i$$

anwenden würden.

Da elementare Zeilenoperationen die Lösungsmenge nicht verändern, ist das System

$$Ay_i = e_i$$

äquivalent zu dem System, das nach dem Gaußverfahren in der i-ten rechten Spalte steht.

Wenn die linke Seite zu E_n geworden ist, dann lautet das i-te System

$$E_n y_i = c_i.$$

Dieses System hat die offensichtliche Lösung

$$y_i = c_i.$$

Also gilt für jedes $i \in \{1, \dots, n\}$

$$Ac_i = e_i.$$

Nach Korollar 6.4.7 folgt

$$AC = E_n.$$

Nach Korollar 6.4.5 ist also

$$C = A^{-1}.$$

Es bleibt der Fall, dass sich der linke Block nicht zu E_n umformen lässt. Bringt man den linken Block in strenge Zeilenstufenform, dann bedeutet das: Er hat weniger als n Pivotstellen. Nach dem Rang-Kriterium gilt dann

$$\mathrm{Rang}(A) < n.$$

Also ist

$$L_A : k^n \to k^n$$

kein Isomorphismus. Nach Lemma 6.4.1 ist A daher nicht invertierbar.

□

Zur einfacheren Notation führen wir die Relation $\rightsquigarrow$ auf der Menge der Matrizen ein. Wir schreiben $A \rightsquigarrow B$ falls es eine Kette von Zeilenstufentransformationen gibt, die A in B verwandeln. Bemerke: $\rightsquigarrow$ ist eine Äquivalenzrelation.

Algorithmus 6.4.13 (Eine Matrix invertieren)**.** *Sei*

$$A \in M_n(k).$$

Um A^{-1} zu berechnen, gehen wir so vor:

1. *Bilde die mehrfach erweiterte Matrix*
$$(A|E_n).$$
2. *Führe das Gaußverfahren bis zur Zeilenstufenform aus, danach bringt man die Matrix über elementare Zeilenoperationen in strenge Zeilenstufenform.*
3. *Entsteht links die Einheitsmatrix,*
$$(A|E_n) \rightsquigarrow (E_n|C),$$
dann gilt
$$A^{-1} = C.$$
4. *Entsteht links nicht die Einheitsmatrix, dann ist A nicht invertierbar.*

Bemerkung 6.4.14 (Der rote Faden)**.** Das Verfahren ist nur das erweiterte Gaußverfahren mit mehreren rechten Seiten:

$$Ay_1 = e_1, \quad \dots, \quad Ay_n = e_n.$$

Statt diese Systeme einzeln zu lösen, lösen wir sie gleichzeitig:

$$(A|E_n) \rightsquigarrow (E_n|A^{-1}).$$

Die rechte Hälfte enthält am Ende die Spalten der inversen Matrix.

Leitbeispiel 6.4.15 (Das Straßennetz: warum es keine Inverse gibt)**.** Zum Abschluss die Frage, mit der wir das Netz aus Leitbeispiel 6.1.5 verlassen: Legt eine Randvorgabe b die Verkehrsführung im Inneren eindeutig fest — und zwar für *jedes* b? Das wäre genau dann der Fall, wenn die Netzmatrix M invertierbar ist; dann wäre $x = M^{-1}b$ die eine Lösung.

Unser M ist zwar quadratisch (4×4), aber *nicht* invertierbar. Der Grund steht schon in Leitbeispiel 6.2.16: Der Kreisfluss $(1, -1, 1, -1)$ liegt im Kern von L_M, dieser ist also nicht injektiv und damit kein Isomorphismus — nach Lemma 6.4.1 ist M nicht invertierbar. Und das ist zwingend, nicht zufällig: Sobald ein Netz auch nur einen Kreis enthält, kann man zu jeder Lösung einen Umlauf addieren — Eindeutigkeit ist dann unmöglich. Für unpassende Randvorgaben — etwa 100 hinein, aber nur 90 hinaus, also $b = (100, 0, 0, 90)^\top$ — liefert das Rang-Kriterium Theorem 6.3.22 zudem gar keine Lösung.

Ein invertierbares Netz wäre eines, in dem die Knotenbilanzen jede einzelne Straße festnageln: kein Kreis, den man drehen, keine Straße, die frei bleibt. Bei Straßennetzen dieser Bauart ist das allerdings *nie* zu erreichen — versuchen Sie gar nicht erst, eines zu zeichnen. Jede innere Straße taucht in genau zwei Knotenbilanzen auf, einmal als Abfluss und einmal als Zufluss; deshalb sind die Zeilen der Netzmatrix immer voneinander abhängig (bei unserem M gilt $-Z_1 + Z_2 + Z_3 + Z_4 = 0$, dahinter steckt die Gesamtbilanz „hinein = hinaus“).

Sortieren wir zum Abschied genau, wer hier was verhindert — denn Kreis und Gesamtbilanz sind *nicht* dasselbe Argument in zwei Gewändern. Invertierbarkeit verlangt zweierlei: eine Lösung für *jedes* b (Existenz) und jeweils nur *eine* (Eindeutigkeit). Der *Kreis* sitzt im *Kern* und zerstört die Eindeutigkeit; in Leitbeispiel 6.2.16 haben wir ausgerechnet, dass der Kern genau vom Umlauf aufgespannt wird. Die *Gesamtbilanz* ist dagegen eine Relation zwischen den *Zeilen* und zerstört die Existenz: Dieselbe Relation muss auch die rechte Seite erfüllen, lösbar sind also nur Randvorgaben mit

$$-b_1 + b_2 + b_3 + b_4 = 0,$$

sprich „hinein = hinaus“ — genau daran ist $b = (100, 0, 0, 90)^\top$ oben gescheitert.

Dass das wirklich zwei verschiedene Phänomene sind, zeigt ein Netz *ohne* Kreis: $A \to B \to C$, mit den Straßen x_1 und x_2 und 100 Autos hindurch. Die drei Knotengleichungen $x_1 = 100$, $x_1 = x_2$ und $x_2 = 100$ haben die Zeilen $(1, 0)$, $(1, -1)$ und $(0, 1)$, und wieder gilt $-Z_1 + Z_2 + Z_3 = 0$ — die Gesamtbilanz gibt es in *jedem* Netz. Aber der Kern ist trivial: Aus $x_1 = 0$ und $x_1 = x_2$ folgt $x = 0$, und tatsächlich ist der Verkehr hier eindeutig festgelegt, nämlich $x_1 = x_2 = 100$. Ohne Kreis keine Freiheit — die Zeilenrelation gefährdet nur die Existenz, nie die Eindeutigkeit.

Warum treten bei unserem M dann beide Defekte gemeinsam auf? Weil M *quadratisch* ist: Für quadratische Matrizen sind „Kern nichttrivial“ und „Zeilen abhängig“ nach der Rangtheorie äquivalent — zwei Lesarten *desselben* Rangdefekts, von denen jede für sich die Nicht-Invertierbarkeit beweist. (Beim 3×2-Netz von eben konnten die beiden nur auseinanderfallen, weil die Matrix nicht quadratisch ist — dort scheitert Invertierbarkeit schon an der Form.) Für unser Netz gilt dabei wörtlich: Kern = Kreisflüsse — das haben wir ausgerechnet. Dass sich auch in beliebigen Netzen jeder Vektor im Kern aus Kreis-Umläufen zusammensetzt, ist ein hübscher Fakt der Graphentheorie, den wir hier nur aussprechen. Kreis im Netz und Kern der Matrix sind dasselbe Phänomen — einmal in der Sprache der Straßen, einmal in der Sprache der linearen Algebra.

Kapitel 7

Die Determinante

7.1 Determinantenfunktionen

Wir beginnen mit einer abstrakten Definition. Sie legt nicht direkt eine konkrete Formel für die Determinante fest. Stattdessen beschreibt sie, welche Eigenschaften eine Determinante haben soll. Später werden wir sehen, dass diese bereits die Determinante eindeutig bestimmen.

Wie zuvor schreiben wir

$$M_n(k) := k^{n\times n}$$

für die Menge der quadratischen $n \times n$-Matrizen über einem Körper k.

Ist

$$A \in M_n(k),$$

so schreiben wir ihre Zeilen als

$$Z_1(A), \dots, Z_n(A) \in k^n.$$

Wir schreiben gelegentlich auch

$$\det(z_1, \dots, z_n).$$

Damit ist die Determinante der Matrix gemeint, deren i-te Zeile z_i ist.

Definition 7.1.1 (Determinantenfunktion)**.** Sei k ein Körper. Eine Abbildung

$$\det : M_n(k) \to k$$

heißt eine *Determinantenfunktion*, wenn sie die folgenden drei Eigenschaften erfüllt:

Determinanteneigenschaft (D1). *Linearität in jeder Zeile.*

Hält man alle Zeilen bis auf eine fest, dann hängt die Determinante linear von dieser einen Zeile ab. Wichtig ist hier das Festhalten aller anderen Zeilen!

Das heißt: Für alle $i \in \{1, \dots, n\}$, alle Zeilen $z_1, \dots, z_n, v, w \in k^n$ und alle Skalare $r, s \in k$ gilt

$$\det(z_1, \dots, z_{i-1}, rv + sw, z_{i+1}, \dots, z_n)$$

$$= r\det(z_1, \dots, z_{i-1}, v, z_{i+1}, \dots, z_n) + s\det(z_1, \dots, z_{i-1}, w, z_{i+1}, \dots, z_n).$$

Determinanteneigenschaft (D2). *Alternierung.*

Sind zwei Zeilen gleich, dann ist die Determinante gleich 0.

Das heißt: Für $i \neq j$ gilt

$$\det(z_1, \dots, z_{i-1}, v, z_{i+1}, \dots, z_{j-1}, v, z_{j+1}, \dots, z_n) = 0.$$

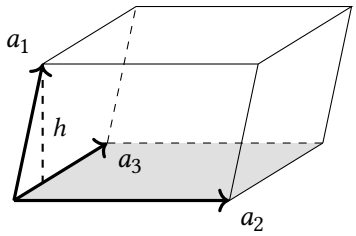
Determinanteneigenschaft (D3). *Normierung.*

Die Einheitsmatrix hat Determinante 1:

$$\det(E_n) = 1.$$

Leitbeispiel 7.1.2 (Das Kristallgitter)**.** Die drei Axiome (D1)–(D3) wirken zunächst technisch. Über den reellen Zahlen haben sie aber eine anschauliche Bedeutung, die uns durch das ganze Kapitel trägt.

Ein Kristall wird durch drei Gittervektoren $a_1, a_2, a_3 \in \mathbb{R}^3$ aufgespannt. Sie bilden die Kanten der *Elementarzelle*, eines *Spats* (Parallelepipeds) — das ist ein „schiefer Quader": sechs Seitenflächen, von denen gegenüberliegende parallel sind.



Grau unterlegt ist die von a_2 und a_3 aufgespannte *Grundfläche*; h ist die Höhe der Spitze von a_1 über der Grundflächenebene. Dieses eine Bild trägt uns durch alle Leitbeispiele des Kapitels. Schreibt man die drei Vektoren als Zeilen einer Matrix

$$A = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \in \mathbb{R}^{3\times 3},$$

so ist $\det(A)$ — das ist die Leitvorstellung, die dieses Kapitel plausibel macht — das *vorzeichenbehaftete Volumen* dieser Zelle. Und genau das erklärt die drei Axiome:

(D1) Linearität in jeder Zeile. Wir lesen „Volumen = Grundfläche mal Höhe" in der variablen Kante a_i: Die Grundfläche ist das Parallelogramm der beiden *festgehaltenen* Kanten, die Höhe der Abstand der Spitze von a_i zur Grundflächenebene (im Bild: Grundfläche von a_2, a_3, Höhe h von a_1). Verdoppelt man a_i, so verdoppelt sich die Höhe und damit das Zellvolumen. Zerlegt man $a_i = v + w$, so ist die Höhe von $v + w$ die Summe der Höhen von v und w — bei gleicher Grundfläche addieren sich also die Volumina der Zelle zu v und der Zelle zu w. (Vorsicht mit der Vorstellung: Die Zelle zu $v + w$ wird *nicht* in die Zellen zu v und w zerschnitten — es sind die *Höhen*, die sich addieren. Und liegen v und w auf verschiedenen Seiten der Grundflächenebene, stimmt die Höhen-Addition nur, wenn man die Höhe *mit Vorzeichen* zählt — schon hier zeigt sich, dass das vorzeichenbehaftete Volumen die bessere Größe ist.)

(D2) Alternierung. Fallen zwei Kanten zusammen ($a_i = a_j$), so ist die Zelle platt: Sie liegt in einer Ebene und hat Volumen 0.

(D3) Normierung. Die Standardzelle (die Zeilen von E_3) ist der Einheitswürfel mit Volumen 1.

Die Axiome sind also nicht willkürlich, sondern die definierenden Eigenschaften des Volumens. Über einem beliebigen Körper k ist det die algebraische Verallgemeinerung dieser Idee.

Beispiel 7.1.3 (Das Vorzeichen: Händigkeit)**.** Warum *vorzeichenbehaftet*? Der Betrag $|\det(A)|$ ist das Volumen, das Vorzeichen misst die *Orientierung* (Händigkeit) der Kanten.

Am klarsten ist das in der Ebene, wo „Volumen“ die Fläche bedeutet. Die Vektoren $u = (2, 0)$ und $v = (0, 3)$ spannen ein Rechteck der Fläche 6 auf:

$$\det \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} = 6 > 0.$$

Diesen Wert können wir schon jetzt allein aus den Axiomen ausrechnen — mit (D1) klammern wir 2 aus der ersten und 3 aus der zweiten Zeile aus, mit (D3) bleibt die Einheitsmatrix:

$$\det \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} = 2 \cdot 3 \cdot \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 6.$$

Die Axiome können also wirklich rechnen. Hier liegt v gegen den Uhrzeigersinn von u — ein *rechtshändiges* Paar. Weil die Determinante alternierend ist (D2), kehrt das Vertauschen der beiden Kanten das Vorzeichen um (die Regel (D5), Typ 1, weiter unten macht das präzise):

$$\det \begin{pmatrix} 0 & 3 \\ 2 & 0 \end{pmatrix} = -6 < 0.$$

Dieselbe Fläche 6, aber *linkshändig* durchlaufen. Auch eine Spiegelung erzeugt das Minuszeichen: $v' = (0, -3)$ liefert

$$\det \begin{pmatrix} 2 & 0 \\ 0 & -3 \end{pmatrix} = -6$$

(wieder per Ausklammern: $2 \cdot (-3) \cdot \det(E_2)$). Im Raum ist es die *Rechte-Hand-Regel*: Bilden (a_1, a_2, a_3) Daumen, Zeige- und Mittelfinger der rechten Hand, so ist $\det(A) > 0$ (rechtshändige Zelle); ein linkshändiges System oder eine Spiegelung liefert $\det(A) < 0$; und $\det(A) = 0$ heißt, die Zelle ist in eine Ebene kollabiert.

Bemerkung 7.1.4 (Multilinearität)**.** Die Eigenschaft (D1) heißt auch *Multilinearität in den Zeilen*. Sie unterscheidet sich deutlich von gewöhnlicher Linearität.

Sei zunächst

$$L : M_n(k) \to k$$

eine lineare Abbildung im gewöhnlichen Sinn, also linear in der ganzen Matrix. Sei außerdem

$$M : M_n(k) \to k$$

eine Abbildung, die multilinear in den Zeilen ist.

Skalieren wir die gesamte Matrix $A \in M_n(k)$ mit einem Skalar $\lambda \in k$, dann gilt für L

$$L(\lambda A) = \lambda L(A).$$

Für M gilt dagegen

$$M(\lambda A) = \lambda^n M(A).$$

Der Grund ist, dass beim Skalieren der ganzen Matrix jede der n Zeilen mit λ multipliziert wird. Durch die Linearität in jeder einzelnen Zeile erhält man daher insgesamt n Faktoren λ.

Auch bei der Addition sieht man den Unterschied. Sei $B \in M_n(k)$. Für die lineare Abbildung L gilt einfach

$$L(A + B) = L(A) + L(B).$$

Für eine multilineare Abbildung ist die entsprechende Formel viel größer. Schreiben wir die Zeilen von A als $a_1, \dots, a_n$ und die Zeilen von B als $b_1, \dots, b_n$, dann hat $A + B$ die Zeilen

$$a_1 + b_1, \dots, a_n + b_n.$$

Im Fall $n = 2$ ergibt Multilinearität:

$$M(a_1 + b_1, a_2 + b_2) = M(a_1, a_2) + M(a_1, b_2) + M(b_1, a_2) + M(b_1, b_2).$$

Es entstehen also bereits vier Summanden.

Im Fall $n = 3$ erhält man entsprechend:

$$\begin{aligned} M(a_1 + b_1, a_2 + b_2, a_3 + b_3) = {} & M(a_1, a_2, a_3) + M(a_1, a_2, b_3) + M(a_1, b_2, a_3) + M(a_1, b_2, b_3) \\ & + M(b_1, a_2, a_3) + M(b_1, a_2, b_3) + M(b_1, b_2, a_3) + M(b_1, b_2, b_3). \end{aligned}$$

Es entstehen also acht Summanden.

Allgemein entstehen bei n Zeilen 2^n Summanden. In jedem Summanden wird für jede Zeile einzeln entschieden, ob man die entsprechende Zeile aus A oder aus B nimmt.

Das zeigt auch, warum man bei einer Abbildung mit nur einem Argument erklären muss, *worin* die Multilinearität wirkt. Als Abbildung

$$M_n(k) \to k$$

hat M formal nur ein Argument, nämlich eine Matrix. Wir betrachten diese Matrix aber zugleich als geordnetes Tupel ihrer Zeilen. In diesem Sinn ist M multilinear in den Zeilen, also linear in jedem Eintrag dieses Zeilentupels.

Hat eine Abbildung dagegen von vornherein mehrere Argumente, zum Beispiel

$$F : V_1 \times \cdots \times V_n \to W,$$

dann bedeutet Multilinearität einfach: Die Abbildung ist linear in jedem einzelnen Argument, wenn alle anderen Argumente festgehalten werden.

Bemerkung 7.1.5 (Existenz einer Determinante?)**.** An dieser Stelle ist noch nicht klar, dass es eine Determinantenfunktion überhaupt gibt.

Es ist auch noch nicht klar, dass sie eindeutig ist.

Wir werden beides zeigen. Die Definition sagt zunächst nur: Falls es eine Determinante gibt, dann soll sie genau diese grundlegenden Eigenschaften haben.

Lemma 7.1.6 (Nullzeilen und elementare Zeilenoperationen)**.** *Sei*

$$\det : M_n(k) \to k$$

eine Determinantenfunktion.

Dann gelten zusätzlich die folgenden Eigenschaften:

Determinanteneigenschaft (D4). Nullzeilen.

Hat A eine Nullzeile, dann gilt

$$\det(A) = 0.$$

Determinanteneigenschaft (D5). Elementare Zeilenoperationen und die Determinante.

Typ 1 (Zeilentausch): *Entsteht B aus A, indem zwei Zeilen vertauscht werden, dann gilt*

$$\det(B) = -\det(A).$$

Typ 2 (Skalierung einer Zeile): *Entsteht B aus A, indem eine Zeile mit einem Skalar $r \in k$ multipliziert wird, dann gilt*

$$\det(B) = r\det(A).$$

Für eigentliche elementare Zeilenoperationen verlangt man $r \neq 0$. Die Formel gilt aber auch für $r = 0$.

Typ 3 (Addition eines Zeilenvielfachen): *Entsteht B aus A, indem das r-fache einer Zeile zu einer anderen Zeile addiert wird, dann gilt*

$$\det(B) = \det(A).$$

Beweis. Wir schreiben die Zeilen der Matrix als $z_1, \dots, z_n$.

Beweis von Determinanteneigenschaft (D4). Angenommen, die i-te Zeile ist die Nullzeile. Wir wählen irgendeinen Vektor $v \in k^n$. Dann gilt

$$0 = 0v + 0v.$$

Mit der Determinanteneigenschaft (D1) folgt daher

$$\begin{aligned} &\det(z_1, \dots, z_{i-1}, 0, z_{i+1}, \dots, z_n) \\ &= 0 \cdot \det(z_1, \dots, z_{i-1}, v, z_{i+1}, \dots, z_n) + 0 \cdot \det(z_1, \dots, z_{i-1}, v, z_{i+1}, \dots, z_n) \\ &= 0. \end{aligned}$$

Also gilt $\det(A) = 0$.

Beweis von Determinanteneigenschaft (D5). Wir beweisen die drei Typen getrennt.

Typ 1 (Zeilentausch): Seien die der Matrix A durch $z_1, \dots, z_n$ gegeben. Wir tauschen Zeilen i und j mit $i < j$. Alle anderen Zeilen bleiben fest. Sei $v := z_i$ und $w := z_j$.
Nach der Determinanteneigenschaft (D2) gilt

$$0 = \det(z_1, \dots, z_{i-1}, v + w, z_{i+1}, \dots, z_{j-1}, v + w, z_{j+1}, \dots, z_n).$$

Mit der Determinanteneigenschaft (D1) in den beiden betroffenen Zeilen folgt

$$\begin{aligned} 0 = \quad &\det(z_1, \dots, z_{i-1}, v, z_{i+1}, \dots, z_{j-1}, v, z_{j+1}, \dots, z_n) \\ &+ \det(z_1, \dots, z_{i-1}, v, z_{i+1}, \dots, z_{j-1}, w, z_{j+1}, \dots, z_n) \\ &+ \det(z_1, \dots, z_{i-1}, w, z_{i+1}, \dots, z_{j-1}, v, z_{j+1}, \dots, z_n) \\ &+ \det(z_1, \dots, z_{i-1}, w, z_{i+1}, \dots, z_{j-1}, w, z_{j+1}, \dots, z_n). \end{aligned}$$

Im folgenden lassen wir die z_i weg und markieren nur mit ...wo wir Einträge nicht geschrieben haben. Der erste und der letzte Summand sind nach der Determinanteneigenschaft (D2) gleich 0. Also bleibt

$$0 = \det(\dots, v, \dots, w, \dots) + \det(\dots, w, \dots, v, \dots).$$

Daher gilt

$$\det(\dots, w, \dots, v, \dots) = -\det(\dots, v, \dots, w, \dots).$$

Das ist genau die Behauptung.

Typ 2 (Skalierung einer Zeile): Entstehe B aus A, indem die i-te Zeile $Z_i(A)$ durch $rZ_i(A)$ ersetzt wird.

Das ist ein Spezialfall der Determinanteneigenschaft (D1) und es folgt sofort

$$\begin{aligned}\det(B) &= \det(Z_1(A), \dots, Z_{i-1}(A), rZ_i(A), Z_{i+1}(A), \dots, Z_n(A)) \\ &= \det(Z_1(A), \dots, Z_{i-1}(A), rZ_i(A) + 0 \cdot v, Z_{i+1}(A), \dots, Z_n(A)) \\ &= r\det(Z_1(A), \dots, Z_{i-1}(A), Z_i(A), Z_{i+1}(A), \dots, Z_n(A)) + 0 \cdot \det(\dots) \\ &= r\det(A).\end{aligned}$$

Typ 3 (Addition eines Zeilenvielfachen): Entstehe B aus A, indem das r-fache der i-ten Zeile zur j-ten Zeile addiert wird. Hier sei $i \neq j$.

Wir nennen die i-te Zeile v und die j-te Zeile w. Alle anderen Zeilen bleiben unverändert.

Dann ist die neue j-te Zeile gleich $w + rv$. Mit der Determinanteneigenschaft (D1) in der j-ten Zeile erhalten wir

$$\det(B) = \det(\dots, v, \dots, w + rv, \dots)$$

$$= \det(\dots, v, \dots, w, \dots) + r\det(\dots, v, \dots, v, \dots).$$

Der zweite Summand ist nach der Determinanteneigenschaft (D2) gleich 0, denn dort kommen zwei gleiche Zeilen vor.

Also gilt

$$\det(B) = \det(\dots, v, \dots, w, \dots) = \det(A).$$ □

Lemma 7.1.7 (Determinante einer Zeilenstufenform)**.** *Sei*

$$\det : M_n(k) \to k$$

eine Determinantenfunktion. Ist $B \in M_n(k)$ in Zeilenstufenform, dann gilt

Determinanteneigenschaft (D6). Zeilenstufenform.

Die Determinante einer quadratischen Matrix in Zeilenstufenform ist das Produkt der Diagonaleinträge:

$$\det(B) = B_{11} \cdots B_{nn}.$$

Beweis. Wir unterscheiden zwei Fälle.

Fall 1: B hat eine Nullzeile. Da B in Zeilenstufenform ist, stehen alle Nullzeilen unten. Also ist für mindestens ein i der Diagonaleintrag B_{ii} gleich 0. Damit gilt

$$B_{11} \cdots B_{nn} = 0.$$

Andererseits gilt nach der Determinanteneigenschaft (D4)

$$\det(B) = 0.$$

Also gilt die behauptete Formel.

Fall 2: B **hat keine Nullzeile.** Dann hat B genau n Pivotstellen. Seien

$$j_1 < \cdots < j_n$$

die Pivotspalten. Da $j_i \geq i$ für alle i gilt und zugleich $j_n \leq n$ ist, folgt

$$j_i = i$$

für alle $i = 1, \ldots, n$. Also sind die Pivotstellen genau die Diagonaleinträge. Insbesondere gilt

$$B_{11}, \ldots, B_{nn} \neq 0.$$

Nun eliminieren wir mit elementaren Zeilenoperationen vom Typ 3 alle Einträge oberhalb der Diagonale. Dabei gehen wir von unten nach oben vor. Diese Operationen verändern die Determinante nach der Determinanteneigenschaft (D5), Typ 3, nicht.

Am Ende erhalten wir die Diagonalmatrix

$$D = \begin{pmatrix} B_{11} & 0 & \cdots & 0 \\ 0 & B_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & B_{nn} \end{pmatrix}.$$

Also gilt

$$\det(B) = \det(D).$$

Aus der Determinanteneigenschaft (D5), Typ 2, folgt durch Ausklammern der Diagonaleinträge aus den Zeilen

$$\det(D) = B_{11} \cdots B_{nn} \det(E_n).$$

Nach der Determinanteneigenschaft (D3) ist $\det(E_n) = 1$. Also gilt

$$\det(B) = B_{11} \cdots B_{nn}.$$ □

7.2 Berechnung mit dem Gaußverfahren

Wir haben bisher noch nicht gezeigt, dass eine Determinantenfunktion überhaupt existiert. Die Eigenschaften (D1), (D2) und (D3) könnten also zunächst widersprüchlich sein. Dann gäbe es gar keine Abbildung, die diese Eigenschaften erfüllt.

Auch die folgenden Rechenregeln sind deshalb zunächst konditional zu verstehen: Wenn eine Determinantenfunktion existiert, dann muss sie sich unter Zeilenoperationen so verhalten, wie es die Determinanteneigenschaft (D5) vorschreibt.

Das ist aber bereits sehr stark. Denn das Gaußverfahren bringt jede Matrix durch elementare Zeilenoperationen in Zeilenstufenform. Auf Zeilenstufenformen ist der Wert der Determinante durch die Determinanteneigenschaft (D6) festgelegt. Also kann es höchstens eine Determinantenfunktion geben.

Algorithmus 7.2.1 (Gaußscher Berechnungsalgorithmus)**.** *Sei*

$$A \in M_n(k).$$

Angenommen, es existiert eine Determinantenfunktion

$$\det : M_n(k) \to k.$$

Dann kann $\det(A)$ *mit dem Gaußverfahren berechnet werden. Das heißt man bringt* A *durch elementare Zeilenoperationen in eine Zeilenstufenform* B*. Dabei führen wir einen Skalar* $c \in k$ *mit. Zu jedem Zeitpunkt soll gelten:*

$$\det(\textit{aktuelle Matrix}) = c \det(A).$$

Am Anfang ist die aktuelle Matrix gleich A*, also setzen wir* $c = 1$*.*
Bei den elementaren Zeilenoperationen aktualisieren wir c *wie folgt:*

Typ 1 (Zeilentausch): *Wird ein Zeilentausch durchgeführt, dann ersetzen wir*

$$c \quad \textit{durch} \quad -c.$$

Typ 2 (Skalierung einer Zeile): *Wird eine Zeile mit* $r \neq 0$ *multipliziert, dann ersetzen wir*

$$c \quad \textit{durch} \quad rc.$$

Typ 3 (Addition eines Zeilenvielfachen): *Wird ein Vielfaches einer Zeile zu einer anderen Zeile addiert, dann bleibt* c *unverändert.*

Am Ende erhalten wir eine Matrix B *in Zeilenstufenform. Dann gilt nach Lemma 7.1.7*

$$\det(B) = B_{1,1} B_{2,2} \cdots B_{n,n}.$$

Da $\det(B) = c \det(A)$ *gilt, erhalten wir*

$$\det(A) = c^{-1} B_{11} B_{22} \cdots B_{nn}.$$

Proposition 7.2.2 (Gauß bestimmt jede Determinantenfunktion)**.** *Angenommen, es existiert eine Determinantenfunktion*

$$\det : M_n(k) \to k.$$

Dann berechnet der Algorithmus 7.2.1 für jede Matrix $A \in M_n(k)$ *den Wert* $\det(A)$*.*

Beweis. Die Behauptung folgt unmittelbar aus den Determinanteneigenschaften (D4) und (D5) und aus Lemma 7.1.7. Die Aktualisierung des Faktors c ist genau so gewählt, dass nach jedem Schritt gilt:

$$\det(\text{aktuelle Matrix}) = c \det(A).$$

Für die Zeilenstufenform B berechnet Lemma 7.1.7 dann $\det(B)$. Also ist auch $\det(A)$ bestimmt. □

Leitbeispiel 7.2.3 (Das Kristallgitter: Scherung erhält das Volumen)**.** Warum darf man die Determinante überhaupt mit Gauß-Elimination ausrechnen? Im Kristallgitter Leitbeispiel 7.1.2 ist der Grund sichtbar: Die drei elementaren Zeilenoperationen sind Manipulationen der Elementarzelle.

- **Typ 3** (das r-fache einer Zeile zu einer anderen addieren) ersetzt eine Kante a_i durch $a_i + r a_j$: Man *schert* die Zelle — wie einen Kartenstapel, den man schräg schiebt: Die Spitze der Kante wandert parallel zur Grundfläche. Grundfläche und Höhe bleiben, also auch das Volumen — det ändert sich nicht (D5, Typ 3).

- **Typ 1** (Zeilentausch) vertauscht zwei Kanten. Aufgepasst: Als Punktmenge ist der Spat danach *derselbe*, sein Volumen auch! Was sich umkehrt, ist die *Reihenfolge* der Kanten, also die Händigkeit aus Beispiel 7.1.3 — die Determinante misst das geordnete Tripel (a_1, a_2, a_3), nicht bloß die Punktmenge. Deshalb wechselt det das Vorzeichen (D5, Typ 1).
- **Typ 2** (Skalierung) streckt eine Kante um r und damit das Volumen um r.

Der Algorithmus bringt die *Matrix* in Dreiecksform — die Zelle ist dann so gestellt, dass sich ihr Volumen nach Lemma 7.1.7 einfach als Produkt der Diagonaleinträge ablesen lässt — und führt dabei genau Buch über die aufgesammelten Vorzeichen und Streckfaktoren.

Korollar 7.2.4 (Eindeutigkeit der Determinante)**.** *Es gibt höchstens eine Determinantenfunktion*

$$\det : M_n(k) \to k.$$

Beweis. Seien $\det_1$ und $\det_2$ zwei Determinantenfunktionen. Nach Proposition 7.2.2 werden beide durch denselben Gauß-Algorithmus berechnet. Also gilt für jede Matrix $A \in M_n(k)$

$$\det_1(A) = \det_2(A).$$

Damit sind die beiden Abbildungen gleich. □

Bemerkung 7.2.5 (Logischer Status)**.** Das Korollar beweist noch nicht, dass eine Determinantenfunktion existiert. Es beweist nur: Falls eine Determinantenfunktion existiert, dann ist sie eindeutig.

Insbesondere muss man an dieser Stelle noch nicht wissen, ob verschiedene mögliche Gaußwege immer denselben Zahlenwert liefern. Wenn die Determinante existiert, dann müssen sie denselben Wert liefern. Die Existenz beweisen wir danach durch eine konkrete Formel.

7.3 Existenz: die Leibnizformel

Wir haben nun gezeigt, dass es höchstens eine Determinantenfunktion geben kann. Es bleibt zu zeigen, dass es tatsächlich eine gibt.

Dafür benutzen wir das Vorzeichen von Permutationen. Für $\sigma \in S_n$ bezeichnen wir mit

$$\operatorname{signum}(\sigma) \in \{1, -1\}$$

das Vorzeichen von σ.

Theorem 7.3.1 (Leibnizformel)**.** *Sei k ein Körper. Für $A \in M_n(k)$ setzen wir*

$$\Delta(A) := \sum_{\sigma \in S_n} \operatorname{signum}(\sigma) A_{1,\sigma(1)} A_{2,\sigma(2)} \cdots A_{n,\sigma(n)}.$$

Dann ist

$$\Delta : M_n(k) \to k$$

eine Determinantenfunktion. Wie bei det *schreiben wir auch $\Delta(z_1, \ldots, z_n)$ für den Wert von Δ auf der Matrix mit Zeilen $z_1, \ldots, z_n$.*

Beweis. Wir prüfen die Determinanteneigenschaften (D1), (D2) und (D3).

Determinanteneigenschaft (D1). Wir zeigen die Linearität in einer festen Zeile. Sei also $i \in \{1, \dots, n\}$ fest. Alle Zeilen außer der i-ten seien fest vorgegeben. Seien $v, w \in k^n$ und $r, s \in k$.

In jedem Summanden der Leibnizformel kommt aus der i-ten Zeile genau ein Faktor vor, nämlich der Eintrag in Spalte $\sigma(i)$. Ersetzen wir die i-te Zeile durch $rv + sw$, dann wird dieser Faktor zu

$$(rv + sw)_{\sigma(i)} = rv_{\sigma(i)} + sw_{\sigma(i)}.$$

Daher können wir die Summe mit dem Distributivgesetz aufspalten:

$$\Delta(z_1, \dots, z_{i-1}, rv + sw, z_{i+1}, \dots, z_n)$$

$$= r\Delta(z_1, \dots, z_{i-1}, v, z_{i+1}, \dots, z_n) + s\Delta(z_1, \dots, z_{i-1}, w, z_{i+1}, \dots, z_n).$$

Also erfüllt Δ die Determinanteneigenschaft (D1).

Determinanteneigenschaft (D2). Angenommen, die p-te und die q-te Zeile von A sind gleich, wobei $p \neq q$. Sei $\tau = (p\ q) \in S_n$ die Transposition, die p und q vertauscht.

Wir paaren jeden Summanden zur Permutation σ mit dem Summanden zur Permutation $\sigma \circ \tau$. Diese Paarung hat keine Fixpunkte und zerlegt S_n in Zweierpaare.

Da τ eine Transposition ist, gilt

$$\operatorname{signum}(\sigma \circ \tau) = -\operatorname{signum}(\sigma).$$

Außerdem sind die Produkte der Matrixeinträge in den beiden gepaarten Summanden gleich. Denn $\sigma \circ \tau$ vertauscht nur die beiden ausgewählten Spalteneinträge in den Zeilen p und q, und diese beiden Zeilen sind gleich. Also gilt

$$A_{1,\sigma(1)} \cdots A_{n,\sigma(n)} = A_{1,(\sigma\circ\tau)(1)} \cdots A_{n,(\sigma\circ\tau)(n)}.$$

Die beiden gepaarten Summanden haben daher entgegengesetztes Vorzeichen und heben sich auf. Also ist die ganze Summe gleich 0. Damit erfüllt Δ die Determinanteneigenschaft (D2).

Determinanteneigenschaft (D3). Wir betrachten die Einheitsmatrix E_n. Für $\sigma \in S_n$ ist das Produkt

$$(E_n)_{1,\sigma(1)}(E_n)_{2,\sigma(2)} \cdots (E_n)_{n,\sigma(n)}$$

genau dann gleich 1, wenn $\sigma(i) = i$ für alle i gilt. Das ist genau für $\sigma = \mathrm{Id}$ der Fall. Für alle anderen Permutationen ist mindestens ein Faktor gleich 0. Also bleibt in der Leibnizformel nur der Summand zur Identität übrig. Daher gilt

$$\Delta(E_n) = \operatorname{signum}(\mathrm{Id}) = 1.$$

Damit erfüllt Δ die Determinanteneigenschaft (D3).

Also ist Δ eine Determinantenfunktion. □

Korollar 7.3.2 (Existenz und Eindeutigkeit der Determinante)**.** *Für jeden Körper k und jedes $n \geq 1$ gibt es genau eine Determinantenfunktion*

$$\det : M_n(k) \to k.$$

Beweis. Die Existenz folgt aus der Leibnizformel in Theorem 7.3.1. Die Eindeutigkeit folgt aus Korollar 7.2.4. □

Korollar 7.3.3 (Wohldefiniertheit der Gauß-Berechnung)**.** *Der Gauß-Algorithmus zur Berechnung der Determinante liefert unabhängig von allen zulässigen Entscheidungen denselben Wert. Insbesondere ist es egal, welche Pivotzeilen man wählt, in welcher zulässigen Reihenfolge man weiterrechnet und welche Zeilenstufenform am Ende entsteht.*

Beweis. Nach Korollar Korollar 7.3.2 existiert genau eine Determinantenfunktion. Nach Proposition 7.2.2 berechnet jedes Gauß-Verfahren diese eine Funktion. Also können verschiedene zulässige Gauß-Verfahren nicht verschiedene Werte liefern. □

Bemerkung 7.3.4. Korollar 7.3.3 ist inhaltlich wichtig. Es gibt sehr viele verschiedene Wege, eine Matrix mit Zeilenoperationen auf Zeilenstufenform zu bringen. Man kann andere Pivotzeilen wählen, Zeilen früher oder später skalieren, oder Einträge in anderer Reihenfolge eliminieren.

Dass trotzdem immer dieselbe Zahl herauskommt, ist nicht selbstverständlich. Es folgt daraus, dass die abstrakten Eigenschaften (D1), (D2) und (D3) tatsächlich widerspruchsfrei sind und die Determinante eindeutig bestimmen.

Theorem 7.3.5 (Determinante der transponierten Matrix)**.** *Sei k ein Körper und sei $A \in M_n(k)$. Dann gilt*

$$\det(A^\top) = \det(A).$$

Beweis. Wir benutzen die Leibnizformel. Für jedes $\sigma \in S_n$ gilt

$$(A^\top)_{i,\sigma(i)} = A_{\sigma(i),i}$$

für alle $i \in \{1, \dots, n\}$. Daher ist

$$\det(A^\top) = \sum_{\sigma \in S_n} \operatorname{signum}(\sigma) A_{\sigma(1),1} \cdots A_{\sigma(n),n}.$$

Setze nun $\tau := \sigma^{-1}$. Die Abbildung $\sigma \mapsto \sigma^{-1}$ ist eine Bijektion von S_n auf sich, denn sie ist ihre eigene Umkehrabbildung. Daher wissen wir: Wenn σ alle Permutationen aus S_n durchläuft, dann durchläuft auch τ alle Permutationen aus S_n. Außerdem gilt $\operatorname{signum}(\sigma) = \operatorname{signum}(\tau)$, denn signum ist ein Gruppenhomomorphismus und

$$\operatorname{signum}(\sigma) \operatorname{signum}(\sigma^{-1}) = \operatorname{signum}(\mathrm{Id}) = 1.$$

Aus $\tau = \sigma^{-1}$ folgt: Wenn $\sigma(i) = j$ gilt, dann gilt $i = \tau(j)$. Also ist

$$A_{\sigma(1),1} \cdots A_{\sigma(n),n} = A_{1,\tau(1)} \cdots A_{n,\tau(n)}.$$

Hier benutzen wir nur, dass das Produkt im Körper kommutativ ist. Damit erhalten wir

$$\det(A^\top) = \sum_{\tau \in S_n} \operatorname{signum}(\tau) A_{1,\tau(1)} \cdots A_{n,\tau(n)} = \det(A).$$ □

Bemerkung 7.3.6 (Konzeptionelle Deutung)**.** Ein Summand der Leibnizformel wählt aus jeder Zeile und aus jeder Spalte genau einen Eintrag aus. Beim Transponieren werden die Rollen von Zeilen und Spalten vertauscht. Die zugehörige Permutation wird dadurch durch ihre inverse Permutation ersetzt. Das Vorzeichen ändert sich dabei nicht.

Danach darf man auch folgern: Alle Rechenregeln für Zeilen gelten entsprechend für Spalten.

7.4 Determinante, Rang und Invertierbarkeit

Bisher haben wir die Determinante axiomatisch beschrieben und berechnet. In diesem Abschnitt zeigt sich ihr diagnostischer Wert: Am Verschwinden der Determinante erkennt man, dass der Rang abfällt und die Matrix nicht invertierbar ist.

Theorem 7.4.1 (Determinanten erkennen Nicht-Invertierbarkeit)**.** *Sei $A \in M_n(k)$. Dann sind äquivalent:*

$$\det(A) = 0 \quad \Longleftrightarrow \quad \mathrm{Rang}(A) < n \quad \Longleftrightarrow \quad A \text{ ist nicht invertierbar.}$$

Beweis. Wir bringen A mit elementaren Zeilenoperationen auf Zeilenstufenform B. Elementare Zeilenoperationen verändern den Rang nicht. Außerdem verändern sie die Determinante nach der Determinanteneigenschaft (D5) höchstens um einen Faktor ungleich 0. Also gilt

$$\det(A) = 0 \quad \Longleftrightarrow \quad \det(B) = 0.$$

Nach Lemma 7.1.7 gilt

$$\det(B) = B_{11}B_{22}\cdots B_{nn}.$$

Da B in Zeilenstufenform ist, ist dieses Produkt genau dann ungleich 0, wenn B vollen Rang n hat. Also gilt

$$\det(B) = 0 \quad \Longleftrightarrow \quad \mathrm{Rang}(B) < n.$$

Da elementare Zeilenoperationen den Rang nicht verändern, ist dies äquivalent zu

$$\mathrm{Rang}(A) < n.$$

Schließlich ist A genau dann invertierbar, wenn die zugehörige lineare Abbildung

$$L_A : k^n \to k^n$$

ein Isomorphismus ist. Nach Lemma 6.4.3 reicht dafür Surjektivität. Surjektivität von L_A ist aber äquivalent zu

$$\mathrm{Rang}(A) = n.$$

Also gilt

$$A \text{ ist nicht invertierbar} \quad \Longleftrightarrow \quad \mathrm{Rang}(A) < n.$$

Damit sind alle Äquivalenzen gezeigt. □

Bemerkung 7.4.2 (Warum die Determinante mehr ist als ein Rangtest)**.** Für die reine Frage, ob eine konkrete Matrix invertierbar ist, ist der Rang zunächst oft der direkteste Zugang. Man kann ihn mit dem Gauß-Verfahren sehr zuverlässig berechnen.

Die Determinante hat aber einen anderen Vorteil: Sie ist nicht nur ein diskreter Wert wie der Rang, sondern ein algebraischer Ausdruck in den Matrixeinträgen. Schon die Leibnizformel zeigt, dass $\det(A)$ ein Polynom in den Einträgen von A ist. Der Rang dagegen ist algebraisch deutlich unschöner.

Über $\mathbb{R}$ kann man deshalb zusätzlich analytische Information sehen. Sei zum Beispiel $A \in M_n(\mathbb{R})$ von vollem Rang. Für jedes $r \neq 0$ hat auch rA vollen Rang, also gilt

$$\mathrm{Rang}(rA) = n.$$

Wenn $r \to 0$, dann geht rA im Sinne der Analysis gegen die Nullmatrix. Der Rang bleibt für $r \neq 0$ trotzdem konstant gleich n und springt erst bei $r = 0$.

Die Determinante sieht diesen Übergang feiner. Wegen der Determinanteneigenschaft (D1) in jeder Zeile gilt

$$\det(rA) = r^n \det(A).$$

Also geht auch

$$\det(rA) \to 0$$

für $r \to 0$. Die Determinante erkennt also nicht nur, ob eine Matrix invertierbar ist, sondern misst auch algebraisch, wie sich eine Matrix einer singulären Situation nähert.

Das wird später besonders wichtig bei der Berechnung von sogenannten „Eigenwerten“.

Leitbeispiel 7.4.3 (Das Kristallgitter: wann die Zelle kollabiert)**.** Für das Gitter Leitbeispiel 7.1.2 liest sich Theorem 7.4.1 unmittelbar. $\det(A) = 0$ heißt: Die drei Gittervektoren sind linear abhängig, einer liegt in der von den beiden anderen aufgespannten Ebene. Dann ist die Zelle platt gedrückt — sie hat kein dreidimensionales Volumen mehr, und das „Gitter“ füllt höchstens noch eine Ebene. Ein echter dreidimensionaler Kristall verlangt also $\det(A) \neq 0$, gleichbedeutend damit, dass A invertierbar ist und die Gittervektoren eine Basis des $\mathbb{R}^3$ bilden. Determinante null, Rangabfall und Kollaps der Zelle sind ein und dasselbe Phänomen.

7.5 Elementarmatrizen und die Produktformel

7.5.1 Matrizen kodieren Zeilenoperationen

Die elementaren Zeilenoperationen lassen sich selbst wieder als Matrizen ausdrücken. Die Idee ist sehr einfach: Eine Zeilenoperation ist dadurch bestimmt, was sie mit den Zeilen einer Matrix macht. Wendet man dieselbe Zeilenoperation auf die Einheitsmatrix an, dann erhält man eine Matrix, die diese Zeilenoperation durch Linksmultiplikation ausführt.

Tatsächlich kann man, wie wir sehen werden jede Matrix als (sehr komplexe) Zeilenoperation kodieren und umgekehrt.

Definition 7.5.1 (Elementarmatrizen)**.** Sei ρ eine elementare Zeilenoperation auf $n \times n$-Matrizen. Die zu ρ gehörige *Elementarmatrix* ist

$$O_\rho := \rho(E_n).$$

Die drei Typen sind:

Typ 1 (Zeilentausch): Vertauscht ρ die Zeilen i und j, dann entsteht O_ρ aus E_n, indem man dort die Zeilen i und j vertauscht.

Typ 2 (Skalierung einer Zeile): Multipliziert ρ die Zeile i mit einem Skalar $r \neq 0$, dann entsteht O_ρ aus E_n, indem man dort die Zeile i mit r multipliziert.

Typ 3 (Addition eines Zeilenvielfachen): Addiert ρ das r-fache der Zeile i zur Zeile j, dann entsteht O_ρ aus E_n, indem man dort das r-fache der Zeile i zur Zeile j addiert.

Lemma 7.5.2 (Elementarmatrizen führen Zeilenoperationen aus)**.** *Sei ρ eine elementare Zeilenoperation auf $n \times n$-Matrizen und sei*

$$O_\rho = \rho(E_n)$$

die zugehörige Elementarmatrix. Dann gilt für jede Matrix $A \in M_n(k)$:

$$O_\rho A = \rho(A).$$

Beweis. Die Zeilen von O_ρ sagen genau, welche Linearkombinationen der ursprünglichen Zeilen gebildet werden sollen. Bei der Multiplikation $O_\rho A$ passiert mit den Zeilen von A genau dasselbe. Genauer gilt für jede Matrix $O \in M_n(k)$:

$$Z_i(OA) = \sum_{\ell=1}^{n} O_{i\ell} Z_\ell(A).$$

Die i-te Zeile von OA ist also dieselbe Linearkombination der Zeilen von A, wie die i-te Zeile von O eine Linearkombination der Standardzeilen ist. Für $O = O_\rho$ sind diese Linearkombinationen gerade durch die Zeilenoperation ρ vorgegeben. Also gilt

$$O_\rho A = \rho(A). \qquad \square$$

7.5.2 Elementarmatrizen und die Determinante

Lemma 7.5.3 (Determinanten von Elementarmatrizen)**.** *Sei O_ρ eine Elementarmatrix. Dann gilt:*

Typ 1 (Zeilentausch): *Ist O_ρ eine Zeilentauschmatrix, dann gilt*

$$\det(O_\rho) = -1.$$

Typ 2 (Skalierung einer Zeile): *Ist O_ρ eine Skalierungsmatrix mit Faktor $r \neq 0$, dann gilt*

$$\det(O_\rho) = r.$$

Typ 3 (Addition eines Zeilenvielfachen): *Ist O_ρ eine Additionsmatrix, dann gilt*

$$\det(O_\rho) = 1.$$

Beweis. Nach Definition ist

$$O_\rho = \rho(E_n).$$

Wir wenden also die Zeilenoperation ρ auf die Einheitsmatrix an. Nach der Determinanteneigenschaft (D5) verändert sich dabei die Determinante genau mit dem Faktor, der zur jeweiligen Zeilenoperation gehört. Da nach der Determinanteneigenschaft (D3) gilt

$$\det(E_n) = 1,$$

folgen die drei angegebenen Werte sofort. $\square$

7.5.3 Die Produktregel

Lemma 7.5.4 (Produktregel für Elementarmatrizen)**.** *Sei $E \in M_n(k)$ eine Elementarmatrix. Dann gilt für jede Matrix $A \in M_n(k)$:*

$$\det(EA) = \det(E)\det(A).$$

Beweis. Sei $O = O_\rho$ die Elementarmatrix zur Zeilenoperation ρ. Nach Lemma 7.5.2 gilt

$$OA = \rho(A).$$

Nach der Determinanteneigenschaft (D5) verändert ρ die Determinante mit demselben Faktor, den ρ nach Lemma 7.5.3 auch auf der Einheitsmatrix erzeugt. Dieser Faktor ist also $\det(O)$. Daher gilt

$$\det(OA) = \det(O)\det(A).$$ □

Bemerkung 7.5.5. Nicht jede Matrix ist ein Produkt von Elementarmatrizen. Das kann auch nicht stimmen, denn Elementarmatrizen sind invertierbar, und ein Produkt invertierbarer Matrizen ist wieder invertierbar. Richtig ist die folgende Aussage für invertierbare Matrizen.

Lemma 7.5.6 (Invertierbare Matrizen als Produkte von Elementarmatrizen)**.** *Sei $A \in M_n(k)$ invertierbar. Dann gibt es Elementarmatrizen $O_1, \dots, O_s \in M_n(k)$ mit*

$$A = O_1 \cdots O_s.$$

Beweis. Da A invertierbar ist, bringt das Gaußverfahren zur Matrixinvertierung die Matrix A durch elementare Zeilenoperationen auf E_n. Es gibt also Elementarmatrizen $F_1, \dots, F_s$ mit

$$F_s \cdots F_1 A = E_n.$$

Daher gilt

$$A = F_1^{-1} \cdots F_s^{-1}.$$

Die Umkehrmatrix einer Elementarmatrix ist wieder eine Elementarmatrix, denn jede elementare Zeilenoperation kann durch eine elementare Zeilenoperation rückgängig gemacht werden. Also ist A ein Produkt von Elementarmatrizen. □

Bemerkung 7.5.7 (Der Gedanke hinter dem Beweis)**.** Eine Matrix ist genau dann invertierbar, wenn sie durch elementare Zeilenoperationen auf die Einheitsmatrix gebracht werden kann. Jede dieser Zeilenoperationen entspricht einer Linksmultiplikation mit einer Elementarmatrix. Damit entspricht die ganze Gaußrechnung einer Multiplikation mit einem Produkt von Elementarmatrizen.

Ist eine Matrix dagegen nicht invertierbar, dann kann sie durch Gauß zwar in Zeilenstufenform gebracht werden, aber nicht bis zur Einheitsmatrix. In diesem Fall entsteht eine Nullzeile. Genau daran sieht man auch aus Determinantensicht, warum eine solche Matrix nicht als Produkt von Elementarmatrizen auftreten kann: Elementarmatrizen haben Determinante ungleich Null, während eine Matrix mit Nullzeile Determinante Null hat.

Korollar 7.5.8 (Produktformel)**.** *Für alle Matrizen $A, B \in M_n(k)$ gilt*

$$\det(AB) = \det(A)\det(B).$$

Beweis. Wir unterscheiden zwei Fälle.

Fall 1: A **ist invertierbar.** Nach Lemma 7.5.6 gibt es Elementarmatrizen $F_1, \dots, F_s$ mit

$$A = F_1 \cdots F_s.$$

Durch wiederholte Anwendung von Lemma 7.5.4 erhalten wir

$$\det(AB) = \det(F_1 \cdots F_s B) = \det(F_1) \cdots \det(F_s) \det(B).$$

Es gilt aber auch wegen Lemma 7.5.4, dass

$$\det(A) = \det(F_1 \cdots F_s) = \det(F_1) \cdots \det(F_s).$$

Also gilt

$$\det(AB) = \det(A) \det(B).$$

Fall 2: A **ist nicht invertierbar.** Dann gilt nach dem bereits bewiesenen Invertierbarkeitskriterium für Determinanten

$$\det(A) = 0.$$

Außerdem ist AB ebenfalls nicht invertierbar. Denn wäre AB invertierbar, so gäbe es eine Matrix C mit

$$ABC = E_n.$$

Dann wäre

$$A(BC) = E_n.$$

Also wäre die von A induzierte lineare Abbildung surjektiv. Nach Lemma 6.4.3 wäre sie ein Isomorphismus. Damit wäre A invertierbar, im Widerspruch zur Annahme.

Also ist AB nicht invertierbar. Wieder nach dem Invertierbarkeitskriterium für Determinanten gilt

$$\det(AB) = 0.$$

Damit folgt

$$\det(AB) = 0 = 0 \cdot \det(B) = \det(A) \det(B).$$ □

Sei

$$\mathrm{GL}\, n(k) := \{A \in M_n(k) \mid A \text{ ist invertierbar } \}.$$

Dann ist $\mathrm{GL}\, n(k)$ eine Gruppe (warum genau?).

Die Produktformel ist sehr wichtig. Zusammen mit dem Fakt, dass

$$\det(A) = 0 \qquad \Longleftrightarrow \qquad A \text{ ist nicht invertierbar}$$

gilt, erhalten wir sofort:

Theorem 7.5.9 (Die Determinante als Gruppenhomomorphismus)**.** *Die Determinante ist ein Gruppenhomomorphismus*

$$\det : \mathrm{GL}\, n(k) \longrightarrow (k^\times, \cdot), A \longmapsto \det(A).$$

Dabei ist $k^\times := k \setminus \{0\}$.

Bemerkung 7.5.10. Aus der allgemeinen Theorie über Gruppenhomomorphismen lernen wir sofort, dass $\det(A^{-1}) = \det(A)^{-1}$. Wir sparen uns also solche Resultate neu zu beweisen!

Leitbeispiel 7.5.11 (Das Kristallgitter: Deformationen multiplizieren Volumina)**.** Die Produktformel Korollar 7.5.8,

$$\det(AB) = \det(A)\det(B),$$

hat im Bild des Gitters Leitbeispiel 7.1.2 eine physikalische Lesart.

Ein Kristallgitter im $\mathbb{R}^n$ ist die linear deformierte Version des Standardgitters. Dieses Standardgitter ist durch den Einheitswürfel $e_1, \dots, e_n$ gegeben ist. Da dieser Einheitswürfel — per *Definition* — vorzeichenbehaftetes Volumen 1. Die Matrix gibt also entweder in ihren Spalten die Gittervektoren oder die Bilder der Einheitsvektoren an (beide Interpretationen liefern die selbe Mathematik).

Sei A die Matrix mit den Spalten $a_1, \dots, a_n$. Die Multiplikation mit der Matrix A verwandelt den Einheitswürfel in das deformierte Gitter $a_1, \dots, a_n$. Dabei transformiert sich das orientierte Volumen des Einheitswürfel (also 1) in das des deformierten Gitters (also $\det(A)$). Damit kann man sich überlegen, dass Multiplikation mit A das orientierte Volumen von allen Parallelepipeden um den Faktor $\det(A)$ skaliert.

Wir sehen: Eine lineare Deformation des Kristalls — etwa eine Streckung oder Scherung — ist eine Matrix, und ihre Determinante ist der Faktor, um den sich *jedes* Volumen ändert (Beträge fürs Volumen, das Vorzeichen für die Händigkeit). Führt man zwei Deformationen nacheinander aus, erst B, dann A, so multiplizieren sich die Volumenfaktoren. Genau das sagt $\det(AB) = \det(A)\det(B)$. Volumenerhaltende Deformationen sind daher genau die mit $\det = \pm 1$, und die orientierungserhaltenden darunter genau die mit $\det = +1$ — daher wird später die Untergruppe der volumen- und orientierungserhaltenden Abbildungen den Namen *spezielle* lineare Gruppe tragen.

Betrachten wir ein kleines Beispiel: Eine Streckung um den Faktor 2 entlang *einer* Kantenrichtung hat $\det(B) = 2$ — Vorsicht, eine Skalierung des Volumens um den Faktor 2 streckt dagegen alle drei Richtungen und hätte $\det = 2^3 = 8$, vergleiche die Bemerkung zur Multilinearität — und gefolgt von einer volumenerhaltenden Scherung mit $\det(A) = 1$ ergibt sie insgesamt den Faktor $2 \cdot 1 = 2$.

7.5.4 Blockmatrizen

Lemma 7.5.12 (Blockobere Dreiecksmatrizen)**.** *Seien $A \in M_p(k)$, $B \in M_q(k)$ und $C \in k^{p\times q}$. Dann gilt*

$$\det\begin{pmatrix} A & C \\ 0 & B \end{pmatrix} = \det(A)\det(B).$$

Insbesondere gilt für Blockdiagonalmatrizen

$$\det\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = \det(A)\det(B).$$

Beweis. Wir geben einen direkten Gaußbeweis.

Die Idee ist, dass wir in A und B die Gaußelimination unabhängig voneinander machen können und sich alles multipliziert.

Hier sind die Details: Setze

$$M := \begin{pmatrix} A & C \\ 0 & B \end{pmatrix}.$$

Zuerst führen wir nur Zeilenoperationen innerhalb der unteren q Zeilen aus. Das ist genau das Gaußverfahren für den Block B. Der linke untere Nullblock bleibt dabei ein Nullblock. Der obere Teil der Matrix bleibt unverändert.

Ist B nicht invertierbar, dann erzeugt das Gaußverfahren im unteren Block eine Nullzeile. Diese ist dann eine Nullzeile der ganzen Matrix. Also gilt nach der Determinanteneigenschaft (D4)

$$\det(M) = 0.$$

Gleichzeitig ist $\det(B) = 0$, also gilt die behauptete Formel in diesem Fall.

Sei nun B invertierbar. Dann können wir den unteren rechten Block durch Gaußoperationen zu E_q machen. Der dabei auftretende Korrekturfaktor ist genau derselbe wie bei der Berechnung von $\det(B)$. Wir erhalten also eine Matrix der Form

$$\begin{pmatrix} A & C' \\ 0 & E_q \end{pmatrix}.$$

Nun addieren wir geeignete Vielfache der unteren Zeilen zu den oberen Zeilen. Dadurch können wir den Block C' vollständig zu 0 machen. Diese Operationen sind vom Typ 3, verändern die Determinante also nach der Determinanteneigenschaft (D5) nicht. Damit bleibt nur noch

$$\begin{pmatrix} A & 0 \\ 0 & E_q \end{pmatrix}.$$

Jetzt führen wir nur Zeilenoperationen innerhalb der oberen p Zeilen aus. Das ist genau das Gaußverfahren für den Block A. Der untere rechte Einheitsblock bleibt unberührt. Der dabei auftretende Korrekturfaktor ist genau derselbe wie bei der Berechnung von $\det(A)$. Am Ende liest das Gaußverfahren auf der ganzen Blockmatrix daher genau das Produkt der Beiträge aus A und aus B ab. Also gilt

$$\det(M) = \det(A)\det(B).$$ □

Lemma 7.5.13 (Transposition dreht Produkte um)**.** *Seien $A \in k^{m\times n}$ und $B \in k^{n\times p}$. Dann gilt*

$$(AB)^\top = B^\top A^\top.$$

Beweis. Konzeptionell vertauscht die Transposition die Rollen von Zeilen und Spalten. Beim Produkt AB wird eine Zeile von A mit einer Spalte von B gepaart. Nach dem Transponieren wird daraus eine Zeile von $B^\top$ und eine Spalte von $A^\top$.

Wir prüfen einen Eintrag. Seien $i \in \{1, \dots, p\}$ und $j \in \{1, \dots, m\}$. Dann gilt

$$\begin{aligned}
\left((AB)^\top\right)_{ij} &= (AB)_{ji} \\
&= \sum_{\ell=1}^{n} A_{j\ell} B_{\ell i} \\
&= \sum_{\ell=1}^{n} B_{\ell i} A_{j\ell} \\
&= \sum_{\ell=1}^{n} (B^\top)_{i\ell} (A^\top)_{\ell j} \\
&= (B^\top A^\top)_{ij}.
\end{aligned}$$

Dabei haben wir benutzt, dass die Multiplikation im Körper k kommutativ ist. Also sind die Matrizen gleich. □

7.5.5 Alternativer Beweis zur Invarianz der Determinante unter Transposition

Lemma 7.5.14 (Transposition von Elementarmatrizen). *Sei $O \in M_n(k)$ eine Elementarmatrix. Dann ist $O^\top$ ebenfalls eine Elementarmatrix und es gilt*

$$\det(O^\top) = \det(O).$$

Beweis. Wir betrachten die drei Typen von Elementarmatrizen.

Typ 1 (Zeilentausch): Die Zeilentauschmatrix entsteht aus E_n, indem zwei Zeilen vertauscht werden. Sie ist ihre eigene Transponierte. Also gilt sofort $O^\top = O$, und damit $\det(O^\top) = \det(O)$.

Typ 2 (Skalierung einer Zeile): Die Skalierungsmatrix ist eine Diagonalmatrix. Daher ist auch sie gleich ihrer Transponierten. Also gilt wieder $O^\top = O$, und damit $\det(O^\top) = \det(O)$.

Typ 3 (Addition eines Zeilenvielfachen): Angenommen, O gehört zur Operation, das r-fache der Zeile i zur Zeile j zu addieren. Dann gehört $O^\top$ zur Operation, das r-fache der Zeile j zur Zeile i zu addieren. Insbesondere ist $O^\top$ wieder eine Elementarmatrix vom Typ 3. Nach Lemma 7.5.3 haben beide Matrizen Determinante 1. Also gilt auch hier $\det(O^\top) = \det(O)$.

□

Wir führen nun einen alternativen Beweis von Theorem 7.3.5, einfach nur aus Spaß und um unsere Fähigkeiten zu testen und zu sehen, wie das selbe Theorem unter anderem Licht erscheint.

Alternativer Beweis von Theorem 7.3.5. Wir benutzen die Produktformel und Elementarmatrizen. Zuerst sei A invertierbar. Nach Lemma 7.5.6 gibt es Elementarmatrizen $O_1, \dots, O_s \in M_n(k)$ mit

$$A = O_1 \cdots O_s.$$

Mit Lemma 7.5.13 folgt dann

$$A^\top = O_s^\top \cdots O_1^\top.$$

Nach der Produktformel und Lemma 7.5.14 gilt daher

$$\begin{aligned} \det(A^\top) &= \det(O_s^\top) \cdots \det(O_1^\top) \\ &= \det(O_s) \cdots \det(O_1) \\ &= \det(O_1) \cdots \det(O_s) \\ &= \det(A). \end{aligned}$$

Im dritten Schritt benutzen wir, dass die Werte $\det(O_i)$ im Körper k liegen und dort kommutieren.

Nun sei A nicht invertierbar. Dann gilt nach Theorem 7.4.1

$$\det(A) = 0.$$

Wir zeigen, dass auch $A^\top$ nicht invertierbar ist. Wäre $A^\top$ invertierbar, dann gäbe es eine Matrix $C \in M_n(k)$ mit

$$CA^\top = E_n \quad \text{und} \quad A^\top C = E_n.$$

Transponieren und Lemma 7.5.13 liefern

$$AC^\top = E_n \quad \text{und} \quad C^\top A = E_n.$$

Also wäre A invertierbar, im Widerspruch zur Annahme. Somit ist $A^\top$ nicht invertierbar. Wieder nach Theorem 7.4.1 folgt

$$\det(A^\top) = 0.$$

Also gilt auch in diesem Fall

$$\det(A^\top) = 0 = \det(A).$$

Damit ist die Behauptung gezeigt. □

7.6 Laplace Entwicklung

Die Laplace-Entwicklung ist ein weiteres Verfahren zur Berechnung von Determinanten. Sie führt eine $n \times n$-Determinante auf Determinanten kleinerer Matrizen zurück und ist besonders nützlich, wenn eine Zeile oder Spalte viele Nullen enthält.

Lemma 7.6.1 (Laplace-Entwicklung in einem Schritt)**.** *Seien $n \geq 2$ und $A \in M_n(k)$. Für $i, j \in \{1, \dots, n\}$ bezeichne $A(i,j) \in M_{n-1}(k)$ die Matrix, die aus A entsteht, wenn man die i-te Zeile und die j-te Spalte streicht. Dann gelten die folgenden beiden Formeln:*

Entwicklung nach einer Zeile *Für jedes $i \in \{1, \dots, n\}$ gilt*

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

Entwicklung nach einer Spalte *Für jedes $j \in \{1, \dots, n\}$ gilt*

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

Beweis. Wir beweisen zuerst die Entwicklung nach einer festen Zeile. Sei also $i \in \{1, \dots, n\}$ fest. Wir schreiben die i-te Zeile von A als Linearkombination der Standardzeilen:

$$z_i = A_{i1} e_1 + \cdots + A_{in} e_n.$$

Nach der Determinanteneigenschaft (D1) ist die Determinante linear in der i-ten Zeile. Also gilt

$$\det(A) = \sum_{j=1}^{n} A_{ij} \det(B_j),$$

wobei B_j die Matrix ist, die aus A entsteht, indem man die i-te Zeile durch e_j ersetzt.

Es bleibt zu zeigen, dass

$$\det(B_j) = (-1)^{i+j} \det(A(i,j))$$

gilt. Dazu bringen wir in B_j die besondere Zeile e_j nach oben. Das braucht $i - 1$ Zeilentausche. Danach bringen wir die besondere Spalte j nach links. Das braucht $j - 1$ Spaltentausche. Nach der Determinanteneigenschaft (D5) und der entsprechenden Spaltenregel verändert jeder dieser Tausche das Vorzeichen der Determinante. Insgesamt entsteht also der Faktor $(-1)^{i+j}$.

Die so erhaltene Matrix hat die Blockgestalt

$$\begin{pmatrix} 1 & 0 \\ * & A(i,j) \end{pmatrix}.$$

Durch Addition geeigneter Vielfacher der ersten Zeile zu den darunterliegenden Zeilen machen wir die erste Spalte unterhalb des ersten Eintrags zu Null. Nach der Determinanteneigenschaft (D5) ändert das die Determinante nicht. Wir erhalten die Blockmatrix

$$\begin{pmatrix} 1 & 0 \\ 0 & A(i,j) \end{pmatrix}.$$

Nach der Blockformel hat diese Matrix die Determinante $\det(A(i,j))$. Damit folgt

$$\det(B_j) = (-1)^{i+j} \det(A(i,j)).$$

Einsetzen in die obige Summe liefert die Entwicklung nach der i-ten Zeile.

Die Entwicklung nach einer festen Spalte folgt daraus, dass $\det(A^\top) = \det(A)$ gilt. Wendet man die bereits bewiesene Zeilenentwicklung auf $A^\top$ an, so ist die Entwicklung nach der j-ten Zeile von $A^\top$ genau die Entwicklung nach der j-ten Spalte von A. Außerdem gilt $A^\top(j,i) = A(i,j)^\top$, und wegen $\det(C^\top) = \det(C)$ haben die auftretenden Untermatrizen dieselbe Determinante. □

Algorithmus 7.6.2 (Laplace-Algorithmus)**.** *Sei $A \in M_n(k)$. Die Laplace-Entwicklung liefert einen rekursiven Algorithmus zur Berechnung von* $\det(A)$.

1. *Ist $n = 1$, dann ist $A = (a)$ und* $\det(A) = a$.
2. *Ist $n \geq 2$, dann wählt man eine Zeile oder eine Spalte aus. Praktisch wählt man möglichst eine Zeile oder Spalte mit vielen Nullen.*
3. *Entwickelt man nach der i-ten Zeile, dann verwendet man*

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

   Entwickelt man nach der j-ten Spalte, dann verwendet man

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

4. *Die Determinanten der Matrizen $A(i,j) \in M_{n-1}(k)$ berechnet man wieder mit demselben Verfahren.*

Bemerkung 7.6.3. Der Laplace-Algorithmus ist meistens deutlich langsamer als das Gaußverfahren. Der Grund ist die Rekursion: Aus einer $n \times n$-Determinante entstehen im ungünstigen Fall viele $(n-1) \times (n-1)$-Determinanten, und diese verzweigen wieder weiter. Das Gaußverfahren arbeitet dagegen systematisch mit Zeilenoperationen und ist für große Matrizen in der Regel wesentlich günstiger.

Die Laplace-Entwicklung bleibt trotzdem nützlich. Sie ist gut für kleine Matrizen, für Matrizen mit vielen Nullen und für theoretische Rechnungen, bei denen man die Determinante nach einer bestimmten Zeile oder Spalte zerlegen will.

7.7 Die Determinante eines Endomorphismus

Das begriffliche Fundament für diesen Abschnitt haben wir in Kapitel 5 gelegt. Weil seither einige Wochen vergangen sind, erinnern wir kurz an die Kernpunkte.

Bemerkung 7.7.1 (Erinnerung: Koordinaten, Matrixdarstellung, Basiswechsel)**.** Sei V ein endlich-dimensionaler k-Vektorraum. Zu einer Basis B von V gehört der Koordinatenvektor $[v]_B \in k^n$ eines Vektors $v \in V$ (Definition 5.2.1). Zu Basen B von V und C von W und einer linearen Abbildung $F : V \to W$ gehört die Matrixdarstellung $M_{C\leftarrow B}(F)$, die in Koordinaten rechnet: $[F(v)]_C = M_{C\leftarrow B}(F)[v]_B$ (Theorem 5.3.4). Wechselt man die Basen, ändert sich die Matrix nach der Basiswechselformel (Korollar 5.4.10); für einen Endomorphismus mit *einer* Basis pro Seite heißt das: Ein Basiswechsel *konjugiert* die Matrix,

$$M_{B'\leftarrow B'}(F) = P^{-1}\, M_{B\leftarrow B}(F)\, P \qquad \text{mit } P = M_{B\leftarrow B'}(\mathrm{Id}_V)$$

(Korollar 5.4.12). Genau diese Konjugation trifft jetzt auf die Produktformel der Determinante — mit einer bemerkenswerten Konsequenz.

Definition 7.7.2 (Endomorphismus)**.** Sei V ein k-Vektorraum. Ein *Endomorphismus* von V ist eine lineare Abbildung

$$F : V \to V$$

von V nach sich selbst. Die Menge aller Endomorphismen von V bezeichnen wir mit $\mathrm{End}(V)$.

Theorem 7.7.3 (Die Determinante eines Endomorphismus ist wohldefiniert)**.** *Sei V ein endlich-dimensionaler k-Vektorraum mit $\dim(V) = n \geq 1$, und sei $F : V \to V$ ein Endomorphismus. Sind B und B' zwei Basen von V, dann gilt*

$$\det\left(M_{B\leftarrow B}(F)\right) = \det\left(M_{B'\leftarrow B'}(F)\right).$$

Beweis. Setze

$$P := M_{B\leftarrow B'}(\mathrm{Id}_V).$$

Nach Korollar 5.4.7 ist

$$P^{-1} = M_{B'\leftarrow B}(\mathrm{Id}_V).$$

Die Basiswechselformel liefert daher

$$M_{B'\leftarrow B'}(F) = P^{-1} M_{B\leftarrow B}(F) P.$$

Mit der Produktregel für Determinanten folgt

$$\det\left(M_{B'\leftarrow B'}(F)\right) = \det(P^{-1}) \det\left(M_{B\leftarrow B}(F)\right) \det(P).$$

Da $P^{-1}P = E_n$, gilt wieder mit der Produktregel

$$\det(P^{-1}) \det(P) = \det(P^{-1}P) = \det(E_n) = 1.$$

Also bleibt nur

$$\det\left(M_{B'\leftarrow B'}(F)\right) = \det\left(M_{B\leftarrow B}(F)\right). \qquad \square$$

Definition 7.7.4 (Determinante eines Endomorphismus)**.** Sei V ein endlich-dimensionaler k-Vektorraum mit $\dim(V) = n \geq 1$, und sei $F : V \to V$ ein Endomorphismus. Wir definieren die *Determinante* von F durch

$$\det(F) := \det\left(M_{B\leftarrow B}(F)\right),$$

wobei B eine beliebige Basis von V ist. Nach Theorem 7.7.3 hängt dieser Wert nicht von der gewählten Basis ab.

Bemerkung 7.7.5 (Das erste Versprechen ist eingelöst)**.** In der Sprache von Kapitel 5 haben wir gerade gezeigt: Ähnliche Matrizen (Definition 5.4.17) haben dieselbe Determinante — der Beweis von Theorem 7.7.3 rechnet ja genau $\det(P^{-1}MP) = \det(M)$ nach. Die Determinante ist also eine *Ähnlichkeitsinvariante* und damit, wie in Bemerkung 5.4.21 angekündigt, in Wahrheit keine Größe der Matrix, sondern eine Größe der linearen Abbildung selbst.

Leitbeispiel 7.7.6 (Das Kristallgitter: der Volumenfaktor ist koordinatenfrei)**.** Definition 7.7.4 krönt das Kapitel: Die Determinante eines Endomorphismus $F : V \to V$ hängt nicht von der gewählten Basis ab. Im Bild des Gitters Leitbeispiel 7.1.2 ist das selbstverständlich. F ist eine Deformation des Raumes und multipliziert jedes Volumen mit einem festen Faktor. Dieser Faktor — wie stark der Raum gedehnt wird — ist eine geometrische Größe des Vorgangs selbst und kann nicht davon abhängen, in welchem Koordinatensystem, also in welcher Basis, wir ihn ausrechnen.

Der Beweis von Theorem 7.7.3 sagt algebraisch dasselbe: Ein Basiswechsel konjugiert die Matrix,

$$M_{B' \leftarrow B'}(F) = P^{-1}\, M_{B \leftarrow B}(F)\, P,$$

und die Produktformel lässt die Faktoren $\det(P^{-1})\det(P) = 1$ verschwinden. Die Koordinaten heben sich weg, der Volumenfaktor bleibt. Das ist die reife Form der Idee, mit der wir das Kapitel begonnen haben: Die Determinante misst, was eine lineare Abbildung mit dem Volumen macht.

Ein ehrlicher Statusbericht zum Abschluss: *Bewiesen* haben wir das Volumen-Bild in diesem Kapitel nicht — dafür müsste man erst präzise sagen, was „Volumen“ überhaupt ist, und das ist Stoff einer späteren Vorlesung. Bewiesen ist der algebraische Kern: Die Axiome (D1)–(D3) legen det eindeutig fest, und ein Basiswechsel ändert nichts an ihr. Das Volumen-Bild war unsere Leitvorstellung — und sie hat uns an keiner Stelle in die Irre geführt.

7.8 Komplexe Konjugation und Determinanten

Definition 7.8.1 (Matrixnotation)**.** Wir führen eine weitere Notation für Matrizen ein. Gegeben $a_{i,j} \in k$ für $i \in \{1, \dots, m\}$ und $j \in \{1, \dots, n\}$ sei $A := \left(a_{i,j}\right)_{i,j} \in k^{m \times n}$ die Matrix mit $A_{i,j} = a_{i,j}$. Falls $a_{i,j}$ auch für Paare (i, j) definiert ist, die über die gewünschte Matrixgröße hinausgehen, geben wir die Grenzen explizit an.

Definition 7.8.2 (Komplexe Konjugation)**.** Die *komplexe Konjugation* ist die Abbildung

$$\kappa : \mathbb{C} \to \mathbb{C}, \quad z \mapsto \overline{z}.$$

Hierbei ist $\overline{a + b \cdot i} = a - b \cdot i$ für $a, b \in \mathbb{R}$.

Ist $A = (a_{i,j}) \in M_n(\mathbb{C})$, dann bezeichnen wir mit $\overline{A}$ die Matrix, die durch eintragsweise Konjugation entsteht:

$$\overline{A} := \left(\overline{a_{i,j}}\right)_{i,j}.$$

Lemma 7.8.3 (Konjugation ist ein Körperisomorphismus)**.** *Die komplexe Konjugation*

$$\kappa : \mathbb{C} \to \mathbb{C}, \quad z \mapsto \overline{z}$$

ist ein Körperisomorphismus von $\mathbb{C}$ nach $\mathbb{C}$. Das heißt: κ ist eine Bijektion und für alle $z, w \in \mathbb{C}$ gilt

$$\overline{z + w} = \overline{z} + \overline{w}, \quad \overline{zw} = \overline{z}\,\overline{w},$$

und außerdem gilt

$$\overline{0} = 0, \quad \overline{1} = 1.$$

Beweis. Schreiben wir

$$z = a + bi \quad \text{und} \quad w = c + di$$

mit $a, b, c, d \in \mathbb{R}$. Dann ist

$$\overline{z + w} = \overline{(a + c) + (b + d)i} = (a + c) - (b + d)i = (a - bi) + (c - di) = \overline{z} + \overline{w}.$$

Außerdem ist

$$zw = (ac - bd) + (ad + bc)i.$$

Also gilt

$$\overline{zw} = (ac - bd) - (ad + bc)i.$$

Andererseits ist

$$\overline{z}\,\overline{w} = (a - bi)(c - di) = (ac - bd) - (ad + bc)i.$$

Damit ist

$$\overline{zw} = \overline{z}\,\overline{w}.$$

Die Gleichungen $\overline{0} = 0$ und $\overline{1} = 1$ sind direkt klar.

Es bleibt nur die Bijektivität. Diese folgt daraus, dass zweimaliges Konjugieren wieder die Ausgangszahl ergibt:

$$\overline{\overline{z}} = z.$$

Also ist κ ihre eigene Umkehrabbildung. Damit ist κ ein Körperisomorphismus. □

Lemma 7.8.4 (Konjugation und Determinante). *Für jede Matrix $A \in M_n(\mathbb{C})$ gilt*

$$\det\left(\overline{A}\right) = \overline{\det(A)}.$$

Beweis. Wir verwenden die Leibnizformel für die Determinante. Ist $A = (a_{i,j})$, dann gilt

$$\det\left(\overline{A}\right) = \sum_{\sigma \in S_n} \operatorname{signum}(\sigma) \prod_{i=1}^{n} \overline{a_{i,\sigma(i)}}.$$

Da die komplexe Konjugation mit Produkten und Summen verträglich ist und da $\operatorname{signum}(\sigma) \in \{-1, 1\} \subseteq \mathbb{R}$ gilt, ist dies gleich

$$\overline{\sum_{\sigma \in S_n} \operatorname{signum}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}} = \overline{\det(A)}.$$ □

Kapitel 8

Eigenwerte und Eigenvektoren

8.1 Definition von Eigenwerten und Eigenvektoren

Eine lineare Abbildung kann auf verschiedene Richtungen sehr unterschiedlich wirken. Eigenvektoren beschreiben die besonders einfachen Richtungen: Die Abbildung dreht sie nicht in eine neue Richtung, sondern streckt sie nur mit einem Skalar.

Sei k ein Körper und V ein k-Vektorraum mit $\dim(V) = n \in \mathbb{N}$.

Definition 8.1.1 (Eigenwert und Eigenvektor)**.** Sei $F \in \mathrm{End}(V)$. Ein Skalar $r \in k$ heißt ein *Eigenwert* von F, wenn es einen Vektor $v \in V$ mit $v \neq 0$ gibt, so dass

$$F(v) = rv$$

gilt. Ein solcher Vektor v heißt ein *Eigenvektor* von F zum Eigenwert r. In diesem Abschnitt sind Eigenwerte immer Skalare im Grundkörper k.

Für $A \in M_n(k)$ nennen wir r einen Eigenwert und $v \in k^n \setminus \{0\}$ einen Eigenvektor von A, wenn dies für den Endomorphismus $L_A \in \mathrm{End}(k^n)$ gilt.

Bemerkung 8.1.2 (Warum der Nullvektor kein Eigenvektor ist)**.** Der Nullvektor erfüllt zwar für jeden Skalar $r \in k$ die Gleichung

$$F(0) = 0 = r0.$$

Genau deshalb schließen wir ihn aus. Würde man 0 als Eigenvektor zulassen, dann wäre jeder Skalar $r \in k$ automatisch ein Eigenwert jedes Endomorphismus. Der Begriff würde also seine Bedeutung verlieren.

Außerdem wäre dann der wichtigste Unabhängigkeitssatz über Eigenvektoren falsch formuliert. Eine Menge von Vektoren, die den Nullvektor enthält, ist immer linear abhängig. Eigenvektoren zu verschiedenen Eigenwerten sollen aber gerade linear unabhängig sein.

Bemerkung 8.1.3 (Warum Eigenvektoren nützlich sind)**.** Die Berechnung von $F^m(v)$ oder für eine Matrix A die Berechnung von

$$A^m v$$

kann für großes m sehr teuer sein. Wenn v aber ein Eigenvektor von F zum Eigenwert r ist, dann gilt

$$F(v) = rv.$$

Daraus folgt durch Induktion über m:

$$F^m(v) = r^m v.$$

Analog gilt für Matrizen $A^m v = r^m v$. Auf einem Eigenvektor wird also aus wiederholter Anwendung eine gewöhnliche Potenz im Körper.

Leitbeispiel 8.1.4 (Zwei gekoppelte Pendel)**.** Dieses Beispiel begleitet uns durch das ganze Kapitel und bis zu den Spektralsätzen im Kapitel über Skalarprodukte.

Zwei gleiche Pendel hängen nebeneinander und sind durch eine Feder verbunden. Lenken wir sie um x_1 und x_2 aus, dann wirkt auf sie (für kleine Auslenkungen und in geeigneten Einheiten) die Rückstellkraft

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = -K \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \qquad K = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}.$$

Dabei ist wichtig, wie dieser Vektor $(y_1, y_2)^\top$ zu lesen ist: Die erste Komponente y_1 ist die Kraft auf Pendel 1, die zweite Komponente y_2 ist die Kraft auf Pendel 2. Wir bündeln also zwei Zahlen zu *einem* Vektor, genau wie wir die beiden Auslenkungen zu $(x_1, x_2)^\top$ gebündelt haben. Die Diagonale bündelt die eigene Aufhängung jedes Pendels *und* den Beitrag der Feder (auf Pendel 1 wirkt $-x_1 - (x_1 - x_2) = -(2x_1 - x_2)$, das ist die erste Zeile); die Einträge -1 sind der Anteil, mit dem die Feder die Pendel aneinander koppelt.

Die physikalische Frage lautet: *Gibt es Auslenkungsmuster, die das System beim Schwingen beibehält?* Dass das eine echte Frage ist, zeigt ein Gegenbeispiel: Lenkt man nur Pendel 1 aus, also $x = (1, 0)$, dann ist

$$-Kx = \begin{pmatrix} -2 \\ 1 \end{pmatrix}$$

— auf das (noch) ruhende Pendel 2 wirkt bereits eine Kraft. Das Muster „nur Pendel 1 ausgelenkt“ bleibt also *nicht* erhalten: Die Feder reicht die Bewegung an Pendel 2 weiter. Gesucht sind demnach die besonderen Vektoren $v \neq 0$, bei denen die Rückstellkraft exakt entgegen der Auslenkung zeigt, sodass sich nur die Amplitude ändert, nicht die Form der Auslenkung. Das heißt: Gesucht sind $v \neq 0$ und $r \in \mathbb{R}$ mit

$$Kv = rv.$$

Das ist Wort für Wort die Definition von Eigenvektor und Eigenwert.

Zwei solche Muster kann man physikalisch erraten.

- *Gleichtakt* $v = (1, 1)$: Beide Pendel schwingen parallel, die Kopplungsfeder bleibt entspannt und spielt keine Rolle. Tatsächlich:

  $$K \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 - 1 \\ -1 + 2 \end{pmatrix} = 1 \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

  Also ist $(1, 1)$ ein Eigenvektor von K zum Eigenwert 1.

- *Gegentakt* $w = (1, -1)$: Die Pendel schwingen gegeneinander, die Kopplungsfeder wird doppelt gedehnt und zieht kräftig zurück. Tatsächlich:

  $$K \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 2 + 1 \\ -1 - 2 \end{pmatrix} = 3 \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

  Also ist $(1, -1)$ ein Eigenvektor von K zum Eigenwert 3.

In der Physik heißen diese ausgezeichneten Muster die *Eigenmoden* (oder Normalschwingungen) des Systems. Der größere Eigenwert 3 bedeutet eine stärkere Rückstellkraft: Der Gegentakt schwingt schneller als der Gleichtakt.

Drei Sichtweisen auf dasselbe Phänomen:

1. *Geometrisch:* K verdreht die Richtungen $(1, 1)$ und $(1, -1)$ nicht, sondern streckt sie nur. Jede andere Richtung der Ebene wird gekippt.

2. *Physikalisch:* In einer Eigenmode schwingt das System „als Ganzes“, statt Energie zwischen den Pendeln hin- und herzuschieben.

3. *Algebraisch:* Die Komponenten von Kx sind $2x_1 - x_2$ und $-x_1 + 2x_2$. Betrachten wir den Gleichtakt-Anteil $g = x_1 + x_2$ und den Gegentakt-Anteil $d = x_1 - x_2$, dann rechnet man nach, was aus ihnen nach Anwendung von K wird:

$$(2x_1 - x_2) + (-x_1 + 2x_2) = x_1 + x_2 = g, \qquad (2x_1 - x_2) - (-x_1 + 2x_2) = 3(x_1 - x_2) = 3d.$$

Kurz: $g \longmapsto g$ und $d \longmapsto 3d$. In diesen Koordinaten *entkoppelt* das System: zwei unabhängige Pendel statt eines gekoppelten Systems. Gute Koordinaten wählen heißt hier, Eigenvektoren als Basis zu nehmen — dieser Gedanke bekommt am Ende des Kapitels den Namen *Diagonalisierung*.

Ein Ausblick: Die Matrix K ist symmetrisch, und die beiden Eigenrichtungen stehen senkrecht aufeinander — senkrecht als Vektoren in der (x_1, x_2)-Ebene wohlgemerkt, nicht im Zimmer. Das ist kein Zufall, sondern der später behandelte Spektralsatz in seiner kleinsten Ausgabe.

Definition 8.1.5 (Eigenraum)**.** Sei $F \in \mathrm{End}(V)$, und sei $r \in k$. Wir setzen

$$E_r(F) := \{v \in V \mid F(v) = rv\}.$$

Diese Menge heißt der *Eigenraum* von F zum Skalar r. Falls r kein Eigenwert ist, dann ist $E_r(F) = \{0\}$. Falls r ein Eigenwert ist, dann besteht $E_r(F)$ aus 0 und allen Eigenvektoren zum Eigenwert r.

Lemma 8.1.6 (Eigenräume sind Kerne)**.** *Sei $F \in \mathrm{End}(V)$, und sei $r \in k$. Dann gilt*

$$E_r(F) = \mathrm{Kern}(r \cdot \mathrm{Id}_V - F).$$

Insbesondere ist $E_r(F)$ ein Untervektorraum von V.

Beweis. Für $v \in V$ gilt

$$\begin{aligned} v \in E_r(F) &\iff F(v) = rv \\ &\iff rv - F(v) = 0 \\ &\iff (r \cdot \mathrm{Id}_V - F)v = 0 \\ &\iff v \in \mathrm{Kern}(r \cdot \mathrm{Id}_V - F). \end{aligned}$$

Also sind die beiden Mengen gleich. Da Kerne linearer Abbildungen Untervektorräume sind, ist auch $E_r(F)$ ein Untervektorraum von V. □

Theorem 8.1.7 (Eigenvektoren zu verschiedenen Eigenwerten sind linear unabhängig)**.** *Sei $F \in \mathrm{End}(V)$. Seien $r_1, \dots, r_m \in k$ paarweise verschiedene Eigenwerte von F. Für jedes $i \in \{1, \dots, m\}$ sei v_i ein Eigenvektor von F zum Eigenwert r_i. Dann sind $v_1, \dots, v_m$ linear unabhängig.*

Beweis. Angenommen, die Behauptung ist falsch. Dann gibt es unter den Vektoren $v_1, \dots, v_m$ eine kürzeste linear abhängige Teilfamilie. Nach Umnummerierung dürfen wir annehmen, dass diese Teilfamilie $v_1, \dots, v_s$ ist. Da kein Eigenvektor der Nullvektor ist, gilt $s \geq 2$.

Es gibt also Skalare $a_1, \dots, a_s \in k$, nicht alle gleich 0, mit

$$a_1 v_1 + \cdots + a_s v_s = 0.$$

Wegen der Minimalität dieser Abhängigkeit sind sogar alle $a_i \neq 0$. Wenden wir F auf die Gleichung an, erhalten wir

$$a_1 r_1 v_1 + \cdots + a_s r_s v_s = 0.$$

Multiplizieren wir die ursprüngliche Gleichung mit r_s, erhalten wir außerdem

$$a_1 r_s v_1 + \cdots + a_s r_s v_s = 0.$$

Subtraktion liefert

$$a_1(r_1 - r_s)v_1 + \cdots + a_{s-1}(r_{s-1} - r_s)v_{s-1} + \underbrace{a_s(r_s - r_s)v_s}_{=0} = 0.$$

Da die Eigenwerte paarweise verschieden sind, gilt $r_i - r_s \neq 0$ für $i < s$. Da außerdem $a_i \neq 0$ gilt, ist dies eine nichttriviale lineare Abhängigkeit der kürzeren Familie $v_1, \ldots, v_{s-1}$. Das widerspricht der Wahl von $v_1, \ldots, v_s$. □

Leitbeispiel 8.1.8 (Zwei gekoppelte Pendel: Moden mischen sich nicht)**.** Im Leitbeispiel Leitbeispiel 8.1.4 gehören die Eigenvektoren $(1, 1)$ und $(1, -1)$ zu den verschiedenen Eigenwerten 1 und 3. Nach dem Satz sind sie linear unabhängig — zwei unabhängige Vektoren in $\mathbb{R}^2$, also eine Basis.

Physikalisch gelesen: *Jede* Anfangsauslenkung lässt sich auf genau eine Weise als Überlagerung von Gleichtakt und Gegentakt schreiben,

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \frac{x_1 + x_2}{2} \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \frac{x_1 - x_2}{2} \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

Die Moden sind also echte, getrennte Bausteine der Bewegung: Der Satz garantiert, dass sie nichts voneinander doppelt zählen. Dass die Eigenwerte *verschieden* sind, ist dabei die entscheidende Voraussetzung — sie hat im Beweis die ganze Arbeit gemacht.

Lemma 8.1.9 (Kern und Invertierbarkeit)**.** *Sei $F \in \mathrm{End}(V)$. Dann gilt*

$$\mathrm{Kern}(F) \neq \{0\} \quad \Longleftrightarrow \quad F \textit{ ist nicht invertierbar.}$$

Beweis. Es gilt

$$\mathrm{Kern}(F) \neq \{0\} \quad \Longleftrightarrow \quad F \text{ ist nicht injektiv.}$$

Da Definitionsbereich und Zielbereich beide Dimension n haben, gilt

$$F \text{ ist nicht injektiv} \quad \Longleftrightarrow \quad F \text{ ist nicht invertierbar.}$$

Der Beweis dazu ist analog zu dem Beweis von Lemma 6.4.3. □

Korollar 8.1.10 (Eigenwerte als Nicht-Invertierbarkeit)**.** *Sei $F \in \mathrm{End}(V)$, und sei $r \in k$. Dann gilt*

$$\begin{aligned} r \textit{ ist Eigenwert von } F \quad &\Longleftrightarrow \quad \mathrm{Kern}(r \cdot \mathrm{Id}_V - F) \neq \{0\} \\ &\Longleftrightarrow \quad r \cdot \mathrm{Id}_V - F \textit{ ist nicht invertierbar.} \end{aligned}$$

Beweis. Der erste Übergang ist genau Lemma 8.1.6 zusammen mit der Definition eines Eigenwertes. Der zweite Übergang ist Lemma 8.1.9 angewandt auf $G = r \cdot \mathrm{Id}_V - F$. □

Bemerkung 8.1.11 (Warum jetzt die Determinante kommt)**.** Wir müssen also verstehen, für welche Skalare r der Endomorphismus $r \cdot \mathrm{Id}_V - F$ nicht invertierbar ist. Man könnte das grundsätzlich über den Rang untersuchen. Der Rang ist für konkrete Rechnungen sehr nützlich, als Ausdruck in der Variablen r aber algebraisch unhandlich.

Die Determinante ist hier besser geeignet und es gilt

$$r \cdot \mathrm{Id}_V - F \text{ ist nicht invertierbar} \quad \Longleftrightarrow \quad \det(r \cdot \mathrm{Id}_V - F) = 0.$$

Korollar 8.1.12 (Eigenwerte als Nullstellen einer Determinante)**.** *Sei $F \in \mathrm{End}(V)$, und sei $r \in k$. Dann gilt*

$$r \text{ ist Eigenwert von } F \quad \Longleftrightarrow \quad \det(r \cdot \mathrm{Id}_V - F) = 0.$$

Beweis. Nach Korollar 8.1.10 ist r genau dann ein Eigenwert von F, wenn $r \cdot \mathrm{Id}_V - F$ nicht invertierbar ist. Nach Theorem 7.4.1 ist das äquivalent zu

$$\det(r \cdot \mathrm{Id}_V - F) = 0. \qquad \square$$

Leitbeispiel 8.1.13 (Zwei gekoppelte Pendel: die Determinante findet die Eigenwerte)**.** Wenden wir das Korollar auf die Pendelmatrix K aus Leitbeispiel 8.1.4 an. Für $r \in \mathbb{R}$ ist

$$\det(r \cdot 1_2 - K) = \det \begin{pmatrix} r-2 & 1 \\ 1 & r-2 \end{pmatrix} = (r-2)^2 - 1 = (r-1)(r-3).$$

Die Nullstellen sind genau 1 und 3 — die beiden Eigenwerte, die wir im Leitbeispiel noch durch physikalisches Raten gefunden haben. Das Raten ist jetzt überflüssig: Die Determinante verwandelt die Eigenwertsuche in das Lösen einer Polynomgleichung. Dieses Polynom in r bekommt im nächsten Abschnitt einen Namen.

Beispiel 8.1.14 (Fibonacci und der goldene Schnitt)**.** Ein mathematisches Goldstück zum Abschluss — im wörtlichen Sinn.

Fibonacci beschrieb 1202 eine idealisierte Kaninchenpopulation: Jeden Monat bekommt jedes geschlechtsreife Paar ein junges Paar als Nachwuchs, und junge Paare werden nach einem Monat geschlechtsreif. Bezeichnet f_m die Anzahl der Paare im Monat m, dann gilt

$$f_{m+2} = f_{m+1} + f_m, \qquad f_1 = f_2 = 1,$$

also 1, 1, 2, 3, 5, 8, 13, 21, 34, ...

Die Rekursion wird zu einer Matrix, wenn man zwei aufeinanderfolgende Werte zu einem Vektor bündelt:

$$\begin{pmatrix} f_{m+2} \\ f_{m+1} \end{pmatrix} = A \begin{pmatrix} f_{m+1} \\ f_m \end{pmatrix} \qquad \text{mit} \qquad A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \text{also} \qquad \begin{pmatrix} f_{m+1} \\ f_m \end{pmatrix} = A^{m-1} \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Das ist genau die Situation aus der Bemerkung „Warum Eigenvektoren nützlich sind“: Wir müssen hohe Potenzen von A verstehen.

Suchen wir Eigenvektoren der Form $v = (x, 1)$:

$$A \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} x+1 \\ x \end{pmatrix}.$$

Das ist genau dann ein Vielfaches von $(x, 1)$, wenn $\frac{x+1}{x} = \frac{x}{1}$ gilt, also $x^2 = x + 1$. Diese Gleichung hat die beiden Lösungen

$$\varphi = \frac{1+\sqrt{5}}{2} \approx 1{,}618 \qquad \text{und} \qquad \psi = \frac{1-\sqrt{5}}{2} \approx -0{,}618,$$

und φ ist der berühmte *goldene Schnitt*. Mit $v_\varphi = (\varphi, 1)$ und $v_\psi = (\psi, 1)$ gilt $Av_\varphi = \varphi v_\varphi$ und $Av_\psi = \psi v_\psi$, und auf diesen Richtungen wird aus Iteration eine Potenz: $A^m v_\varphi = \varphi^m v_\varphi$.

Zunächst zerlegen wir den Startvektor $(1, 1)$ in die beiden Eigenrichtungen, suchen also $a, b \in \mathbb{R}$ mit

$$\begin{pmatrix}1\\1\end{pmatrix} = a\,v_\varphi + b\,v_\psi = a\begin{pmatrix}\varphi\\1\end{pmatrix} + b\begin{pmatrix}\psi\\1\end{pmatrix} = \begin{pmatrix}a\varphi + b\psi\\ a + b\end{pmatrix}.$$

Die zweite Komponente sagt $a + b = 1$. Wir setzen also $b = 1 - a$ in die erste Komponente ein. Dabei helfen zwei Identitäten, die man direkt aus den Formeln für φ und ψ abliest (es sind die Wurzelsätze der Gleichung $x^2 = x + 1$):

$$\varphi + \psi = 1 \qquad \text{und} \qquad \varphi - \psi = \sqrt{5}.$$

Damit wird die erste Komponente zu

$$1 = a\varphi + (1-a)\psi = a(\varphi - \psi) + \psi = a\sqrt{5} + \psi,$$

also, wegen $1 - \psi = (\varphi + \psi) - \psi = \varphi$,

$$a = \frac{1-\psi}{\sqrt{5}} = \frac{\varphi}{\sqrt{5}}, \qquad b = 1 - a = \frac{\sqrt{5}-\varphi}{\sqrt{5}} = -\frac{\psi}{\sqrt{5}},$$

wobei der letzte Schritt $\sqrt{5} - \varphi = \frac{\sqrt{5}-1}{2} = -\psi$ benutzt.

Jetzt kommt der Eigenvektor-Trick zum Einsatz: Wir wenden A^{m-1} auf die Zerlegung an, und auf den Eigenrichtungen ist das nur eine Potenz.

$$\begin{pmatrix}f_{m+1}\\f_m\end{pmatrix} = A^{m-1}\begin{pmatrix}1\\1\end{pmatrix} = a\,\varphi^{m-1}v_\varphi + b\,\psi^{m-1}v_\psi = \frac{\varphi}{\sqrt{5}}\,\varphi^{m-1}\begin{pmatrix}\varphi\\1\end{pmatrix} - \frac{\psi}{\sqrt{5}}\,\psi^{m-1}\begin{pmatrix}\psi\\1\end{pmatrix}.$$

In der *zweiten* Komponente steht links f_m — und rechts lesen wir die geschlossene *Binet-Formel* ab:

$$f_m = \frac{\varphi}{\sqrt{5}}\,\varphi^{m-1} - \frac{\psi}{\sqrt{5}}\,\psi^{m-1} = \frac{\varphi^m - \psi^m}{\sqrt{5}}.$$

Eine Formel voller Irrationalitäten, die für jedes m eine natürliche Zahl ausspuckt.

Zwei Einsichten stecken darin.

1. *Die dominante Eigenrichtung gewinnt:* Wegen $|\psi| < 1$ stirbt der ψ-Anteil beim Iterieren aus, und der Zustandsvektor kippt in die Richtung v_φ. Deshalb näheren sich die Verhältnisse aufeinanderfolgender Fibonaccizahlen dem goldenen Schnitt:

   $$\frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \ldots \longrightarrow \varphi.$$

   Die Population wächst langfristig geometrisch mit Faktor φ pro Monat — der goldene Schnitt als Wachstumsrate eines simplen Zählproblems.

2. *Eigenvektoren machen Dynamik berechenbar:* Ohne sie müsste man für f_{100} hundertmal addieren, mit ihnen ist f_{100} eine einzige Potenz. Das systematische Rezept hinter dieser Rechnung — *Diagonalisierung* — entwickeln wir im Rest des Kapitels.

8.2 Das charakteristische Polynom

Definition 8.2.1 (Charakteristisches Polynom)**.** Sei $F \in \mathrm{End}(V)$. Das Polynom

$$p_F(X) := \det(X \cdot \mathrm{Id}_V - F) \in k[X]$$

heißt das *charakteristische Polynom* von F. Hierbei ist $k[X]$ der Ring aller Polynome in der Variablen X. Für $A \in M_n(k)$ ist entsprechend $p_A(X) = \det(X \cdot 1_n - A)$.

Bemerkung 8.2.2 (Warum das wirklich ein Polynom ist)**.** Die Schreibweise in Definition 8.2.1 ist nicht nur symbolisch gemeint. Nach der Leibnizformel ist $\det(X \cdot \mathrm{Id}_V - F)$ eine endliche Summe von Produkten von Einträgen einer Matrixdarstellung von $X \cdot \mathrm{Id}_V - F$ bezüglich einer beliebigen Basis von V. (Dass das Ergebnis nicht von der Basiswahl abhängt, zeigt der Satz weiter unten.) Diese Einträge liegen alle in $k[X]$. Also liegt auch die ganze Leibnizsumme in $k[X]$.

Korollar 8.2.3 (Eigenwerte sind Nullstellen des charakteristischen Polynoms)**.** *Sei $F \in \mathrm{End}(V)$, und sei $r \in k$. Dann gilt*

$$r \text{ ist Eigenwert von } F \quad \Longleftrightarrow \quad p_F(r) = 0.$$

Beweis. Nach Definition gilt

$$p_F(r) = \det(r \cdot \mathrm{Id}_V - F).$$

Die Behauptung folgt also aus Korollar 8.1.12. □

Bemerkung 8.2.4 (Recap: Polynomdivision mit Rest)**.** Sei k ein Körper. Sind $f, g \in k[X]$ Polynome mit $g \neq 0$, dann gibt es eindeutig bestimmte Polynome $q, r \in k[X]$ mit

$$f = qg + r$$

und mit $r = 0$ oder $\deg(r) < \deg(g)$. Das Polynom q heißt der Quotient, und r heißt der Rest.

Besonders wichtig ist der Fall $g = X - \lambda$ mit $\lambda \in k$. Dann hat der Rest Grad kleiner als 1, ist also ein konstantes Polynom. Es gibt also ein Polynom $q \in k[X]$ und ein $c \in k$ mit

$$f(X) = (X - \lambda)q(X) + c.$$

Setzt man $X = \lambda$ ein, dann bleibt nur der Rest übrig. Also gilt $c = f(\lambda)$. Kurz gesagt: Bei Division durch $X - \lambda$ ist der Rest genau $f(\lambda)$.

Lemma 8.2.5 (Nullstellen und Linearfaktoren)**.** *Sei $f \in k[X]$ ein Polynom. Dann gelten:*

1. *Sei $\lambda \in k$. Dann ist $f(\lambda) = 0$ genau dann, wenn $X - \lambda$ das Polynom f teilt.*
2. *Ist $f \neq 0$ und $\deg(f) = n$, dann hat f höchstens n verschiedene Nullstellen in k.*

Beweis. Wir zeigen zuerst Teil (1). Wenn $X - \lambda$ das Polynom f teilt, dann gibt es ein $q \in k[X]$ mit

$$f(X) = (X - \lambda)q(X).$$

Einsetzen von $X = \lambda$ ergibt sofort $f(\lambda) = 0$.

Sei umgekehrt $f(\lambda) = 0$. Nach Polynomdivision mit Rest gibt es ein $q \in k[X]$ und ein $c \in k$ mit

$$f(X) = (X - \lambda)q(X) + c.$$

Der Rest ist nach dem Recap gleich $f(\lambda)$. Also ist $c = 0$, und damit teilt $X - \lambda$ das Polynom f.

Nun zeigen wir Teil (2). Seien $\lambda_1, \dots, \lambda_m \in k$ paarweise verschiedene Nullstellen von f. Wir zeigen, dass dann das Produkt

$$(X - \lambda_1) \cdots (X - \lambda_m)$$

das Polynom f teilt. Daraus folgt sofort $m \leq n$, denn ein Teiler eines von Null verschiedenen Polynoms kann keinen größeren Grad haben.

Wir beweisen die Teilbarkeit per Induktion über m. Für $m = 0$ ist nichts zu zeigen. Für den Induktionsschritt nehmen wir an, dass

$$h(X) := (X - \lambda_1) \cdots (X - \lambda_{m-1})$$

das Polynom f teilt. Dann gibt es ein $q \in k[X]$ mit $f = hq$. Da λ_m von $\lambda_1, \dots, \lambda_{m-1}$ verschieden ist, gilt $h(\lambda_m) \neq 0$. Aus $0 = f(\lambda_m) = h(\lambda_m)q(\lambda_m)$ folgt daher $q(\lambda_m) = 0$. Nach Teil (1) teilt $X - \lambda_m$ das Polynom q. Also teilt

$$h(X)(X - \lambda_m) = (X - \lambda_1) \cdots (X - \lambda_m)$$

das Polynom f. Damit ist die Induktion abgeschlossen. □

Definition 8.2.6 (Spur)**.** Sei $A \in M_n(k)$. Die *Spur* von A ist die Summe der Diagonaleinträge:

$$\mathrm{Spur}(A) := \sum_{i=1}^{n} A_{ii}.$$

Ist B eine Basis eines endlich-dimensionalen k-Vektorraums V, und ist $F \in \mathrm{End}(V)$, dann setzen wir zunächst

$$\mathrm{Spur}_B(F) := \mathrm{Spur}\left(M_{B \leftarrow B}(F)\right).$$

Bemerkung 8.2.7 (Warum diese Definition zunächst wacklig ist)**.** Für Matrizen ist die Spur völlig klar: Man addiert die Diagonaleinträge. Für Endomorphismen steht diese Definition aber zunächst auf ziemlich wackligen Füßen. Die Diagonaleinträge entstehen erst nach Wahl einer Basis. Bei einem Basiswechsel kann die Matrixdarstellung eines Endomorphismus ganz anders aussehen. Es ist also nicht offensichtlich, warum ausgerechnet die Summe der Diagonaleinträge gleich bleiben sollte.

Der nächste Satz zeigt, dass diese Sorge berechtigt, aber am Ende harmlos ist: Die Spur eines Endomorphismus ist tatsächlich wohldefiniert.

Theorem 8.2.8 (Eigenschaften des charakteristischen Polynoms)**.** *Sei V ein n-dimensionaler k-Vektorraum mit $n \geq 1$, und sei $F \in \mathrm{End}(V)$. Dann gelten:*

1. *Das charakteristische Polynom $p_F(X)$ ist wohldefiniert, das heißt: Es hängt nicht von der gewählten Basis ab. Auch $\mathrm{Spur}_B(F)$ hängt nicht von der gewählten Basis B ab. Wir schreiben diesen gemeinsamen Wert als $\mathrm{Spur}(F)$.*
2. *Das Polynom $p_F(X)$ ist normiert vom Grad n. Sein Absolutglied ist $(-1)^n \det(F)$, und der Koeffizient von X^{n-1} ist $-\mathrm{Spur}(F)$.*
3. *Der Endomorphismus F hat höchstens n verschiedene Eigenwerte.*

Beweis. Wir beginnen mit einer Matrix $A \in M_n(k)$. Setze

$$D := X \cdot 1_n - A.$$

Dann ist $p_A(X) = \det(D)$. Nach der Leibnizformel gilt

$$p_A(X) = \sum_{\sigma \in S_n} \operatorname{signum}(\sigma) \prod_{i=1}^{n} D_{i,\sigma(i)}.$$

Jeder Faktor $D_{i,\sigma(i)}$ ist entweder ein Polynom vom Grad höchstens 1 oder ein konstantes Polynom. Also hat jeder Summand Grad höchstens n, und damit gilt $\deg(p_A) \leq n$.

Jetzt betrachten wir die höchsten Grade genauer. Ein Faktor enthält nur dann einen Anteil X, wenn er ein Diagonaleintrag ist. Der Term vom Grad n kann daher nur aus der identischen Permutation entstehen: In jeder Zeile muss der Diagonaleintrag gewählt werden. Der Beitrag der identischen Permutation ist

$$\prod_{i=1}^{n} (X - A_{ii}).$$

Daraus kommt der Term X^n mit Koeffizient 1. Also ist $p_A(X)$ normiert vom Grad n.

Auch der Koeffizient von X^{n-1} kommt nur von der identischen Permutation. Denn jede nicht-identische Permutation bewegt mindestens zwei Indizes. In einem solchen Summanden werden also mindestens zwei Nicht-Diagonaleinträge gewählt, und der Grad ist höchstens $n - 2$. Im Produkt der Diagonaleinträge gilt

$$\prod_{i=1}^{n} (X - A_{ii}) = X^n - \left(\sum_{i=1}^{n} A_{ii} \right) X^{n-1} + \text{Terme vom Grad höchstens } n - 2.$$

Der Koeffizient von X^{n-1} in $p_A(X)$ ist daher $-\operatorname{Spur}(A)$.

Das Absolutglied erhält man durch Einsetzen von $X = 0$:

$$p_A(0) = \det(-A) = (-1)^n \det(A).$$

Damit sind die Aussagen über Grad, führenden Koeffizienten, Absolutglied und den Koeffizienten von X^{n-1} für Matrizen gezeigt.

Nun behandeln wir Endomorphismen. Seien B und C zwei Basen von V. Setze

$$A_B := M_{B \leftarrow B}(F), \quad A_C := M_{C \leftarrow C}(F)$$

und

$$P := M_{B \leftarrow C}(\mathrm{Id}_V).$$

Dann gilt

$$A_C = P^{-1} A_B P.$$

Weil P konstante Einträge aus k hat, können wir dieselbe Gleichung in Matrizen über dem Polynomring $k[X]$ benutzen. Es gilt

$$X \cdot 1_n - A_C = P^{-1} (X \cdot 1_n - A_B) P.$$

Mit der Produktregel für die Determinante folgt

$$\begin{aligned} \det(X \cdot 1_n - A_C) &= \det\left(P^{-1}\right) \det(X \cdot 1_n - A_B) \det(P) \\ &= \det(X \cdot 1_n - A_B). \end{aligned}$$

Also ist $p_F(X)$ unabhängig von der gewählten Basis.

Da wir für Matrizen bereits gezeigt haben, dass der Koeffizient von X^{n-1} gleich minus der Spur ist, folgt aus der Basisunabhängigkeit von $p_F(X)$ sofort auch die Basisunabhängigkeit der Spur. Damit ist $\operatorname{Spur}(F)$ wohldefiniert. Die Aussagen über Grad, Normiertheit, Absolutglied und den

Koeffizienten von X^{n-1} gelten nun ebenfalls für Endomorphismen, weil man sie in irgendeiner Basis berechnen darf.

Es bleibt die Aussage über die Anzahl der Eigenwerte. Nach Korollar 8.2.3 ist jeder Eigenwert von F eine Nullstelle von $p_F(X)$. Nach dem bereits bewiesenen Teil ist $p_F(X)$ ein von Null verschiedenes Polynom vom Grad n. Nach Lemma 8.2.5 hat es höchstens n verschiedene Nullstellen. Also hat F höchstens n verschiedene Eigenwerte. □

Leitbeispiel 8.2.9 (Zwei gekoppelte Pendel: der Satz im Schnelltest)**.** Für die Pendelmatrix K aus Leitbeispiel 8.1.4 haben wir am Ende des letzten Abschnitts schon gerechnet:

$$p_K(X) = \det(X \cdot 1_2 - K) = (X-2)^2 - 1 = X^2 - 4X + 3 = (X-1)(X-3).$$

Der Satz sagt für eine 2×2-Matrix voraus: normiert vom Grad 2, Absolutglied $(-1)^2 \det(K)$, Koeffizient von X gleich $-\operatorname{Spur}(K)$. Tatsächlich ist

$$\det(K) = 2 \cdot 2 - (-1) \cdot (-1) = 3, \qquad \operatorname{Spur}(K) = 2 + 2 = 4,$$

und $p_K(X) = X^2 - \operatorname{Spur}(K) \cdot X + \det(K)$.

An der Faktorisierung lesen wir zugleich ab:

$$\operatorname{Spur}(K) = 4 = 1 + 3, \qquad \det(K) = 3 = 1 \cdot 3.$$

Die Spur ist hier also die *Summe* und die Determinante das *Produkt* der Eigenwerte. Für 2×2-Matrizen lohnt sich der Merksatz

$$p_A(X) = X^2 - \operatorname{Spur}(A) \cdot X + \det(A) \ :$$

Berechnete Eigenwerte kontrolliert man blitzschnell, indem man ihre Summe mit der Spur und ihr Produkt mit der Determinante vergleicht. Und schließlich: K hat genau $2 = n$ verschiedene Eigenwerte — mehr lässt der Satz nicht zu.

Bemerkung 8.2.10 (Warum die Spur in der Physik auftaucht)**.** Die Spur ist eine basisunabhängige Zahl, die man aus einem Endomorphismus gewinnt. Das macht sie in der Physik sehr nützlich: Sie kann eine Größe beschreiben, die nicht von der Wahl der Koordinaten abhängen soll. In der Quantenmechanik und statistischen Mechanik treten zum Beispiel Ausdrücke der Form $\operatorname{Spur}(\rho A)$ auf, wobei ρ einen Zustand und A eine beobachtbare Größe beschreibt. In der linearen Algebra hilft die Spur außerdem dabei, charakteristische Polynome kleiner Matrizen schnell zu kontrollieren.

Beispiel 8.2.11 (Eine Drehung hat keine reellen Eigenwerte)**.** Die Drehung der Ebene um 90° gegen den Uhrzeigersinn hat die Matrix

$$R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in M_2(\mathbb{R}).$$

Ihr charakteristisches Polynom ist

$$p_R(X) = \det \begin{pmatrix} X & 1 \\ -1 & X \end{pmatrix} = X^2 + 1.$$

Dieses Polynom hat keine reelle Nullstelle, also hat R keinen reellen Eigenwert — und das *muss* auch so sein: Eine Drehung um 90° kippt jede Richtung der Ebene, keine Gerade durch den Ursprung bleibt liegen. Die Algebra (keine Nullstelle) und die Geometrie (keine invariante Richtung) erzählen hier dieselbe Geschichte.

Über den komplexen Zahlen ändert sich das Bild: Es gilt $X^2+1 = (X-i)(X+i)$, und tatsächlich hat R, aufgefasst als Matrix in $M_2(\mathbb{C})$, die beiden Eigenwerte $\pm i$. Der Schnelltest funktioniert auch hier: $\mathrm{Spur}(R) = 0 = i + (-i)$ und $\det(R) = 1 = i \cdot (-i)$. Dass $\mathbb{R}$ manchmal zu klein ist und $\mathbb{C}$ aushilft, ist ein wiederkehrendes Motiv der Eigenwerttheorie — es kehrt bei den Spektralsätzen im nächsten Kapitel zurück.

Für die Drehung um einen beliebigen Winkel θ gilt übrigens

$$p_{R_\theta}(X) = X^2 - 2\cos(\theta)\,X + 1.$$

Reelle Nullstellen gibt es nur für $\cos(\theta) = \pm 1$: bei der Drehung um 0° (die Identität, Eigenwert 1) und bei der Drehung um 180° (die Punktspiegelung, Eigenwert -1) — genau die beiden Drehungen, die Geraden durch den Ursprung an ihrem Platz lassen.

8.3 Vielfachheiten und Diagonalisierbarkeit

8.3.1 Vielfachheiten

Definition 8.3.1 (Vielfachheiten)**.** Sei $F \in \mathrm{End}(V)$, und sei $\lambda \in k$ ein Eigenwert von F. Die *algebraische Vielfachheit* von λ ist die Vielfachheit von λ als Nullstelle des charakteristischen Polynoms $p_F(X)$. Das heißt: Sie ist die größte Zahl $a \in \mathbb{N}$, so dass

$$(X-\lambda)^a \mid p_F(X)$$

in $k[X]$ gilt. Dabei steht $d \mid q$ für „d teilt q“.

Die *geometrische Vielfachheit* von λ ist die Dimension des Eigenraums:

$$\dim E_\lambda(F).$$

Lemma 8.3.2 (Geometrische und algebraische Vielfachheit)**.** *Sei $F \in \mathrm{End}(V)$, und sei $\lambda \in k$ ein Eigenwert von F. Dann gilt*

$$1 \le \dim E_\lambda(F) \le \textit{algebraische Vielfachheit von } \lambda \le \dim(V).$$

Beweis. Die erste Ungleichung gilt, weil λ ein Eigenwert ist und der Eigenraum daher einen Eigenvektor enthält. Die letzte Ungleichung gilt, weil $p_F(X)$ ein Polynom vom Grad $\dim(V)$ ist.

Es bleibt die mittlere Ungleichung. Setze $n := \dim(V)$ und

$$r := \dim E_\lambda(F).$$

Falls $r = n$ gilt, ist $F = \lambda\,\mathrm{Id}_V$, und daher ist $p_F(X) = (X-\lambda)^n$. Dann ist nichts weiter zu zeigen. Wir dürfen also $r < n$ annehmen. Wähle eine Basis $b_1, \dots, b_r$ von $E_\lambda(F)$, und ergänze sie zu einer Basis

$$B = (b_1, \dots, b_r, b_{r+1}, \dots, b_n)$$

von V. Für $j \le r$ gilt $F(b_j) = \lambda b_j$. Die ersten r Spalten der Matrix $M_{B\leftarrow B}(F)$ sind also genau die ersten r Spalten von λE_n. Daher hat diese Matrix die Blockform

$$M_{B\leftarrow B}(F) = \begin{pmatrix} \lambda E_r & C \\ 0 & D \end{pmatrix}$$

mit passenden Matrizen C und D. Folglich gilt

$$XE_n - M_{B\leftarrow B}(F) = \begin{pmatrix} (X-\lambda)E_r & -C \\ 0 & XE_{n-r} - D \end{pmatrix}.$$

Nach Lemma 7.5.12 gilt: Die Determinante einer oberen Blockdreiecksmatrix ist das Produkt der Determinanten der Diagonalblöcke. Also ist

$$p_F(X) = \det\left(XE_n - M_{B\leftarrow B}(F)\right) = (X-\lambda)^r \det\left(XE_{n-r} - D\right).$$

Damit teilt $(X-\lambda)^r$ das charakteristische Polynom. Die algebraische Vielfachheit von λ ist also mindestens $r = \dim E_\lambda(F)$. □

8.3.2 Mehrfache Direkte Summen

Definition 8.3.3 (Mehrfache direkte Summe)**.** Seien $U_1, \dots, U_r$ Untervektorräume von V. Ihre Summe ist

$$U_1 + \cdots + U_r := \{u_1 + \cdots + u_r \mid u_i \in U_i\}.$$

Diese Summe heißt *direkt*, wenn jedes Element von $U_1 + \cdots + U_r$ genau eine Darstellung der Form

$$u_1 + \cdots + u_r \quad \text{mit} \quad u_i \in U_i$$

hat. In diesem Fall schreiben wir auch

$$U_1 \oplus \cdots \oplus U_r.$$

Äquivalent dazu ist: Aus

$$u_1 + \cdots + u_r = 0 \quad \text{mit} \quad u_i \in U_i$$

folgt immer $u_1 = \cdots = u_r = 0$.

Lemma 8.3.4 (Dimension einer mehrfachen Summe)**.** *Seien $U_1, \dots, U_r$ endlich-dimensionale Untervektorräume von V. Dann gilt*

$$\dim(U_1 + \cdots + U_r) \le \sum_{i=1}^{r} \dim(U_i).$$

Gleichheit gilt genau dann, wenn die Summe direkt ist. Ist die Summe direkt, dann erhält man eine Basis von $U_1 \oplus \cdots \oplus U_r$, indem man Basen der Summanden zusammenlegt.

Beweis. Betrachte die lineare Abbildung

$$\Phi : U_1 \times \cdots \times U_r \to V, \quad (u_1, \dots, u_r) \mapsto u_1 + \cdots + u_r.$$

Ihr Bild ist genau $U_1 + \cdots + U_r$. Daher gilt

$$\dim(U_1 + \cdots + U_r) = \dim \operatorname{Bild}(\Phi) \le \dim(U_1 \times \cdots \times U_r) = \sum_{i=1}^{r} \dim(U_i).$$

Gleichheit gilt genau dann, wenn Φ injektiv ist. Das bedeutet genau, dass aus $u_1 + \cdots + u_r = 0$ nur die triviale Darstellung folgt. Nach Definition ist das genau die Direktheit der Summe.

Sei nun die Summe direkt. Wähle für jedes i eine Basis B_i von U_i. Die zusammengelegte Familie $B_1 \cup \cdots \cup B_r$ erzeugt offensichtlich $U_1 + \cdots + U_r$. Sie ist linear unabhängig, weil jede lineare Abhängigkeit eine Darstellung von 0 als Summe von Vektoren aus den U_i liefert. Wegen der Direktheit müssen alle diese Beiträge gleich 0 sein. Da die einzelnen B_i Basen sind, müssen alle Koeffizienten verschwinden. Also ist die zusammengelegte Familie eine Basis der Summe. □

Korollar 8.3.5 (Eigenräume zu verschiedenen Eigenwerten bilden eine direkte Summe)**.** *Sei $F \in \mathrm{End}(V)$. Seien $\lambda_1, \dots, \lambda_r \in k$ paarweise verschiedene Eigenwerte von F. Dann ist die Summe*

$$E_{\lambda_1}(F) + \cdots + E_{\lambda_r}(F)$$

direkt.

Beweis. Seien

$$v_i \in E_{\lambda_i}(F) \quad \text{und} \quad v_1 + \cdots + v_r = 0.$$

Falls ein $v_i \neq 0$ ist, dann sind die von Null verschiedenen Vektoren unter den v_i Eigenvektoren zu paarweise verschiedenen Eigenwerten. Nach Theorem 8.1.7 sind sie linear unabhängig. Ihre Summe kann also nicht 0 sein. Folglich gilt $v_1 = \cdots = v_r = 0$. Nach Definition ist die Summe direkt. □

Leitbeispiel 8.3.6 (Zwei gekoppelte Pendel: der Zustandsraum zerfällt in Moden)**.** Für die Pendelmatrix K aus Leitbeispiel 8.1.4 sind die Eigenräume

$$E_1(K) = \mathrm{Span}\,((1,1)) \qquad \text{und} \qquad E_3(K) = \mathrm{Span}\,((1,-1))\,,$$

beide mit geometrischer (und algebraischer) Vielfachheit 1. Nach dem Korollar ist ihre Summe direkt, und da sie Dimension $1 + 1 = 2$ hat, füllt sie ganz $\mathbb{R}^2$:

$$\mathbb{R}^2 = E_1(K) \oplus E_3(K).$$

Der Raum aller Auslenkungen zerfällt also restlos und überschneidungsfrei in die beiden Modenrichtungen. Die Direktheit ist der mathematische Grund dafür, dass die Zerlegung einer Bewegung in Gleichtakt- und Gegentaktanteil *eindeutig* ist: Kein Anteil kann heimlich in den anderen hinüberwandern.

8.3.3 Diagonalisierbarkeit

Definition 8.3.7 (Diagonalisierbarkeit)**.** Ein Endomorphismus $F : V \to V$ heißt *diagonalisierbar*, falls es eine Basis B von V gibt, so dass $M_{B \leftarrow B}(F)$ Diagonalgestalt hat. Eine solche Basis heißt eine *diagonalisierende* Basis (für F).

Lemma 8.3.8 (Eigenbasen sind die diagonalisierenden Basen)**.** *Eine Basis ist genau dann diagonalisierend für F, wenn sie nur aus Eigenvektoren von F besteht. Eine solche Basis nennt man auch* Eigenbasis.

Beweis. Die Grundidee ist die folgende. Eine Diagonalmatrix beschreibt eine lineare Abbildung, die die gewählten Koordinatenrichtungen nicht miteinander vermischt. Für jeden Basisvektor b_j bedeutet das: Sein Bild $F(b_j)$ liegt wieder auf derselben Geraden kb_j. Genau das ist aber die Eigenvektorbedingung. Diagonalisierbarkeit fragt also, ob man den ganzen Raum in passende Eigenrichtungen zerlegen kann.

Hier sind die Details: Sei $B = (b_1, \dots, b_n)$ eine Basis von V. Die j-te Spalte von $M_{B \leftarrow B}(F)$ enthält die B-Koordinaten von $F(b_j)$.

Die Matrix ist genau dann diagonal, wenn in jeder j-ten Spalte nur der j-te Eintrag möglicherweise ungleich Null ist. Das heißt genau: Für jedes j gibt es einen Skalar $d_j \in k$ mit

$$F(b_j) = d_j b_j.$$

Da $b_j \neq 0$ gilt, ist dies genau die Aussage, dass jeder Basisvektor b_j ein Eigenvektor von F ist.

Also ist B genau dann diagonalisierend, wenn sie eine Eigenbasis ist. □

Lemma 8.3.9 (Basiswechselmatrizen für Standardbasis). *Sei $A \in M_n(k)$, und sei $F = L_A : k^n \to k^n$ die zugehörige lineare Abbildung. Sei $E = (e_1, \dots, e_n)$ die Standardbasis und $B = (b_1, \dots, b_n)$ eine weitere Basis von k^n.*

Es gilt dann $T_B = M_{E \leftarrow B}(\mathrm{Id})$ und weiterhin

$$M_{B \leftarrow B}(L_A) = T_B^{-1} A T_B.$$

Wobei T_B die Matrix ist, deren i-te Spalte genau b_i ist.

Beweis. Es ist $T_B = M_{E \leftarrow B}(\mathrm{Id})$, denn für alle $i \in \{1, \dots, n\}$ gilt:

$$\begin{aligned}[\mathrm{Id}(b_i)]_E = [b_i]_E &= b_i \\ &= T_B \cdot e_i \\ &= T_B \cdot [b_i]_B .\end{aligned}$$

Der wichtigste Schritt ist genau die Erkenntnis, dass $[b_i]_B = e_i$. Das liegt daran, dass $b_i = \sum_{j=1}^n \delta_{j,i} b_j$, wobei

$$\delta_{j,i} = \begin{cases} 1 & i = j \\ 0 & i \neq j . \end{cases}$$

Es ist natürlich $(e_i)_j = \delta_{j,i}$ und daher folgt $[b_i]_B = e_i$.

Da die b_i eine Basis bilden zeigt das, dass die definierende Gleichung (†) erfüllt ist.

Damit folgt die Behauptung aus der Basiswechselformel Korollar 5.4.10.

Wir gehen es nochmal im Detail durch: T übersetzt B-Koordinaten in Standardkoordinaten:

$$[v]_E = T[v]_B.$$

Für $v \in k^n$ gilt daher

$$[F(v)]_E = A[v]_E = AT[v]_B.$$

Um wieder zu B-Koordinaten zurückzukehren, muss man mit $T^{-1} = M_{B \leftarrow E}(\mathrm{Id})$ multiplizieren. Also gilt

$$[F(v)]_B = T^{-1} AT [v]_B.$$

Damit ist

$$M_{B \leftarrow B}(L_A) = T^{-1} AT.$$ □

Lemma 8.3.10 (Matrixform der Diagonalisierbarkeit). *Sei $A \in M_n(k)$, und sei $F = L_A : k^n \to k^n$ die zugehörige lineare Abbildung. Dann ist F genau dann diagonalisierbar, wenn es eine invertierbare Matrix $T \in M_n(k)$ gibt, so dass*

$$T^{-1} AT$$

Diagonalgestalt hat.

Beweis. Sei E die Standardbasis von k^n. Sei zunächst $B = (b_1, \dots, b_n)$ eine Basis von k^n, und sei T_B die Matrix, deren Spalten die Vektoren $b_1, \dots, b_n$ sind.

Es gilt dann

$$M_{B \leftarrow B}(L_A) = T_B^{-1} A T_B.$$

Also hat $T_B^{-1} A T_B$ Diagonalgestalt, genau dann wenn $M_{B \leftarrow B}(L_A)$ Diagonalgestalt hat. □

Theorem 8.3.11 (Charakterisierungen der Diagonalisierbarkeit). *Sei $F \in \mathrm{End}(V)$, und setze $n := \dim(V)$. Die Eigenwerte von F in k bilden eine endliche Menge. Wir bezeichnen sie mit $\lambda_1, \dots, \lambda_s$. Falls F keine Eigenwerte in k hat, sind die Summe in (3) als $\{0\}$ und die Summe in (4) als 0 zu lesen. Dann sind äquivalent:*

1. *F ist diagonalisierbar.*
2. *V besitzt eine Basis aus Eigenvektoren von F.*
3. *V ist die Summe der Eigenräume:*

$$V = E_{\lambda_1}(F) + \cdots + E_{\lambda_s}(F).$$

4. *Die Summe der geometrischen Vielfachheiten aller Eigenwerte ist n:*

$$\sum_{i=1}^{s} \dim E_{\lambda_i}(F) = n.$$

Beweis. Nun zeigen wir Implikationen und Äquivalenzen einzeln, zusammen ergeben sie die behauptete Äquivalenz aller Aussagen.

1. $\Leftrightarrow$ 2.**:** Das ist genau Lemma 8.3.8.

2. $\Rightarrow$ 3.**:** Sei B eine Basis aus Eigenvektoren von F. Jeder Vektor aus B liegt in einem Eigenraum von F. Da B den ganzen Raum V erzeugt, liegt jeder Vektor aus V in der Summe der Eigenräume. Also gilt
$$V = E_{\lambda_1}(F) + \cdots + E_{\lambda_s}(F).$$

3. $\Rightarrow$ 2.**:** Nach Korollar 8.3.5 ist die Summe der Eigenräume zu paarweise verschiedenen Eigenwerten direkt. Wählt man in jedem Eigenraum $E_{\lambda_i}(F)$ eine Basis, dann darf man diese Basen nach Lemma 8.3.4 zusammenlegen. Man erhält dadurch eine Basis der Summe
$$E_{\lambda_1}(F) + \cdots + E_{\lambda_s}(F).$$
Falls diese Summe gleich V ist, ist die zusammengelegte Familie eine Basis von V. Alle ihre Vektoren sind Eigenvektoren von F. Also besitzt V eine Basis aus Eigenvektoren.

3. $\Leftrightarrow$ 4.**:** Wegen Korollar 8.3.5 ist die Summe der Eigenräume direkt. Daher gilt nach Lemma 8.3.4
$$\dim\left(E_{\lambda_1}(F) + \cdots + E_{\lambda_s}(F)\right) = \sum_{i=1}^{s} \dim E_{\lambda_i}(F).$$
Die Summe der Eigenräume ist ein Untervektorraum von V. Ein Untervektorraum eines n-dimensionalen Raums ist genau dann der ganze Raum, wenn seine Dimension gleich n ist. Also ist 3. genau dann erfüllt, wenn die Summe der geometrischen Vielfachheiten gleich n ist. Das ist Aussage 4. □

Korollar 8.3.12 (Maximal viele Eigenwerte erzwingen Diagonalisierbarkeit)**.** *Ein Endomorphismus $F : V \to V$ mit* $\dim(V)$*-vielen verschiedenen Eigenwerten ist diagonalisierbar.*

Beweis. Jeder der $\dim(V)$ Eigenwerte steuert einen Eigenraum der Dimension mindestens 1 bei. Die Summe der Eigenräume ist direkt, also hat sie mindestens Dimension $\dim(V)$ — und damit genau $\dim(V)$. Die Eigenräume spannen also ganz V auf, und aus Basen der Eigenräume setzt sich eine Eigenbasis von V zusammen. □

Leitbeispiel 8.3.13 (Zwei gekoppelte Pendel: Diagonalisieren heißt entkoppeln)**.** Die Pendelmatrix K aus Leitbeispiel 8.1.4 hat die zwei verschiedenen Eigenwerte 1 und 3 bei $\dim(\mathbb{R}^2) = 2$. Nach dem Korollar ist K also diagonalisierbar — ganz ohne weitere Rechnung.

Die Rechnung ist trotzdem lehrreich. Als Spalten der Basiswechselmatrix T nehmen wir die Eigenvektoren. Merkregel für die Richtung: T trägt die Eigenvektoren als Spalten und übersetzt Moden-Koordinaten in Standard-Koordinaten — deshalb steht T in $T^{-1}KT$ *rechts*:

$$T = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad T^{-1} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad T^{-1}KT = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}.$$

In der Basis aus Eigenvektoren ist von der Kopplung nichts mehr übrig: Die Diagonalmatrix beschreibt zwei getrennte Systeme, eines mit Rückstellfaktor 1, eines mit Rückstellfaktor 3. Der Übergang $x \mapsto T^{-1}x$ ist dabei (bis auf den harmlosen Faktor $\frac{1}{2}$) genau der Wechsel zu den Modenkoordinaten $u = x_1 + x_2$ und $w = x_1 - x_2$ aus dem Leitbeispiel. Das ist die verlässlichste Intuition dieses Kapitels:

Diagonalisieren heißt: Koordinaten finden, in denen das System entkoppelt.

Dasselbe Rezept steckt hinter der Binet-Formel aus Beispiel 8.1.14: Dort entkoppelt der Wechsel in die φ- und ψ-Richtung die Fibonacci-Rekursion, und aus der Iteration werden zwei unabhängige Potenzen.

Beispiel 8.3.14 (Eine Scherung ist nicht diagonalisierbar)**.** Dass Diagonalisierbarkeit keine Selbstverständlichkeit ist, zeigt schon eine 2×2-Matrix: die *Scherung*

$$S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad S\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + y \\ y \end{pmatrix}.$$

Man kann sie sich als das Schieben eines Kartenstapels vorstellen: Jede waagerechte Schicht gleitet proportional zu ihrer Höhe zur Seite.

Das charakteristische Polynom ist

$$p_S(X) = (X - 1)^2,$$

der einzige Eigenwert ist also 1, mit algebraischer Vielfachheit 2. Der zugehörige Eigenraum ist

$$E_1(S) = \operatorname{Kern}(S - 1_2) = \operatorname{Kern}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \operatorname{Span}\left((1, 0)\right),$$

also nur die x-Achse: Die geometrische Vielfachheit ist 1. Anschaulich ist das klar — die unterste Karte bleibt liegen, jede andere Richtung wird beim Scheren gekippt.

Die Summe der geometrischen Vielfachheiten ist damit $1 < 2$, und nach dem Charakterisierungssatz ist S *nicht* diagonalisierbar. Hier klafft zum ersten Mal die Lücke

$$\text{geometrische Vielfachheit} \;<\; \text{algebraische Vielfachheit},$$

die das Lemma vom Anfang dieses Abschnitts ausdrücklich erlaubt.

Ein zweites Argument kommt ganz ohne Rechnung aus: Wäre S diagonalisierbar, dann wäre S in einer geeigneten Basis die Diagonalmatrix mit dem einzigen Eigenwert 1 auf der Diagonale — also die Einheitsmatrix. Dann wäre aber schon $S = T \cdot 1_2 \cdot T^{-1} = 1_2$, ein Widerspruch: Die Scherung ist nicht die Identität.

Kapitel 9

Skalarprodukte

9.1 Euklidische Vektorräume

Wir arbeiten in diesem Abschnitt ausschließlich über dem Körper $\mathbb{R}$. Das ist wichtig: Die Begriffe „positiv“ und „größer als Null“ sind Begriffe für reelle Zahlen.

9.1.1 Reelle Bilinearformen

Sei V ein $\mathbb{R}$-Vektorraum.

Definition 9.1.1 (Bilinearform)**.** Eine Abbildung

$$b : V \times V \to \mathbb{R}$$

heißt eine *Bilinearform*, wenn b linear in beiden Argumenten ist.
Genauer heißt das: Für alle $u, v, w \in V$ und alle $\lambda, \mu \in \mathbb{R}$ gilt

$$b(\lambda u + \mu v, w) = \lambda b(u, w) + \mu b(v, w)$$

und

$$b(u, \lambda v + \mu w) = \lambda b(u, v) + \mu b(u, w).$$

Definition 9.1.2 (Symmetrische Bilinearform)**.** Eine Bilinearform

$$b : V \times V \to \mathbb{R}$$

heißt *symmetrisch*, wenn für alle $u, w \in V$ gilt

$$b(u, w) = b(w, u).$$

Definition 9.1.3 (Positive Definitheit)**.** Sei V ein $\mathbb{R}$-Vektorraum, und sei $b : V \times V \to \mathbb{R}$ eine symmetrische Bilinearform. Dann heißt b *positiv definit*, wenn für alle $v \in V$ mit $v \neq 0$ gilt

$$b(v, v) > 0.$$

Beispiel 9.1.4 (Ein Beispiel und ein Gegenbeispiel)**.** Auf $\mathbb{R}^n$ ist

$$b(u, w) := w^\top u = \sum_{i=1}^{n} u_i w_i$$

eine positiv definite symmetrische Bilinearform. Denn b ist bilinear, symmetrisch, und für $u \neq 0$ gilt

$$b(u, u) = u_1^2 + \cdots + u_n^2 > 0.$$

Ein Gegenbeispiel auf $\mathbb{R}^2$ ist

$$b\left(\begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} r \\ s \end{pmatrix}\right) := xr - ys.$$

Diese Abbildung ist bilinear und symmetrisch. Sie ist aber nicht positiv definit, denn

$$b\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = -1 < 0.$$

9.1.2 Bilinearformen als Matrizen

Lemma 9.1.5 (Bilinearformen und Matrizen)**.** *Sei $b : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ eine Bilinearform. Dann gibt es genau eine Matrix $A \in M_n(\mathbb{R})$ mit*

$$b(v, w) = v^\top A w$$

für alle $v, w \in \mathbb{R}^n$. Sie ist gegeben durch

$$A_{ij} := b(e_i, e_j),$$

wobei $e_1, \ldots, e_n$ die Standardbasis von $\mathbb{R}^n$ ist.

Umgekehrt definiert jede Matrix $A \in M_n(\mathbb{R})$ durch

$$b_A(v, w) := v^\top A w$$

eine Bilinearform auf $\mathbb{R}^n$.

Beweis. Seien

$$v = \sum_{i=1}^{n} v_i e_i \quad \text{und} \quad w = \sum_{j=1}^{n} w_j e_j.$$

Dann folgt aus der Bilinearität

$$b(v, w) = \sum_{i=1}^{n} \sum_{j=1}^{n} v_i w_j b(e_i, e_j).$$

Setzen wir $A_{ij} := b(e_i, e_j)$, dann ist dies genau

$$b(v, w) = v^\top A w.$$

Damit ist auch die Eindeutigkeit klar: Die Matrixeinträge müssen notwendigerweise die Zahlen $b(e_i, e_j)$ sein.

Das passt genau zum Prinzip der linearen Fortsetzung. Für festes v ist die Abbildung

$$w \mapsto b(v, w)$$

linear. Also reicht es, ihre Werte auf der Basis $e_1, \dots, e_n$ zu kennen. Diese Werte sind die Zahlen $b(v, e_j)$. Für festes e_j ist wiederum

$$v \mapsto b(v, e_j)$$

linear. Also reichen auch hier die Werte auf der Basis $e_1, \dots, e_n$. Am Ende ist die ganze Bilinearform durch die Zahlen $b(e_i, e_j)$ bestimmt.

Ist umgekehrt $A \in M_n(\mathbb{R})$, dann ist

$$(v, w) \mapsto v^\top A w$$

linear in beiden Argumenten. Also ist b_A eine Bilinearform. □

Lemma 9.1.6 (Symmetrie und Matrixsymmetrie)**.** *Sei $b : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ eine Bilinearform, und sei $A \in M_n(\mathbb{R})$ die assoziierte Matrix aus dem vorherigen Lemma. Dann ist b genau dann symmetrisch, wenn A symmetrisch ist, also wenn*

$$A^\top = A$$

gilt.

Beweis. Ist b symmetrisch, dann gilt für alle $i, j \in \{1, \dots, n\}$

$$A_{ij} = b(e_i, e_j) = b(e_j, e_i) = A_{ji}.$$

Also ist $A^\top = A$.

Sei umgekehrt $A^\top = A$. Dann gilt für alle $v, w \in \mathbb{R}^n$

$$b(v, w) = v^\top A w.$$

Da $v^\top A w$ eine 1×1-Matrix ist, ist sie gleich ihrer Transponierten. Also gilt

$$v^\top A w = \left(v^\top A w\right)^\top = w^\top A^\top v = w^\top A v = b(w, v).$$

Also ist b symmetrisch. □

Definition 9.1.7 (Positive Definitheit von Matrizen im reellen Fall)**.** Eine symmetrische Matrix $A \in M_n(\mathbb{R})$ heißt *positiv definit*, wenn für alle $v \in \mathbb{R}^n$ mit $v \neq 0$

$$v^\top A v > 0$$

gilt.

Lemma 9.1.8 (Positive Definitheit und Matrizen)**.** *Sei $b : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ eine Bilinearform, und sei $A \in M_n(\mathbb{R})$ die assoziierte Matrix. Dann ist b genau dann ein Skalarprodukt auf $\mathbb{R}^n$, wenn A symmetrisch positiv definit ist.*

Beweis. Nach dem vorherigen Lemma ist b genau dann symmetrisch, wenn A symmetrisch ist. Außerdem gilt für alle $v \in \mathbb{R}^n$

$$b(v, v) = v^\top A v.$$

Daher ist die positive Definitheit von b genau die Bedingung

$$v^\top A v > 0 \quad \text{für alle } v \neq 0.$$

Zusammen ergibt das genau die Behauptung. □

9.1.3 Reelle Skalarprodukte und Normen

Definition 9.1.9 (Skalarprodukt und induzierte Norm)**.** Sei V ein $\mathbb{R}$-Vektorraum. Ein *Skalarprodukt* auf V ist eine positiv definite symmetrische Bilinearform auf V.

Für ein Skalarprodukt schreibt man meistens

$$\langle u, w\rangle$$

statt $b(u, w)$.

Bemerkung 9.1.10. Eine Norm ist ein mathematisches Objekt das Längen auf einem Vektorraum auf eine konsistente Weise festlegt bzw. misst. Der Abstand zweier Vektoren $v, w \in V$ unter einer Norm $\|\cdot\|$ ist dann definiert als

$$\|v - w\| .$$

Man kann Normen auch abstrakt definieren und stellt dann fest, dass nicht jede Norm von einem Skalarprodukt kommt. Dies wird aber erst im unendlich-dimensionalen relevant, ist daher vorallem für die Analysis von Interesse. Im endlich-dimensionalen gilt tatsächlich, dass – unter einem bestimmten, engen Begriff von Äquivalenz – alle Normen äquivalent sind.

Exakt gleich sind natürlich nicht alle Normen. Es kommen auch nicht alle Normen von einem Skalarprodukt.

Bemerkung 9.1.11 (Warum wir positive Definitheit wollen)**.** Die Zahl $\langle v, v\rangle$ soll das Quadrat der Länge von v sein. Positive Definitheit sagt genau die beiden Dinge, die man für einen Längenbegriff erwartet:

1. Es gibt keine negativen Quadratlängen.
2. Nur der Nullvektor hat Länge Null.

Ohne positive Definitheit könnte ein Nichtnullvektor Länge Null haben, oder sogar eine negative Quadratlänge. Dann wäre $\sqrt{\langle v, v\rangle}$ kein sinnvoller reeller Längenbegriff mehr.

Normen sind Arten, Längen zu messen. Ein Skalarprodukt ist noch stärker: Es misst nicht nur Längen, sondern auch Winkel und Projektionen.

Definition 9.1.12 (Euklidischer Vektorraum)**.** Ein *euklidischer Vektorraum* ist ein endlich-dimensionaler $\mathbb{R}$-Vektorraum V zusammen mit einem Skalarprodukt $\langle\cdot,\cdot\rangle$ auf V. Das Skalarprodukt induziert auf V den Längenbegriff (die *Norm*)

$$\|v\| = \sqrt{\langle v, v\rangle}.$$

Bemerkung 9.1.13 (Warum abstrakte Skalarprodukte nützlich sind)**.** Das Standardskalarprodukt auf $\mathbb{R}^n$ ist sehr wichtig, aber es ist nicht das einzige sinnvolle Skalarprodukt. Allgemeiner definiert jede symmetrische Matrix $A \in M_n(\mathbb{R})$ eine symmetrische Bilinearform

$$\langle u, w\rangle_A := w^\top A u.$$

(Man beachte die Reihenfolge: Das zweite Argument steht links vor der Matrix. Für symmetrisches A gilt $w^\top A u = u^\top A w$, beide Lesarten stimmen also überein — wir schreiben die Variante, die später zum komplexen Fall passt.) Wir nennen A positiv definit, falls die assoziierte symmetrische Bilinearform positiv definit ist. Wir werden später ein Kriterium dafür kennenlernen.

In verschiedenen Situationen ist nicht das Standardskalarprodukt die richtige Wahl, sondern ein auf das Problem zugeschnittenes Skalarprodukt. Ein typisches physikalisches Beispiel kommt aus

der Mechanik. Beschreibt man ein System von Teilchen durch ihre gewöhnlichen Ortskoordinaten, dann ist die kinetische Energie zunächst einfach die Summe

$$E_{\text{kinetisch}} = \frac{1}{2} \sum_i m_i \|v_i\|^2 .$$

Das kleinste Beispiel macht den Übergang zur Matrix sichtbar: Zwei Teilchen auf einer Schiene haben je eine Geschwindigkeit $v_1, v_2 \in \mathbb{R}$. Wir *stapeln* beide zu einem Vektor $v = (v_1, v_2) \in \mathbb{R}^2$ und erhalten

$$E_{\text{kinetisch}} = \tfrac{1}{2} m_1 v_1^2 + \tfrac{1}{2} m_2 v_2^2 = \frac{1}{2} v^\top D v \qquad \text{mit} \qquad D = \begin{pmatrix} m_1 & 0 \\ 0 & m_2 \end{pmatrix}.$$

Genauso im Allgemeinen: Man stapelt alle Geschwindigkeitskomponenten aller Teilchen zu einem einzigen langen Vektor v (bei N Teilchen im Raum hat er $3N$ Einträge), und D ist die Diagonalmatrix, in der jede Masse einmal pro Raumkoordinate — also dreimal — auftaucht.

Benutzt man andere Koordinaten, zum Beispiel Winkel statt Ortskoordinaten (sogenannte generalisierte Koordinaten), dann kann dieselbe kinetische Energie die Form

$$E_{\text{kinetisch}}(v) = \frac{1}{2} v^\top M v$$

haben, wobei M eine symmetrische positiv definite Matrix ist. Dabei können auch Einträge außerhalb der Diagonale auftreten. Sie bedeuten nicht, dass der physikalische Raum selbst schief ist, sondern dass die gewählten Koordinatenrichtungen in der kinetischen Energie miteinander gekoppelt sind.

In dieser Situation definiert

$$\langle v, w \rangle_M := w^\top M v$$

ein natürliches Skalarprodukt auf dem Raum der Geschwindigkeiten. Die kinetische Energie ist dann

$$E_{\text{kinetisch}}(v) = \frac{1}{2} \langle v, v \rangle_M .$$

Das Skalarprodukt enthält also die physikalische Information darüber, welche Geschwindigkeitsrichtungen viel oder wenig kinetische Energie kosten.

Leitbeispiel 9.1.14 (Der Trägheitstensor)**.** Das eben genannte physikalische Beispiel wird unser Leitfaden durch das ganze Kapitel. Ein starrer Körper (*Körper* hier im Alltagssinn — nicht der algebraische!) drehe sich mit der Winkelgeschwindigkeit $\omega \in \mathbb{R}^3$. Dabei ist ω ein Vektor, der zwei Angaben zugleich kodiert: Er zeigt entlang der *Drehachse*, und seine Länge ist das *Drehtempo*. Die Rotationsenergie des Körpers ist

$$T(\omega) = \tfrac{1}{2}\, \omega^\top I \omega,$$

wobei $I \in M_3(\mathbb{R})$ der *Trägheitstensor* des Körpers ist: eine symmetrische Matrix, die die Massenverteilung kodiert. Diese Formel ist das Dreh-Analogon der kinetischen Energie $\frac{1}{2} m v^2$ — nur ist die „Masse“ jetzt eine Matrix, weil der Körper um verschiedene Achsen verschieden träge ist. Wie man I aus der Massenverteilung ausrechnet, ist ein Integral und gehört in die Physik; wir nehmen die Matrix als gegeben. („Tensor“ ist nur der historische Name — für uns ist I eine symmetrische Matrix.

Und das Energiesymbol T hat mit dem Transponieren in $\omega^\top$ nichts zu tun; eine unglückliche, aber übliche Doppelbelegung. Diese wird (in dieser neuen Version des Skriptes) auch dadurch abgemildert, dass das Symbol $\top$ statt T zum Transponieren verwendet wird.) Wie im vorigen Beispiel ist

$$\langle \omega, \omega' \rangle_I := \omega'^\top I \omega$$

eine symmetrische Bilinearform, und die Energie ist $T(\omega) = \frac{1}{2}\langle \omega, \omega \rangle_I$.

Wann ist diese Form *positiv definit*, also ein Skalarprodukt? Genau dann, wenn jede noch so kleine Drehung Energie kostet, wenn also $T(\omega) > 0$ für alle $\omega \neq 0$ gilt. Das trifft auf jeden Körper zu, dessen Masse nicht vollständig auf einer einzigen Geraden liegt. (Der idealisierte, unendlich dünne Stab ist die Ausnahme — aber nur für eine ganz bestimmte Drehachse: Für ω *entlang der Stabachse* ist $T(\omega) = 0$, denn alle Masse liegt auf der Achse und nichts bewegt sich; für jedes andere ω ist $T(\omega) > 0$. Die Form ist dann nur *positiv semidefinit* — ein konkreter Vektor $\omega \neq 0$ mit $\langle \omega, \omega \rangle_I = 0$.) Für einen echten dreidimensionalen Körper ist I also symmetrisch positiv definit — ein maßgeschneidertes Skalarprodukt, das misst, welche Drehachsen viel und welche wenig Energie kosten.

Dieses eine Beispiel liefert uns Intuition für alle großen Sätze des Kapitels: orthonormale *Hauptachsen* des Körpers, die Drehgruppe als Symmetrie, ein Kriterium für positive Definitheit (Hurwitz) — und als Höhepunkt die *Hauptachsentransformation*, die den Trägheitstensor diagonalisiert und die Drehung in unabhängige Achsen entkoppelt.

Bemerkung 9.1.15 (Positive Definitheit und zweite Ableitungen)**.** Positive Definitheit tritt auch in der Analysis natürlich auf. Bei einer zweimal stetig-differenzierbaren Funktion $f : \mathbb{R} \to \mathbb{R}$ untersucht man an einem Punkt a mit $f'(a) = 0$ das Vorzeichen von $f''(a)$. Ist $f''(a) > 0$, dann krümmt sich die Funktion dort nach oben, und man hat ein lokales Minimum.

Für Funktionen $f : \mathbb{R}^n \to \mathbb{R}$ übernimmt die Hesse-Matrix die Rolle der zweiten Ableitung. Ist f zweimal stetig-differenzierbar, dann ist die Hesse-Matrix

$$H_f(a) = \left(\frac{\partial^2 f}{\partial x_i \partial x_j}(a) \right)_{i,j}$$

wegen des Satzes von Schwarz symmetrisch. Sie definiert daher eine symmetrische Bilinearform

$$b_a(v, w) := w^\top H_f(a) v.$$

Positive Definitheit bedeutet dann: In jeder von Null verschiedenen Richtung ist die zweite Änderung positiv. Das ist die mehrdimensionale Version der Bedingung $f''(a) > 0$.

Bemerkung 9.1.16 (Zur Bezeichnung „euklidisch“)**.** Der Ausdruck „euklidischer Vektorraum“ ist moderne mathematische Sprache. Er bedeutet nicht, dass Euklid selbst Geometrie in der Sprache von Vektorräumen, Skalarprodukten oder Koordinaten betrieben hätte. Euklid dachte synthetisch: Punkte, Geraden, Kreise, Konstruktionen und Winkel standen im Vordergrund, nicht Abbildungen $V \times V \to \mathbb{R}$.

Die Verbindung ist eine moderne abstrakte Identifikation. Wenn man die Ebene als $\mathbb{R}^2$ mit dem Standardskalarprodukt modelliert, dann lassen sich viele klassische geometrische Aussagen als Aussagen über Vektoren und Skalarprodukte formulieren. Ob man deshalb sagen möchte, dass „derselbe Gegenstand“ betrachtet wird, ist eher eine philosophische Frage als eine Rechenregel.

Ein gutes Beispiel ist Rechtwinkligkeit. Bei Euklid ist ein rechter Winkel ein geometrischer Grundbegriff, beschrieben über Geraden und die Gleichheit benachbarter Winkel. Im modernen euklidischen Vektorraum definieren wir dagegen

$$v \perp w \quad \Longleftrightarrow \quad \langle v, w \rangle = 0.$$

Das ist nicht Euklids Definition in neuer Schrift, sondern eine moderne Definition, die im Standardmodell genau die erwartete Geometrie rekonstruiert.

Man sollte „euklidisch“ hier also freundlich aber nüchtern lesen: Es geht um die moderne lineare Algebra der positiven definiten Längen- und Winkelgeometrie. Es geht nicht unmittelbar um die historische Arbeitsweise in den *Elementen*.

9.2 Unitäre Vektorräume

Wir arbeiten in diesem Abschnitt über dem Körper $\mathbb{C}$. Der wesentliche Unterschied zum reellen Fall ist die komplexe Konjugation. Ein Skalarprodukt auf einem komplexen Vektorraum kann nicht in beiden Argumenten komplex-linear und zugleich positiv definit sein. Darum ersetzt man Bilinearität durch Sesquilinearität.

9.2.1 Komplexe Sesquilinearformen

Sei V ein $\mathbb{C}$-Vektorraum.

Definition 9.2.1 (Sesquilinearform)**.** Eine Abbildung

$$b : V \times V \to \mathbb{C}$$

heißt eine *Sesquilinearform*, wenn sie linear im ersten Argument und antilinear im zweiten Argument ist.

Genauer heißt das: Für alle $u, v, w \in V$ und alle $\lambda, \mu \in \mathbb{C}$ gilt also die Linearität im ersten Argument

$$b(\lambda u + \mu v, w) = \lambda b(u, w) + \mu b(v, w)$$

und die Antilinearität im zweiten Argument

$$b(u, \lambda v + \mu w) = \overline{\lambda} b(u, v) + \overline{\mu} b(u, w).$$

Bemerkung 9.2.2 (Antilinearität)**.** Der Begriff „antilinear“ klingt deutlich dramatischer als er letztlich ist. Insbesondere heißt Antilinearität nicht das völlige Gegenteil von Linearität sondern lediglich, dass Skalare beim herausziehen noch komplex konjugiert werden.

Bemerkung 9.2.3 (Konvention)**.** Wir verwenden die mathematische Konvention, dass das Sesquilinearformen im ersten Argument linear und im zweiten Argument antilinear sind. In Teilen der Physik wird die umgekehrte Konvention verwendet. Die Begriffe bleiben gleich, aber manche Formeln werden dann komplex konjugiert.

Definition 9.2.4 (Hermitesche Form)**.** Sei V ein $\mathbb{C}$-Vektorraum. Eine Sesquilinearform

$$b : V \times V \to \mathbb{C}$$

heißt *hermitesch-symmetrisch* und eine *hermitesche Form*, wenn für alle $u, w \in V$ gilt

$$b(u, w) = \overline{b(w, u)}.$$

Bemerkung 9.2.5 (Reelle Werte)**.** Für jede Hermitesche Form gilt $b(v, v) \in \mathbb{R}$ für alle $v \in V$.

Definition 9.2.6 (Positive Definitheit)**.** Sei V ein $\mathbb{C}$-Vektorraum, und sei $b : V \times V \to \mathbb{C}$ eine hermitesche Form. Dann heißt b *positiv definit*, wenn für alle $v \in V$ mit $v \neq 0$ gilt

$$b(v, v) > 0.$$

Diese Ungleichung ist sinnvoll, weil $b(v, v)$ für hermitesche Formen reell ist.

Beispiel 9.2.7 (Ein Beispiel und ein Gegenbeispiel)**.** Auf $\mathbb{C}^n$ ist

$$b(u,w) := w^H u = \sum_{i=1}^{n} u_i \overline{w_i}$$

eine positiv definite hermitesche Form. Hier bezeichnet w^H die hermitesch transponierte Zeile $\overline{w}^\top$. Für $u \neq 0$ gilt

$$b(u,u) = |u_1|^2 + \cdots + |u_n|^2 > 0.$$

Ein Gegenbeispiel auf $\mathbb{C}^2$ ist

$$b\left(\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}, \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}\right) := z_1\overline{w_1} - z_2\overline{w_2}.$$

Diese Abbildung ist hermitesch, aber nicht positiv definit, denn

$$b\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = -1 < 0.$$

9.2.2 Sesquilinearformen als Matrizen

Lemma 9.2.8 (Sesquilinearformen und Matrizen)**.** *Sei $b : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$ eine Sesquilinearform. Dann gibt es genau eine Matrix $A \in M_n(\mathbb{C})$ mit*

$$b(v,w) = w^H A v$$

für alle $v, w \in \mathbb{C}^n$. Sie ist gegeben durch

$$A_{ij} := b(e_j, e_i),$$

wobei $e_1, \ldots, e_n$ die Standardbasis von $\mathbb{C}^n$ ist.

Umgekehrt definiert jede Matrix $A \in M_n(\mathbb{C})$ durch

$$b_A(v,w) := w^H A v$$

eine Sesquilinearform auf $\mathbb{C}^n$.

Beweis. Seien

$$v = \sum_{j=1}^{n} v_j e_j \quad \text{und} \quad w = \sum_{i=1}^{n} w_i e_i.$$

Da b im ersten Argument linear und im zweiten Argument antilinear ist, gilt

$$b(v,w) = \sum_{j=1}^{n} \sum_{i=1}^{n} v_j \overline{w_i}\, b(e_j, e_i).$$

Setzen wir $A_{ij} := b(e_j, e_i)$, dann ist dies genau

$$b(v,w) = w^H A v.$$

Damit ist auch die Eindeutigkeit klar: Die Matrixeinträge müssen notwendigerweise die Zahlen $b(e_j, e_i)$ sein.

Auch hier ist das nur lineare Fortsetzung mit einem Konjugationstwist. Für festes v ist die Abbildung

$$w \mapsto b(v, w)$$

antilinear. Also reicht es, die Werte auf der Basis $e_1, \dots, e_n$ zu kennen. Für festes e_i ist wiederum

$$v \mapsto b(v, e_i)$$

linear. Also reichen auch hier die Werte auf der Basis $e_1, \dots, e_n$. Am Ende ist die ganze Sesquilinearform durch die Zahlen $b(e_j, e_i)$ bestimmt.

Ist umgekehrt $A \in M_n(\mathbb{C})$, dann ist

$$(v, w) \mapsto w^H A v$$

linear im ersten Argument und antilinear im zweiten Argument. Also ist b_A eine Sesquilinearform. □

Definition 9.2.9 (Hermitesche Matrix)**.** Eine Matrix $A \in M_n(\mathbb{C})$ heißt *hermitesch*, wenn

$$A^H = A$$

gilt. Dabei ist

$$A^H := \overline{A}^\top$$

die hermitesch transponierte Matrix.

Korollar 9.2.10 (Determinante der hermitesch transponierten Matrix)**.** *Für jede Matrix $A \in M_n(\mathbb{C})$ gilt*

$$\det\left(A^H\right) = \overline{\det(A)}.$$

Insbesonder gilt für eine hermitesche Matrix A, dass

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

Beweis. Wir erinnern an Theorem 7.3.5

$$\det\left(A^\top\right) = \det(A)\,.$$

Daher gilt für jede Matrix $A \in M_n(\mathbb{C})$

$$\det\left(A^H\right) = \det\left(\overline{A}^\top\right) = \det\left(\overline{A}\right) = \overline{\det(A)}.$$

Ist nun $A^H = A$, dann folgt

$$\det(A) = \det\left(A^H\right) = \overline{\det(A)}.$$

Eine komplexe Zahl ist genau dann reell, wenn sie gleich ihrer komplex konjugierten Zahl ist. Also ist $\det(A) \in \mathbb{R}$. □

Lemma 9.2.11 (Hermitesche Formen und hermitesche Matrizen)**.** *Sei $b : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$ eine Sesquilinearform, und sei $A \in M_n(\mathbb{C})$ die assoziierte Matrix aus dem vorherigen Lemma. Dann ist b genau dann hermitesch, wenn A hermitesch ist.*

Beweis. Sei zunächst A hermitesch. Dann gilt für alle $v, w \in \mathbb{C}^n$

$$b(v, w) = w^H A v.$$

Außerdem gilt

$$\overline{b(w, v)} = \overline{v^H A w} = w^H A^H v = w^H A v = b(v, w).$$

Also ist b hermitesch.

Sei umgekehrt b hermitesch. Dann gilt für alle $v, w \in \mathbb{C}^n$

$$w^H A v = b(v, w) = \overline{b(w, v)} = w^H A^H v.$$

Also gilt

$$w^H \left(A - A^H\right) v = 0$$

für alle $v, w \in \mathbb{C}^n$. Setzen wir $v = e_j$ und $w = e_i$, erhalten wir

$$\left(A - A^H\right)_{ij} = 0.$$

Also ist $A = A^H$. □

Definition 9.2.12 (Positive Definitheit von Matrizen im komplexen Fall)**.** Eine Matrix $A \in M_n(\mathbb{C})$ heißt *hermitesch positiv definit*, wenn

$$A^H = A$$

gilt und für alle $v \in \mathbb{C}^n$ mit $v \neq 0$

$$v^H A v > 0$$

gilt. In vielen Texten sagt man dafür kurz: *A ist positiv definit*.

Lemma 9.2.13 (Positive Definitheit und Matrizen)**.** *Sei $b : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$ eine Sesquilinearform, und sei $A \in M_n(\mathbb{C})$ die assoziierte Matrix. Dann ist b genau dann ein Skalarprodukt auf $\mathbb{C}^n$, wenn A hermitesch positiv definit ist.*

Beweis. Nach dem vorherigen Lemma ist b genau dann hermitesch, wenn A hermitesch ist. Außerdem gilt für alle $v \in \mathbb{C}^n$

$$b(v, v) = v^H A v.$$

Daher ist die positive Definitheit von b genau die Bedingung

$$v^H A v > 0 \quad \text{für alle } v \neq 0.$$

Zusammen ergibt das genau die Behauptung. □

Bemerkung 9.2.14 (Hermitesche Matrizen als komplexe Analogie)**.** Im reellen Fall gehören symmetrische Matrizen zu symmetrischen Bilinearformen. Im komplexen Fall übernehmen hermitesche Matrizen diese Rolle.

So wie positive definite Hesse-Matrizen im reellen Fall lokale Minima erkennen, treten positive definite hermitesche Matrizen im komplexen Fall überall dort auf, wo komplexe Zustände eine reelle positive Größe bestimmen sollen: Normquadrate, Energien oder Wahrscheinlichkeiten.

9.2.3 Komplexe Skalarprodukte und Normen

Definition 9.2.15 (Skalarprodukt und induzierte Norm)**.** Sei V ein $\mathbb{C}$-Vektorraum. Ein *Skalarprodukt* auf V ist eine positiv definite hermitesche Form auf V.

Für ein Skalarprodukt schreibt man meistens

$$\langle u, w\rangle$$

statt $b(u, w)$.

Bemerkung 9.2.16 (Warum wir positive Definitheit wollen)**.** Auch im komplexen Fall soll $\langle v, v\rangle$ das Quadrat der Länge von v sein. Positive Definitheit sagt daher wieder genau:

1. Es gibt keine negativen Quadratlängen.
2. Nur der Nullvektor hat Länge Null.

Ohne positive Definitheit wäre $\|v\| = \sqrt{\langle v, v\rangle}$ kein sinnvoller reeller Längenbegriff.

In der Quantenmechanik ist diese Bedingung besonders natürlich: Normquadrate werden als Größen interpretiert, die nicht negativ sein dürfen, zum Beispiel als Wahrscheinlichkeiten (nach geeigneter Normierung).

Definition 9.2.17 (Unitärer Vektorraum)**.** Ein *unitärer Vektorraum* ist ein endlich-dimensionaler $\mathbb{C}$-Vektorraum V zusammen mit einem Skalarprodukt $\langle\cdot,\cdot\rangle$ auf V. Das Skalarprodukt induziert auf V den Längenbegriff (die *Norm*)

$$\|v\| = \sqrt{\langle v, v\rangle}.$$

Bemerkung 9.2.18 (Viele Skalarprodukte)**.** Auch auf $\mathbb{C}^n$ gibt es viele Skalarprodukte. Ist $A \in M_n(\mathbb{C})$ hermitesch und positiv definit, dann definiert

$$\langle u, w\rangle_A := w^H A u$$

ein Skalarprodukt auf $\mathbb{C}^n$. Das Standardskalarprodukt ist der Spezialfall $A = E_n$.

Ein physikalisches Beispiel entsteht bei endlich-dimensionalen Modellen der Quantenmechanik oder bei Diskretisierungen von Wellenfunktionen. Wenn die Komponenten eines Vektors Werte einer Wellenfunktion auf einem Gitter beschreiben, dann sollte das Skalarprodukt die Gittergewichte berücksichtigen. Statt

$$\sum_i \psi_i \overline{\varphi_i}$$

verwendet man dann zum Beispiel

$$\langle \psi, \varphi\rangle_h := \sum_i h_i \psi_i \overline{\varphi_i}$$

mit Gewichten $h_i > 0$. Das ist wieder ein Skalarprodukt, aber eines, das besser zur konkreten physikalischen Modellierung passt.

9.3 Orthogonalität und Orthonormalisierung

Wir arbeiten in diesem Abschnitt in einem euklidischen oder unitären Vektorraum. Im komplexen Fall verwenden wir weiterhin die Konvention, dass das Skalarprodukt im ersten Argument linear und im zweiten Argument antilinear ist.

Definition 9.3.1 (Orthogonalität)**.** Seien V ein euklidischer oder unitärer Vektorraum, und seien $v, w \in V$. Wir sagen, dass v und w *orthogonal* sind, wenn

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

gilt. In diesem Fall schreiben wir

$$v \perp w.$$

Ein System $(v_1, \dots, v_k)$ heißt *orthogonal*, wenn je zwei verschiedene Vektoren aus dem System orthogonal sind. Das heißt: Für alle $i \neq j$ gilt

$$\langle v_i, v_j \rangle = 0.$$

Definition 9.3.2 (Orthonormalität)**.** Ein System $(n_1, \dots, n_k)$ heißt *orthonormal*, wenn es orthogonal ist und zusätzlich jeder Vektor Norm 1 hat. Das heißt: Für alle i, j gilt

$$\langle n_i, n_j \rangle = \begin{cases} 1, & i = j, \\ 0, & i \neq j. \end{cases}$$

Bemerkung 9.3.3 (Normierung)**.** Ist $(v_1, \dots, v_k)$ ein orthogonales System und ist kein v_i der Nullvektor, dann kann man es sofort orthonormalisieren. Man setzt

$$n_i := \frac{1}{\|v_i\|} v_i.$$

Dann ist $(n_1, \dots, n_k)$ orthonormal. Die Orthogonalität bleibt erhalten, weil jeder Vektor nur mit einem von Null verschiedenen Skalar multipliziert wird.

Lemma 9.3.4 (Koordinaten in einem orthonormalen System)**.** *Sei $(n_1, \dots, n_k)$ ein orthonormales System in einem euklidischen oder unitären Vektorraum V. Dann gilt für jeden Vektor*

$$v \in \operatorname{Span}(n_1, \dots, n_k)$$

die Formel

$$v = \sum_{i=1}^{k} \langle v, n_i \rangle n_i.$$

Beweis. Da $v \in \operatorname{Span}(n_1, \dots, n_k)$ liegt, gibt es Skalare $\lambda_1, \dots, \lambda_k$ mit

$$v = \sum_{i=1}^{k} \lambda_i n_i.$$

Wir berechnen für ein festes j:

$$\langle v, n_j \rangle = \left\langle \sum_{i=1}^{k} \lambda_i n_i, n_j \right\rangle = \sum_{i=1}^{k} \lambda_i \langle n_i, n_j \rangle = \lambda_j.$$

Also sind die Koeffizienten von v bezüglich des orthonormalen Systems genau die Zahlen $\langle v, n_i \rangle$. Einsetzen ergibt die Behauptung. □

Bemerkung 9.3.5 (Hinweis auf Fourierreihen)**.** Dieses Lemma ist eine endliche Version einer wichtigen Idee aus der Analysis. Auf dem Raum $C^0([-\pi, \pi], \mathbb{R})$ der stetigen reellwertigen Funktionen auf $[-\pi, \pi]$ definiert

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

ein Skalarprodukt. Bezüglich dieses Skalarprodukts sind die Funktionen

$$\frac{1}{\sqrt{2}}, \cos(x), \sin(x), \cos(2x), \sin(2x), \ldots$$

orthonormal.

Für endliche Linearkombinationen solcher Funktionen kann man daher die Koeffizienten genau wie oben durch Skalarprodukte ablesen. In der Analysis wird daraus die Theorie der Fourierreihen. Dort zeigt man präzise, in welchem Sinn diese Funktionen ein vollständiges Orthonormalsystem bilden und von welchem Raum. Im Gegensatz zum endlich dimensionalen Fall ist das deutlich subtiler, weil man dann über Konvergenz von unendlichen Reihen sprechen muss. Das gehört in die Analysis.

Lemma 9.3.6 (Orthogonale Systeme sind linear unabhängig)**.** *Sei $(v_1, \ldots, v_k)$ ein orthogonales System in einem euklidischen oder unitären Vektorraum. Wenn kein v_i der Nullvektor ist, dann ist $(v_1, \ldots, v_k)$ linear unabhängig.*

Beweis. Seien $\lambda_1, \ldots, \lambda_k$ Skalare mit

$$\sum_{i=1}^{k} \lambda_i v_i = 0.$$

Wir zeigen, dass alle λ_j gleich Null sind. Sei dazu $j \in \{1, \ldots, k\}$. Dann gilt

$$0 = \left\langle \sum_{i=1}^{k} \lambda_i v_i, v_j \right\rangle = \sum_{i=1}^{k} \lambda_i \langle v_i, v_j \rangle = \lambda_j \langle v_j, v_j \rangle.$$

Da $v_j \neq 0$ ist, gilt $\langle v_j, v_j \rangle > 0$. Also ist $\lambda_j = 0$. Da j beliebig war, sind alle Koeffizienten gleich Null. Damit ist das System linear unabhängig. □

Bemerkung 9.3.7 (Warum das stark ist)**.** Lineare Unabhängigkeit ist normalerweise keine paarweise Eigenschaft. Ob ein System linear unabhängig ist, hängt im Allgemeinen vom Zusammenspiel aller Vektoren gleichzeitig ab. Orthogonalität ist dagegen paarweise definiert. Trotzdem folgt aus dieser paarweisen Bedingung sofort lineare Unabhängigkeit, sofern kein Nullvektor vorkommt. Das ist einer der Gründe, warum Orthogonalität so nützlich ist.

Lemma 9.3.8 (Einen neuen orthogonalen Vektor erzeugen)**.** *Sei $(n_1, \ldots, n_k)$ ein orthonormales System in einem euklidischen oder unitären Vektorraum V. Sei außerdem*

$$w \notin \operatorname{Span}(n_1, \ldots, n_k).$$

Dann ist

$$v_{k+1} := w - \sum_{i=1}^{k} \langle w, n_i \rangle n_i$$

ein Vektor mit folgenden Eigenschaften:

1. $v_{k+1} \neq 0$.

2. *Für alle $j \in \{1, \dots, k\}$ gilt $v_{k+1} \perp n_j$.*

3. *Es gilt*
$$\operatorname{Span}(n_1, \dots, n_k, w) = \operatorname{Span}(n_1, \dots, n_k, v_{k+1}).$$

Insbesondere ist
$$n_{k+1} := \frac{1}{\|v_{k+1}\|} v_{k+1}$$
wohldefiniert, und $(n_1, \dots, n_k, n_{k+1})$ ist orthonormal.

Beweis. Zunächst gilt $v_{k+1} \neq 0$. Denn wäre $v_{k+1} = 0$, dann wäre
$$w = \sum_{i=1}^{k} \langle w, n_i \rangle n_i$$
und damit $w \in \operatorname{Span}(n_1, \dots, n_k)$. Das widerspricht der Annahme.

Wir zeigen nun die Orthogonalität. Für $j = 1, \dots, k$ gilt
$$\langle v_{k+1}, n_j \rangle = \left\langle w - \sum_{i=1}^{k} \langle w, n_i \rangle n_i, n_j \right\rangle.$$
Da das Skalarprodukt im ersten Argument linear ist, ist dies gleich
$$\langle w, n_j \rangle - \sum_{i=1}^{k} \langle w, n_i \rangle \langle n_i, n_j \rangle = \langle w, n_j \rangle - \langle w, n_j \rangle = 0.$$
Also ist $v_{k+1} \perp n_j$ für alle j.

Es bleibt die Gleichheit der Spannräume. Nach Definition von v_{k+1} ist
$$v_{k+1} \in \operatorname{Span}(n_1, \dots, n_k, w).$$
Also gilt
$$\operatorname{Span}(n_1, \dots, n_k, v_{k+1}) \subseteq \operatorname{Span}(n_1, \dots, n_k, w).$$
Umgekehrt folgt aus der Definition
$$w = v_{k+1} + \sum_{i=1}^{k} \langle w, n_i \rangle n_i.$$
Also liegt w in $\operatorname{Span}(n_1, \dots, n_k, v_{k+1})$. Damit gilt auch die umgekehrte Inklusion.

Da $v_{k+1} \neq 0$, können wir normieren. Der normierte Vektor n_{k+1} hat Norm 1 und ist weiterhin orthogonal zu allen $n_1, \dots, n_k$. Damit ist $(n_1, \dots, n_k, n_{k+1})$ orthonormal. □

Theorem 9.3.9 (Gram-Schmidt-Orthonormalisierung)**.** *Sei V ein endlich-dimensionaler euklidischer oder unitärer Vektorraum. Sei $(b_1, \dots, b_n)$ eine Basis von V. Dann gibt es eine Orthonormalbasis $(n_1, \dots, n_n)$ von V mit*
$$\operatorname{Span}(n_1, \dots, n_k) = \operatorname{Span}(b_1, \dots, b_k)$$
für alle $k \in \{1, \dots, n\}$.

Beweis. Wir konstruieren die Vektoren $n_1, \dots, n_n$ iterativ.

Für $k = 1$ setzen wir

$$n_1 := \frac{1}{\|b_1\|} b_1.$$

Das ist möglich, weil $b_1 \neq 0$ ist. Dann ist (n_1) orthonormal und

$$\operatorname{Span}(n_1) = \operatorname{Span}(b_1).$$

Angenommen, wir haben bereits ein orthonormales System $(n_1, \dots, n_k)$ konstruiert mit

$$\operatorname{Span}(n_1, \dots, n_k) = \operatorname{Span}(b_1, \dots, b_k).$$

Da $(b_1, \dots, b_n)$ linear unabhängig ist, gilt

$$b_{k+1} \notin \operatorname{Span}(b_1, \dots, b_k).$$

Wegen der Gleichheit der Spannräume gilt also auch

$$b_{k+1} \notin \operatorname{Span}(n_1, \dots, n_k).$$

Wir wenden das vorherige Lemma mit $w = b_{k+1}$ an. Dann erhalten wir einen Vektor

$$v_{k+1} = b_{k+1} - \sum_{i=1}^{k} \langle b_{k+1}, n_i \rangle n_i,$$

der nicht Null ist und auf allen bisherigen n_i orthogonal steht. Wir setzen

$$n_{k+1} := \frac{1}{\|v_{k+1}\|} v_{k+1}.$$

Dann ist $(n_1, \dots, n_k, n_{k+1})$ orthonormal. Außerdem bleibt der Spann erhalten:

$$\operatorname{Span}(n_1, \dots, n_k, n_{k+1}) = \operatorname{Span}(n_1, \dots, n_k, b_{k+1}) = \operatorname{Span}(b_1, \dots, b_k, b_{k+1}).$$

Nach endlich vielen Schritten erhalten wir ein orthonormales System $(n_1, \dots, n_n)$ mit

$$\operatorname{Span}(n_1, \dots, n_n) = \operatorname{Span}(b_1, \dots, b_n) = V.$$

Also ist $(n_1, \dots, n_n)$ ein Erzeugendensystem von V. Da orthonormale Systeme insbesondere linear unabhängig sind, ist es eine Basis. □

Definition 9.3.10 (Orthonormalbasis)**.** Eine *Orthonormalbasis*, kurz *ONB*, ist eine Basis, die zugleich ein orthonormales System ist.

Leitbeispiel 9.3.11 (Der Trägheitstensor: die Hauptachsen sind eine ONB)**.** Für den Körper Leitbeispiel 9.1.14 wird der Spektralsatz später eine besondere Basis des $\mathbb{R}^3$ liefern: die *Hauptachsen* des Körpers. Ihre entscheidende Eigenschaft ist, dass sie eine Orthonormalbasis bilden. Das ist physikalisch kein Zufall, sondern eine Aussage über den Körper selbst: Es gibt drei zueinander *senkrechte* Drehachsen, um die er sich „sauber" dreht. Wichtig ist dabei, *welches* Skalarprodukt gemeint ist — es laufen ja inzwischen zwei durch dieses Kapitel. *Orthonormal* heißt hier: bezüglich des gewöhnlichen *Standard*skalarprodukts des $\mathbb{R}^3$, *nicht* bezüglich des maßgeschneiderten $\langle \cdot, \cdot \rangle_I$! (Bezüglich $\langle \cdot, \cdot \rangle_I$ sind die Hauptachsen zwar orthogonal, aber nicht normiert.) Dass ausgerechnet die Standard-Geometrie die Achsen der I-Energieform liefert, ist die eigentliche Pointe des Spektralsatzes; das Nebeneinander der beiden Skalarprodukte klären wir am Ende des Kapitels.

Drückt man eine beliebige Winkelgeschwindigkeit ω in einer solchen ONB (s_1, s_2, s_3) aus, so sind die Koordinaten einfach die Standardskalarprodukte mit den Achsen:

$$\omega = \langle \omega, s_1 \rangle s_1 + \langle \omega, s_2 \rangle s_2 + \langle \omega, s_3 \rangle s_3.$$

Genau dafür sind Orthonormalbasen gemacht. Dass sich eine ONB notfalls aus jeder Basis herstellen lässt, klärt das Gram-Schmidt-Verfahren; dass die Hauptachsen von selbst orthonormal sind, ist der Inhalt des Spektralsatzes.

Korollar 9.3.12 (Fortsetzung zu einer ONB)**.** *Sei V ein endlich-dimensionaler euklidischer oder unitärer Vektorraum. Dann lässt sich jedes orthonormale System in V zu einer ONB von V fortsetzen.*

Beweis. Sei $(n_1, \dots, n_k)$ ein orthonormales System in V. Nach dem Lemma über orthogonale Systeme ist dieses System linear unabhängig. Daher lässt es sich zu einer Basis

$$(n_1, \dots, n_k, b_{k+1}, \dots, b_n)$$

von V ergänzen. Nun wenden wir das Gram-Schmidt-Verfahren auf diese Basis an. Die ersten k Vektoren bleiben dabei unverändert, denn sie sind bereits orthonormal. So erhalten wir eine ONB von V, die das ursprüngliche orthonormale System enthält. □

Definition 9.3.13 (Orthogonales Komplement einer Menge)**.** Sei V ein euklidischer oder unitärer Vektorraum, und sei $M \subseteq V$ eine Teilmenge. Das *orthogonale Komplement* von M ist

$$M^\perp := \{v \in V \mid \text{für alle } m \in M \text{ gilt } v \perp m\}.$$

Lemma 9.3.14. *Für jede Teilmenge $M \subseteq V$ ist $M^\perp$ ein Untervektorraum von V.*

Beweis. Zunächst gilt $0 \in M^\perp$, denn $\langle 0, m \rangle = 0$ für alle $m \in M$.
Seien nun $v, w \in M^\perp$, und seien λ, μ Skalare. Für jedes $m \in M$ gilt

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

Also liegt auch $\lambda v + \mu w$ in $M^\perp$. Damit ist $M^\perp$ ein Untervektorraum. □

Definition 9.3.15 (Orthogonales Komplement eines Untervektorraums)**.** Ist $U \subseteq V$ ein Untervektorraum, dann nennen wir $U^\perp$ das *orthogonale Komplement* von U. Explizit ist also

$$U^\perp = \{v \in V \mid \text{für alle } u \in U \text{ gilt } v \perp u\}.$$

Theorem 9.3.16 (Orthogonale Zerlegung)**.** *Sei V ein endlich-dimensionaler euklidischer oder unitärer Vektorraum, und sei $U \subseteq V$ ein Untervektorraum. Dann gilt*

$$V = U \oplus U^\perp.$$

Insbesondere ist $U^\perp$ ein Komplement von U.

Beweis. Wir wählen eine ONB $(n_1, \dots, n_k)$ von U. Das ist möglich, weil wir zunächst irgendeine Basis von U wählen und dann Gram-Schmidt anwenden können.
Sei nun $v \in V$. Wir setzen

$$u := \sum_{i=1}^{k} \langle v, n_i \rangle n_i \in U$$

(das ist die orthogonale Projektion von v auf U) und

$$w := v - u.$$

Wir zeigen, dass $w \in U^\perp$ gilt. Für jedes $j \in \{1, \dots, k\}$ ist

$$\langle w, n_j \rangle = \langle v, n_j \rangle - \sum_{i=1}^{k} \langle v, n_i \rangle \langle n_i, n_j \rangle = 0.$$

Also steht w orthogonal auf allen n_j. Da die n_j den Untervektorraum U erzeugen, steht w sogar orthogonal auf ganz U. Also gilt $w \in U^\perp$.

Damit haben wir

$$v = u + w$$

mit $u \in U$ und $w \in U^\perp$. Also ist

$$V = U + U^\perp.$$

Es bleibt zu zeigen, dass die Summe direkt ist. Sei dazu $x \in U \cap U^\perp$. Dann ist $x \in U$, aber zugleich steht x orthogonal auf ganz U. Insbesondere gilt also $x \perp x$, also

$$\langle x, x \rangle = 0.$$

Nach positiver Definitheit folgt $x = 0$. Damit ist $U \cap U^\perp = \{0\}$, und die Summe ist direkt. □

Korollar 9.3.17 (Eindeutigkeit des orthogonalen Komplements)**.** *Sei $U \subseteq V$ ein Untervektorraum. Dann ist $U^\perp$ das eindeutig bestimmte Komplement von U, das orthogonal zu U steht. Genauer: Ist $W \subseteq V$ ein Untervektorraum mit*

$$V = U \oplus W$$

und gilt $W \subseteq U^\perp$, dann ist

$$W = U^\perp.$$

Beweis. Aus $W \subseteq U^\perp$ folgt bereits eine Inklusion. Da $V = U \oplus W$ gilt, ist

$$\dim(W) = \dim(V) - \dim(U).$$

Aus dem vorherigen Satz gilt außerdem $V = U \oplus U^\perp$, also

$$\dim(U^\perp) = \dim(V) - \dim(U).$$

Damit haben W und $U^\perp$ dieselbe Dimension. Zusammen mit $W \subseteq U^\perp$ folgt $W = U^\perp$. □

9.4 Polarisierung und Ungleichungen

Wir arbeiten weiterhin in einem euklidischen oder unitären Vektorraum. Im unitären Fall verwenden wir die Konvention, dass das Skalarprodukt im ersten Argument linear und im zweiten Argument antilinear ist.

Theorem 9.4.1 (Polarisierung, Pythagoras und die wichtigsten Ungleichungen)**.** *Sei V ein euklidischer oder unitärer Vektorraum. Dann gelten die folgenden Aussagen.*

1. ***Polarisierung im reellen Fall.*** *Ist V euklidisch, dann gilt für alle $v, w \in V$*

$$\langle v, w\rangle = \frac{1}{2}\left(\|v+w\|^2 - \|v\|^2 - \|w\|^2\right).$$

Äquivalent dazu sind die Formen

$$\langle v, w\rangle = \frac{1}{4}\left(\|v+w\|^2 - \|v-w\|^2\right)$$

und

$$\langle v, w\rangle = \frac{1}{2}\left(\|v\|^2 + \|w\|^2 - \|v-w\|^2\right).$$

2. ***Polarisierung im unitären Fall.*** *Ist V unitär, dann gilt für alle $v, w \in V$*

$$\langle v, w\rangle = \frac{1}{4}\left(\|v+w\|^2 - \|v-w\|^2\right) + \frac{i}{4}\left(\|v+iw\|^2 - \|v-iw\|^2\right).$$

3. ***Satz des Pythagoras.*** *Sind $v, w \in V$ orthogonal, dann gilt*

$$\|v+w\|^2 = \|v\|^2 + \|w\|^2.$$

4. ***Cauchy-Schwarz-Ungleichung.*** *Für alle $v, w \in V$ gilt*

$$|\langle v, w\rangle| \leq \|v\|\,\|w\|.$$

5. ***Dreiecksungleichung.*** *Für alle $v, w \in V$ gilt*

$$\|v+w\| \leq \|v\| + \|w\|.$$

Beweis. Wir beginnen mit der Polarisierung. Im reellen Fall gilt

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

Umstellen ergibt sofort

$$\langle v, w\rangle = \frac{1}{2}\left(\|v+w\|^2 - \|v\|^2 - \|w\|^2\right).$$

Wenn man stattdessen $v - w$ verwendet, erhält man

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

Daraus folgt durch Umstellen auch

$$\langle v, w\rangle = \frac{1}{2}\left(\|v\|^2 + \|w\|^2 - \|v-w\|^2\right).$$

Subtrahiert man die beiden Gleichungen für $\|v+w\|^2$ und $\|v-w\|^2$, erhält man außerdem

$$\|v+w\|^2 - \|v-w\|^2 = 4\langle v, w\rangle.$$

Also gilt auch

$$\langle v, w\rangle = \frac{1}{4}\left(\|v+w\|^2 - \|v-w\|^2\right).$$

Im unitären Fall müssen wir Realteil und Imaginärteil des Skalarprodukts getrennt rekonstruieren. Sei dazu

$$z := \langle v, w \rangle.$$

Unser Ziel ist es, aus Normen zunächst $\mathrm{Re}(z)$ und dann $\mathrm{Im}(z)$ zu bestimmen.

Zuerst bestimmen wir den Realteil. Dazu berechnen wir

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

Mit Sesquilinearität erhalten wir

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

Da $\langle w, v \rangle = \overline{\langle v, w \rangle}$ gilt, ist das

$$\|v + w\|^2 = \|v\|^2 + \|w\|^2 + z + \bar{z} = \|v\|^2 + \|w\|^2 + 2\,\mathrm{Re}(z).$$

Genauso erhält man

$$\|v - w\|^2 = \|v\|^2 + \|w\|^2 - 2\,\mathrm{Re}(z).$$

Wenn wir diese beiden Gleichungen voneinander abziehen, fallen die Terme $\|v\|^2$ und $\|w\|^2$ weg. Es bleibt

$$\|v + w\|^2 - \|v - w\|^2 = 4\,\mathrm{Re}(z).$$

Also gilt

$$\mathrm{Re}\langle v, w \rangle = \frac{1}{4} \left(\|v + w\|^2 - \|v - w\|^2 \right).$$

Nun bestimmen wir den Imaginärteil. Die Idee ist, w durch iw zu ersetzen. Wir berechnen also dieselbe Differenz wie oben, aber mit iw statt w. Nach dem bereits bewiesenen Realteil gilt

$$\|v + iw\|^2 - \|v - iw\|^2 = 4\,\mathrm{Re}\langle v, iw \rangle.$$

Da das Skalarprodukt im zweiten Argument antilinear ist, gilt

$$\langle v, iw \rangle = \bar{i} \langle v, w \rangle = -iz.$$

Für $z = a + ib$ ist

$$-iz = -i(a + ib) = b - ia.$$

Also ist

$$\mathrm{Re}(-iz) = b = \mathrm{Im}(z).$$

Damit erhalten wir

$$\|v + iw\|^2 - \|v - iw\|^2 = 4\,\mathrm{Im}(z).$$

Also gilt

$$\mathrm{Im}\langle v, w \rangle = \frac{1}{4} \left(\|v + iw\|^2 - \|v - iw\|^2 \right).$$

Zusammen folgt

$$\langle v, w \rangle = \mathrm{Re}\langle v, w \rangle + i\,\mathrm{Im}\langle v, w \rangle.$$

Einsetzen der beiden Formeln liefert die unitäre Polarisierungsformel

$$\langle v, w \rangle = \frac{1}{4} \left(\|v + w\|^2 - \|v - w\|^2 \right) + \frac{i}{4} \left(\|v + iw\|^2 - \|v - iw\|^2 \right).$$

Nun folgt Pythagoras. Sind v und w orthogonal, also $\langle v, w\rangle = 0$. Wegen (hermitescher) Symmetrie gilt dann auch $\langle w, v\rangle = 0$. Also ist

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

Wir beweisen nun die Cauchy-Schwarz-Ungleichung. Für $w = 0$ ist die Aussage klar. Sei also $w \neq 0$. Wir zerlegen v in einen Anteil in Richtung von w und einen Anteil orthogonal zu w. Setze

$$u := v - \frac{\langle v, w\rangle}{\langle w, w\rangle} w.$$

Dann gilt

$$\langle u, w\rangle = \langle v, w\rangle - \frac{\langle v, w\rangle}{\langle w, w\rangle}\langle w, w\rangle = 0.$$

Der Vektor u ist also der orthogonale Rest von v nach Abzug des Anteils in Richtung w. Nach Pythagoras gilt daher

$$\|v\|^2 = \|u\|^2 + \left\| \frac{\langle v, w\rangle}{\langle w, w\rangle} w \right\|^2 .$$

Da $\|u\|^2 \geq 0$ ist, folgt

$$\|v\|^2 \geq \left\| \frac{\langle v, w\rangle}{\langle w, w\rangle} w \right\|^2 = \frac{|\langle v, w\rangle|^2}{\|w\|^2}.$$

Multiplikation mit $\|w\|^2$ ergibt

$$|\langle v, w\rangle|^2 \leq \|v\|^2 \|w\|^2 .$$

Nach Wurzelziehen erhalten wir die Cauchy-Schwarz-Ungleichung.

Zum Schluss beweisen wir die Dreiecksungleichung. Es gilt

$$\|v + w\|^2 = \|v\|^2 + 2\,\mathrm{Re}\langle v, w\rangle + \|w\|^2 .$$

Mit

$$\mathrm{Re}\langle v, w\rangle \leq |\langle v, w\rangle| \leq \|v\|\,\|w\|$$

folgt

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

Da Normen nichtnegativ sind, folgt daraus

$$\|v + w\| \leq \|v\| + \|w\| . \qquad \square$$

Korollar 9.4.2 (Die Norm bestimmt das Skalarprodukt)**.** *Sei V ein euklidischer oder unitärer Vektorraum. Dann ist das Skalarprodukt auf V durch die induzierte Norm eindeutig bestimmt. Genauer: Sind $\langle -, -\rangle_1$ und $\langle -, -\rangle_2$ zwei Skalarprodukte auf V, und gilt für alle $v \in V$*

$$\sqrt{\langle v, v\rangle_1} = \sqrt{\langle v, v\rangle_2},$$

dann gilt bereits

$$\langle v, w\rangle_1 = \langle v, w\rangle_2$$

für alle $v, w \in V$.

Beweis. Die Polarisierungsformel rekonstruiert $\langle v, w\rangle$ ausschließlich aus Normen. Im euklidischen Fall genügt zum Beispiel die Formel

$$\langle v, w\rangle = \frac{1}{2}\left(\|v+w\|^2 - \|v\|^2 - \|w\|^2\right).$$

Im unitären Fall verwendet man die unitäre Polarisierungsformel. Wenn zwei Skalarprodukte dieselbe Norm induzieren, haben alle Normausdrücke in diesen Formeln denselben Wert. Also stimmen die Skalarprodukte überein. □

Korollar 9.4.3 (Abstände bestimmen Winkel)**.** *Seien V und W euklidische Vektorräume. Sei*

$$F : V \to W$$

eine Abbildung, die alle Abstände erhält. Das heißt: Für alle $x, y \in V$ gilt

$$\|F(x) - F(y)\| = \|x - y\|.$$

Dann erhält F alle Winkel. Genauer: Für alle $x \in V$ und alle $v, w \in V$ gilt

$$\langle F(x+v) - F(x), F(x+w) - F(x)\rangle = \langle v, w\rangle.$$

Bemerkung 9.4.4. Im unitären Fall stimmt die obige Aussage nicht. Sogar in $\mathbb{C}^1$ ist die komplexe Konjugation ein Gegenbeispiel. Sie erhält offensichtlich alle Längen im Standardskalarprodukt, aber nicht das Skalarprodukt selber: Sei $b > 0$ beliebig, dann gilt

$$\langle bi, 1\rangle = bi \neq -bi = \langle -bi, 1\rangle = \langle \overline{bi}, \overline{1}\rangle.$$

Hier muss also auch die komplexe Struktur erhalten werden, damit man die unitäre Polarisierungsformel anwenden kann.

Beweis. Setze

$$a := F(x+v) - F(x) \quad \text{und} \quad b := F(x+w) - F(x).$$

Dann gilt wegen Abstandserhaltung

$$\|a\| = \|v\|, \qquad \|b\| = \|w\|, \qquad \|a - b\| = \|v - w\|.$$

Mit der Polarisierungsformel in der Form

$$\langle r, s\rangle = \frac{1}{2}\left(\|r\|^2 + \|s\|^2 - \|r - s\|^2\right)$$

folgt daher

$$\langle a, b\rangle = \frac{1}{2}\left(\|v\|^2 + \|w\|^2 - \|v - w\|^2\right) = \langle v, w\rangle.$$

Damit sind die Skalarprodukte und daher auch die Winkel erhalten. □

Bemerkung 9.4.5 (Braucht man Linearität?)**.** Für die Winkelerhaltung im vorherigen Korollar braucht man Linearität nicht vorauszusetzen. Die Aussage folgt direkt aus der Abstandserhaltung und der Polarisierungsformel.

In euklidischen Vektorräumen bekommt man Linearität sogar fast geschenkt: Eine abstandserhaltende Abbildung ist affin. Genauer: Ist $F(0) = 0$, dann ist F linear. Im allgemeinen Fall ist

$$G(v) := F(v) - F(0)$$

linear, und also ist F eine lineare Abbildung plus eine Verschiebung.

Für unitäre Vektorräume ist wieder etwas Vorsicht nötig. Wie oben erläutert gilt: die gewöhnliche Abstandsfunktion sieht zunächst nur die zugrundeliegende reelle Geometrie.

Wieder ist Komplexe Konjugation ein gutes Gegenbeispiel. Sie ist abstandserhaltend, aber nicht komplex-linear. Erhält eine Abbildung zusätzlich die komplexe Struktur, also insbesondere Multiplikation mit i, dann rekonstruiert die unitäre Polarisierungsformel auch das komplexe Skalarprodukt.

Begründung der Linearitätsaussage im Euklidischen Fall. Wir betrachten den Fall $F(0) = 0$. Nach dem vorherigen Korollar gilt dann

$$\langle F(v), F(w)\rangle = \langle v, w\rangle$$

für alle $v, w \in V$. Damit folgt für alle $v, w \in V$

$$\begin{aligned}
&\|F(v+w) - F(v) - F(w)\|^2 \\
=&\langle F(v+w) - F(v) - F(w), F(v+w) - F(v) - F(w)\rangle \\
=&\langle F(v+w), F(v+w) - F(v) - F(w)\rangle \\
&+ \langle F(v), F(v+w) - F(v) - F(w)\rangle \\
&+ \langle F(w), F(v+w) - F(v) - F(w)\rangle \\
=&\langle F(v+w), F(v+w)\rangle + \langle F(v), F(v+w)\rangle + \langle F(w), F(v+w)\rangle \\
&+ \langle F(v+w), F(v)\rangle + \langle F(v), F(v)\rangle + \langle F(w), F(v)\rangle \\
&+ \langle F(v+w), F(w)\rangle + \langle F(v), F(w)\rangle + \langle F(w), F(w)\rangle \\
=&\langle v+w, v+w\rangle + \langle v, v+w\rangle + \langle w, v+w\rangle \\
&+ \langle v+w, v\rangle + \langle v, v\rangle + \langle w, v\rangle \\
&+ \langle v+w, w\rangle + \langle v, w\rangle + \langle w, w\rangle \\
=&\langle v+w-v-w, v+w-v-w\rangle \\
=&\|v+w-v-w\|^2 \\
=&0\,.
\end{aligned}$$

Die Idee ist: Man kann alle Skalarprodukte vollständig ausmultiplizieren, bis nur Terme der Form $\langle F(a), F(b)\rangle$ auftauchen. Dann benutzt man dass $\langle F(a), F(b)\rangle = \langle a, b\rangle$. Schließlich geht man das ausmultiplizieren wieder zurück. So sieht man dann konzeptionell, dass

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

gelten muss. Mit einem analogen Argument sieht man dass

$$\|F(\lambda v) - \lambda F(v)\|^2 = \|\lambda v - \lambda v\|^2$$

für alle $\lambda \in \mathbb{R}$.

Also gilt

$$F(v+w) = F(v) + F(w) \qquad \text{und} \qquad F(\lambda v) = \lambda F(v).$$

Damit ist F linear. Für allgemeines F wendet man dies auf $G(v) = F(v) - F(0)$ an. □

Bemerkung 9.4.6 (Abstandserhaltung vs. Normerhaltung)**.** Für Korollar 9.4.3 brauchen wir, dass *Abstände* erhalten werden. Das heißt, dass für alle $v, w \in V$ wir haben

$$\|F(v) - F(w)\| = \|v - w\|\ .$$

Bemerke, dass dies etwas anderes ist, als *Normerhaltung*, also

$$\|F(v)\| = \|v\| \ .$$

Ein einfaches Gegenbeispiel ist, die folgende Abbildung

$$P_w : V \to V, \ v \longmapsto \|v\| \cdot w$$

für ein beliebiges $w \in V$ mit $\|w\| = 1$. Diese Abbildung erhält Längen, aber keine Abstände.

Aber falls eine *lineare Abbildung* normerhaltend ist, dann ist sie bereits abstandserhaltend, denn

$$\|F(v) - F(w)\| = \|F(v - w)\| = \|v - w\| \ .$$

Ohne Linearität scheitert die erste Gleichheit im Allgemeinen. Für Korollar 9.4.3 ist also Linearität nicht notwendig, aber mit Linearität bekommen wir die folgende Verschärfung:

Korollar 9.4.7. *Eine normerhaltende lineare Abbildung erhält das Skalarprodukt.*

Bemerkung 9.4.8 (Was diese Ungleichungen leisten)**.** Die Cauchy-Schwarz-Ungleichung ist eine der wichtigsten Schätzungen der linearen Algebra. Sie sagt, dass ein Skalarprodukt nicht beliebig groß werden kann: Es ist höchstens das Produkt der Längen. Das macht aus dem Skalarprodukt einen kontrollierten Winkel- und Projektionsbegriff.

Die Dreiecksungleichung sagt, dass die durch das Skalarprodukt induzierte Norm wirklich ein sinnvoller Längenbegriff ist. Der direkte Weg von 0 nach $v + w$ ist nicht länger als der Weg zuerst nach v und dann weiter nach $v + w$.

In der Physik treten diese Aussagen ständig auf. In der Quantenmechanik sind Zustände Vektoren in einem komplexen Skalarproduktraum, und $|\langle\psi, \varphi\rangle|^2$ misst die Überlappung zweier Zustände. Cauchy-Schwarz garantiert, dass diese Überlappung durch die Normen der Zustände beschränkt ist. Bei normierten Zuständen ist sie also höchstens 1.

Auch in der klassischen Mechanik und in der Elektrodynamik sind solche Abschätzungen grundlegend. Wenn ein Skalarprodukt Arbeit, Energie oder eine Projektion beschreibt, dann liefert Cauchy-Schwarz sofort eine obere Schranke: Eine Kraft kann in einer gegebenen Verschiebung höchstens so viel Arbeit leisten, wie es das Produkt aus Kraftstärke und Weglänge erlaubt. Die Dreiecksungleichung ist die abstrakte Form der vertrauten Tatsache, dass zusammengesetzte Wege nicht kürzer sein müssen als die direkte Verbindung.

9.5 Matrixgruppen

Wir betrachten nun einige wichtige Gruppen von Matrizen. Sie beschreiben lineare Abbildungen mit bestimmten geometrischen Eigenschaften. Die Gruppenoperation ist jeweils die Matrizenmultiplikation.

Definition 9.5.1 (Allgemeine lineare Gruppe)**.** Die *allgemeine lineare Gruppe* ist

$$\mathrm{GL}(n, \mathbb{R}) := \{A \in M_n(\mathbb{R}) \mid A \text{ ist invertierbar}\} .$$

Bemerkung 9.5.2 (Geometrische Interpretation von $\mathrm{GL}(n, \mathbb{R})$)**.** Eine Matrix $A \in \mathrm{GL}(n, \mathbb{R})$ beschreibt einen linearen Isomorphismus

$$\mathbb{R}^n \to \mathbb{R}^n, \quad v \mapsto Av.$$

Geometrisch sind das die invertierbaren linearen Verzerrungen des Raumes. Sie dürfen Längen, Winkel und Volumina verändern, aber sie dürfen keine Information verlieren. Die Rechtfertigung ist direkt: Invertierbarkeit bedeutet genau, dass es eine inverse Matrix A^{-1} gibt, also eine lineare Rückabbildung. Matrizenmultiplikation entspricht der Verkettung linearer Abbildungen.

Definition 9.5.3 (Orthogonale Gruppe)**.** Die *orthogonale Gruppe* ist

$$O(n) := \left\{ A \in \mathrm{GL}(n, \mathbb{R}) \;\middle|\; A^\top A = 1_n \right\}.$$

Lemma 9.5.4 (Charakterisierung orthogonaler Matrizen)**.** *Für eine Matrix $A \in M_n(\mathbb{R})$ sind äquivalent:*

1. $A \in O(n)$.
2. *Für alle $v, w \in \mathbb{R}^n$ gilt*
$$\langle Av, Aw \rangle = \langle v, w \rangle.$$
3. *Für alle $v \in \mathbb{R}^n$ gilt*
$$\|Av\| = \|v\|.$$
4. *Für alle $v, w \in \mathbb{R}^n$ gilt*
$$\|Av - Aw\| = \|v - w\|.$$

Beweis. Wir verwenden das Standardskalarprodukt

$$\langle v, w \rangle = w^\top v.$$

Dann gilt

$$\langle Av, Aw \rangle = (Aw)^\top Av = w^\top A^\top Av.$$

Also gilt $A^\top A = 1_n$ genau dann, wenn $\langle Av, Aw \rangle = \langle v, w \rangle$ für alle v, w gilt. Damit sind die ersten beiden Aussagen äquivalent.

Die zweite Aussage impliziert sofort die dritte. Aus der dritten Aussage folgt die zweite durch Polarisierung, denn das Skalarprodukt ist durch die Norm bestimmt. Da A linear ist, gilt

$$Av - Aw = A(v - w).$$

Damit sind die dritte und vierte Aussage äquivalent. □

Bemerkung 9.5.5 (Geometrische Interpretation von $O(n)$)**.** Die Gruppe $O(n)$ besteht aus den linearen Abbildungen des $\mathbb{R}^n$, die alle Längen und Abstände erhalten. Wegen der Polarisierung erhalten sie dann automatisch auch alle Skalarprodukte und damit alle Winkel.

Das rechtfertigt die geometrische Interpretation: Elemente von $O(n)$ sind die linearen starren Bewegungen des Raumes, die den Ursprung festhalten. Sie können rotieren, spiegeln oder beides kombinieren. Sie können aber nicht strecken, stauchen oder scheren.

Bemerkung 9.5.6 (Orthogonalität, Skalarprodukt und $O(n)$)**.** Seien $A, B \in M_n(\mathbb{R})$ Matrizen und seien mit a_i und b_j die Spalten bezeichnet. Sei zudem $\langle v, w \rangle$ das Standardskalarprodukt. Dann ist

$$A^\top B = \begin{pmatrix} \langle a_1, b_1 \rangle & \dots & \langle a_1, b_n \rangle \\ \vdots & & \vdots \\ \langle a_n, b_1 \rangle & \dots & \langle a_n, b_n \rangle \end{pmatrix}$$

Eine Matrix ist also genau dann orthogonal, wenn die Spalten ein orthonormales System bilden. Da die Matrix quadratisch ist, erhalten wir sofort, dass die Spalten sogar eine ONB sind. Die Spalten einer Matrix sind die Bilder der Einheitsvektoren. Eine lineare Abbildung ist also genau dann orthogonal, wenn sie eine ONB auf eine andere ONB schickt.

Korollar 9.5.7 (Rotationen und Spiegelungen sind orthogonal)**.** *Sei $F : \mathbb{R}^n \to \mathbb{R}^n$ eine lineare Abbildung, die alle Abstände erhält. Dann liegt die Matrix von F bezüglich der Standardbasis in $O(n)$.*

Beweis. Da F linear ist, gilt $F(0) = 0$. Nach dem Korollar über abstandserhaltende Abbildungen erhält F das Standardskalarprodukt. Nach dem vorherigen Lemma ist die Matrix von F daher orthogonal. □

Definition 9.5.8 (Spezielle orthogonale Gruppe)**.** Die *spezielle orthogonale Gruppe* ist

$$SO(n) := \{A \in O(n) \mid \det(A) = 1\}.$$

Bemerkung 9.5.9 (Geometrische Interpretation von $SO(n)$)**.** Die Gruppe $SO(n)$ besteht aus den orthogonalen Matrizen, die zusätzlich die Orientierung erhalten. Für $A \in O(n)$ gilt nämlich

$$1 = \det(1_n) = \det(A^\top A) = \det(A)^2.$$

Also ist $\det(A) = 1$ oder $\det(A) = -1$. Der Wert 1 bedeutet: Orientierung wird erhalten. Der Wert -1 bedeutet: Orientierung wird umgekehrt.

Geometrisch ist $SO(n)$ daher der orientierungserhaltende Teil von $O(n)$. In der Ebene ist $SO(2)$ genau die Gruppe der Drehungen um den Ursprung. In Dimension 3 beschreibt $SO(3)$ die üblichen Rotationen des Raumes um Achsen durch den Ursprung.

Leitbeispiel 9.5.10 (Der Trägheitstensor: Drehen des Körpers)**.** Die orthogonale Gruppe ist im Körper Leitbeispiel 9.1.14 unmittelbar greifbar. Wir drehen das *Koordinatensystem* mit einer Rotation $R \in SO(3)$; der Körper bleibt, wo er ist. In den neuen Koordinaten wird der Trägheitstensor zu

$$I' = R^\top I R.$$

Das ist die Basiswechselformel für Bilinearformen — hier als Vorgriff benutzt, sie kommt im nächsten Abschnitt. (Den Körper selbst zu drehen statt der Koordinaten läuft auf dieselbe Formel mit R^{-1} hinaus.) Weil R orthogonal ist, gilt $R^\top = R^{-1}$, und dieser Basiswechsel fällt für die *Form* I und für den *Operator* I zusammen — ein Punkt, auf den wir bei der Hauptachsentransformation zurückkommen. Rotationen erhalten dabei Längen und Winkel: Die geometrische Lage des Körpers ändert sich nicht, nur ihre Beschreibung. Genau deshalb darf man in ein besonders bequemes Koordinatensystem drehen. Die einzige Frage ist, welches das beste ist — und die Antwort geben die Hauptachsen.

Definition 9.5.11 (Unitäre Gruppe)**.** Die *unitäre Gruppe* ist

$$U(n) := \left\{A \in \mathrm{GL}(n, \mathbb{C}) \;\middle|\; A^H A = 1_n\right\}.$$

Dabei bezeichnet

$$A^H := \overline{A}^\top$$

die hermitesch transponierte Matrix.

Lemma 9.5.12 (Charakterisierung unitärer Matrizen)**.** *Für eine Matrix $A \in M_n(\mathbb{C})$ sind äquivalent:*

1. *$A \in U(n)$.*
2. *Für alle $v, w \in \mathbb{C}^n$ gilt*
$$\langle Av, Aw\rangle = \langle v, w\rangle.$$

3. *Für alle $v \in \mathbb{C}^n$ gilt*

$$\|Av\| = \|v\|.$$

4. *Die Spalten von A bilden eine Orthonormalbasis von $\mathbb{C}^n$ bezüglich des Standardskalarprodukts.*

Beweis. Wir verwenden das unitäre Standardskalarprodukt

$$\langle v, w \rangle = w^H v.$$

Dann gilt

$$\langle Av, Aw \rangle = (Aw)^H Av = w^H A^H Av.$$

Also gilt $A^H A = 1_n$ genau dann, wenn $\langle Av, Aw \rangle = \langle v, w \rangle$ für alle v, w gilt. Damit sind die ersten beiden Aussagen äquivalent.

Die zweite Aussage impliziert sofort die dritte. Aus der dritten Aussage folgt die zweite durch die unitäre Polarisierungsformel, denn das Skalarprodukt ist durch die Norm bestimmt.

Seien nun $a_1, \dots, a_n$ die Spalten von A. Dann gilt

$$\left(A^H A\right)_{ij} = a_i^H a_j = \langle a_j, a_i \rangle.$$

Daher gilt $A^H A = 1_n$ genau dann, wenn

$$\langle a_j, a_i \rangle = \delta_{ij}$$

für alle i, j gilt. Das bedeutet genau, dass die Spalten von A eine Orthonormalbasis von $\mathbb{C}^n$ bilden. □

Bemerkung 9.5.13 (Geometrische Interpretation von $U(n)$)**.** Die Gruppe $U(n)$ ist das komplexe Analogon von $O(n)$. Ihre Elemente erhalten das unitäre Standardskalarprodukt und damit Normen, Abstände und Winkel. Man sollte aber nicht einfach $A^\top A = 1_n$ fordern. Im komplexen Fall ist die richtige Bedingung

$$A^H A = 1_n.$$

Das ist genau die Bedingung, dass komplexe Längen und Orthogonalität mit der Konjugation richtig behandelt werden.

Definition 9.5.14 (Spezielle unitäre Gruppe)**.** Die *spezielle unitäre Gruppe* ist

$$SU(n) := \{A \in U(n) \mid \det(A) = 1\}.$$

Bemerkung 9.5.15 (Geometrische Interpretation von $SU(n)$)**.** Für $A \in U(n)$ gilt

$$1 = \det(1_n) = \det(A^H A) = \det(A^H)\det(A) = \overline{\det(A)}\det(A) = |\det(A)|^2.$$

Also liegt $\det(A)$ auf dem komplexen Einheitskreis. Die Gruppe $SU(n)$ besteht aus den unitären Matrizen, deren Determinante genau 1 ist. Sie ist der komplexe Spezialfall, der später im Spektralsatz bei der Hauptachsentransformation natürlich auftaucht.

Lemma 9.5.16 (Gruppeneigenschaften)**.** *Die Mengen* $\mathrm{GL}(n, \mathbb{R})$, $\mathrm{GL}(n, \mathbb{C})$, $O(n)$, $SO(n)$, $U(n)$ *und* $SU(n)$ *sind Gruppen bezüglich Matrizenmultiplikation.*

Beweis. Für $\mathrm{GL}(n,\mathbb{R})$ und $\mathrm{GL}(n,\mathbb{C})$ ist das gerade die Aussage, dass Produkte invertierbarer Matrizen invertierbar sind und dass die inverse Matrix wieder invertierbar ist.

Sind $A, B \in O(n)$, dann gilt

$$(AB)^\top (AB) = B^\top A^\top AB = B^\top B = 1_n.$$

Also ist $AB \in O(n)$. Außerdem ist für $A \in O(n)$ die inverse Matrix durch $A^{-1} = A^\top$ gegeben, und $A^\top$ ist wieder orthogonal. Damit ist $O(n)$ eine Gruppe.

Für $SO(n)$ kommt nur noch die Determinantenbedingung dazu. Sind $A, B \in SO(n)$, dann ist

$$\det(AB) = \det(A)\det(B) = 1.$$

Außerdem gilt

$$\det(A^{-1}) = \det(A)^{-1} = 1.$$

Also ist auch $SO(n)$ eine Gruppe.

Der Beweis für $U(n)$ ist die hermitesche Version des Beweises für $O(n)$. Sind $A, B \in U(n)$, dann gilt

$$(AB)^H (AB) = B^H A^H AB = B^H B = 1_n.$$

Also ist $AB \in U(n)$. Außerdem ist für $A \in U(n)$ die inverse Matrix durch $A^{-1} = A^H$ gegeben, und A^H ist wieder unitär. Damit ist $U(n)$ eine Gruppe.

Für $SU(n)$ kommt wieder nur die Determinantenbedingung dazu. Sind $A, B \in SU(n)$, dann ist

$$\det(AB) = \det(A)\det(B) = 1.$$

Außerdem gilt

$$\det(A^{-1}) = \det(A)^{-1} = 1.$$

Also ist auch $SU(n)$ eine Gruppe. □

9.6 Das Hurwitz-Kriterium

Wir arbeiten in diesem Abschnitt vor allem im unitären Fall. Der euklidische Fall ist völlig analog. Das Hurwitz-Kriterium gibt uns ein rechenbares Kriterium dafür, wann eine hermitesche Matrix positiv definit ist.

9.6.1 Basiswechsel für Sesquilinearformen

Lemma 9.6.1 (Basiswechsel für Sesquilinearformen)**.** *Sei V ein endlich-dimensionaler $\mathbb{C}$-Vektorraum, und sei*

$$b : V \times V \to \mathbb{C}$$

eine Sesquilinearform. Seien

$$B = (u_1, \dots, u_n) \quad \textit{und} \quad C = (v_1, \dots, v_n)$$

zwei Basen von V. Sei A_B die Matrix von b bezüglich B, und sei A_C die Matrix von b bezüglich C. Setzen wir

$$P := M_{B \leftarrow C}(\mathrm{Id}),$$

also

$$[x]_B = P[x]_C$$

für alle $x \in V$, dann gilt

$$A_C = P^H A_B P.$$

Beweis. Nach Definition der Matrix einer Sesquilinearform bedeutet A_B: Für alle $v, w \in V$ gilt

$$b(v,w) = [w]_B^H A_B [v]_B .$$

Nun verwenden wir die Basiswechselmatrix

$$P = M_{B \leftarrow C}(\mathrm{Id}) .$$

Sie übersetzt Koordinaten bezüglich C in Koordinaten bezüglich B:

$$[v]_B = P[v]_C , \quad [w]_B = P[w]_C .$$

Also erhalten wir

$$\begin{aligned} b(v,w) &= [w]_B^H A_B [v]_B \\ &= (P[w]_C)^H A_B (P[v]_C) \\ &= [w]_C^H P^H A_B P [v]_C . \end{aligned}$$

Damit erfüllt $P^H A_B P$ die charakterisierende Eigenschaft der Matrix von b bezüglich C. Aus der Eindeutigkeit dieser Matrix folgt

$$A_C = P^H A_B P . \qquad \square$$

Bemerkung 9.6.2 (Anders als bei linearen Abbildungen)**.** Bei einem Endomorphismus, bei dem man im Definitions- und Zielraum dieselbe Basis wechselt, ändert sich die Matrix durch Konjugation mit einer inversen Matrix. Bei einer Sesquilinearform ändert sich die Matrix anders:

$$A_C = P^H A_B P .$$

Der Grund ist, dass die Form zwei Eingänge hat. Der Basiswechsel tritt daher einmal links und einmal rechts auf. Im linken Faktor entsteht wegen der Antilinearität im zweiten Argument die hermitesch transponierte Matrix.

Korollar 9.6.3 (Vorzeichen der Determinante unter Basiswechsel)**.** *Alle Matrixdarstellungen derselben hermiteschen Sesquilinearform haben Determinanten mit demselben Vorzeichen. Genauer gilt: Sind A_B und A_C die Matrizen derselben hermiteschen Sesquilinearform bezüglich zweier Basen, dann gibt es eine invertierbare Matrix P mit*

$$A_C = P^H A_B P$$

und deshalb

$$\det(A_C) = |\det(P)|^2 \det(A_B) .$$

Da $|\det(P)|^2 > 0$ gilt, haben $\det(A_B)$ und $\det(A_C)$ dasselbe Vorzeichen.

Im euklidischen Fall gilt analog: Sind A_B und A_C die Matrizen derselben symmetrischen Bilinearform, dann gilt

$$A_C = P^\top A_B P \quad \textit{und} \quad \det(A_C) = \det(P)^2 \det(A_B) .$$

Auch hier bleibt das Vorzeichen der Determinante erhalten.

Beweis. Wir beweisen den unitären Fall. Der euklidische Fall ist dieselbe Rechnung mit $P^\top$ statt P^H.

Nach dem Basiswechsel-Lemma gilt

$$A_C = P^H A_B P .$$

Mit der Produktregel für Determinanten folgt

$$\det(A_C) = \det\left(P^H\right) \det(A_B) \det(P)\,.$$

Nach dem vorherigen Korollar über A^H gilt

$$\det\left(P^H\right) = \overline{\det(P)}\,.$$

Also ist

$$\det(A_C) = \overline{\det(P)} \det(P) \det(A_B) = |\det(P)|^2 \det(A_B)\,.$$

Da P invertierbar ist, ist $\det(P) \neq 0$. Also ist

$$|\det(P)|^2 > 0\,.$$

Multiplikation mit einer positiven reellen Zahl ändert das Vorzeichen nicht. Damit ist die Behauptung bewiesen. □

9.6.2 Diagonale Matrizen

Lemma 9.6.4 (Diagonale Darstellung und positive Definitheit)**.** *Sei $b : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$ eine hermitesche Sesquilinearform. Angenommen, die Matrix von b bezüglich einer Basis B ist eine Diagonalmatrix D. Dann gilt:*

$$b \text{ ist positiv definit} \quad \Longleftrightarrow \quad D_{i,i} > 0 \text{ für alle } i \in \{1, \dots, n\}\,.$$

Beweis. Da b hermitesch ist, ist D hermitesch. Für eine Diagonalmatrix bedeutet das insbesondere, dass alle Diagonaleinträge $d_i := D_{i,i}$ reell sind.

Sei nun $v \in \mathbb{C}^n$, und sei

$$[v]_B = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}.$$

Dann gilt

$$b(v,v) = [v]_B^H D [v]_B = \sum_{i=1}^{n} d_i \,|\lambda_i|^2\,.$$

$\Longleftarrow$: Ist $v \neq 0$, dann ist mindestens ein $\lambda_i \neq 0$. Also ist mindestens ein Summand positiv, und alle anderen Summanden sind nichtnegativ. Somit gilt

$$b(v,v) > 0\,.$$

Also ist b positiv definit.

$\Longrightarrow$: Schreiben wir $B = (u_1, \dots, u_n)$. Dann gilt

$$d_i = b(u_i, u_i)\,.$$

Da $u_i \neq 0$ ist und b positiv definit ist, folgt $d_i > 0$.

Damit ist die Äquivalenz bewiesen. □

9.6.3 Das Hurwitz-Kriterium

Definition 9.6.5 (Obere linke Blöcke)**.** Sei $A = (a_{i,j}) \in M_n(\mathbb{C})$. Für $r \in \{1, \dots, n\}$ bezeichnen wir mit $A^{(r)}$ den oberen linken $r \times r$-Block von A:

$$A^{(r)} := \left(a_{i,j}\right)_{1 \le i,j \le r}.$$

Theorem 9.6.6 (Hurwitz-Kriterium)**.** *Sei $A \in M_n(\mathbb{C})$ hermitesch. Dann gilt:*

$$A \text{ ist hermitesch positiv definit} \quad \Longleftrightarrow \quad \det\left(A^{(r)}\right) > 0 \text{ für alle } r \in \{1, \dots, n\}.$$

Die Ungleichungen sind sinnvoll, denn jeder obere linke Block einer hermiteschen Matrix ist wieder hermitesch. Nach Korollar 9.2.10 sind die Determinanten daher reell.

Im reellen Fall gilt analog: Eine symmetrische Matrix $A \in M_n(\mathbb{R})$ ist genau dann positiv definit, wenn alle Determinanten ihrer oberen linken Blöcke positiv sind.

Beweis. Wir beweisen den unitären Fall. Der euklidische Fall folgt mit derselben Argumentation, wobei überall die hermitesche Konjugation H durch Transponierung $\top$ ersetzt wird.

Sei b die zu A gehörige Sesquilinearform auf $\mathbb{C}^n$, also

$$b(v, w) = w^H A v.$$

Positive Definitheit impliziert positive Hauptminoren. Angenommen, A ist hermitesch positiv definit. Dann ist b ein Skalarprodukt auf $\mathbb{C}^n$. Nach dem Orthonormalisierungsverfahren gibt es eine Orthonormalbasis bezüglich dieses Skalarprodukts. Bezüglich dieser Basis ist die Matrix von b die Einheitsmatrix 1_n. Ihre Determinante ist $1 > 0$. Nach dem Vorzeichen-Lemma für Basiswechsel folgt daher

$$\det(A) > 0.$$

Nun sei $r \in \{1, \dots, n\}$. Setze

$$U_r := \operatorname{Span}(e_1, \dots, e_r) \subseteq \mathbb{C}^n.$$

Die Einschränkung von b auf U_r ist wieder ein Skalarprodukt. Bezüglich der Standardbasis $(e_1, \dots, e_r)$ von U_r ist ihre Matrix genau $A^{(r)}$. Mit demselben Argument wie oben folgt

$$\det\left(A^{(r)}\right) > 0.$$

Also sind alle oberen linken Hauptminoren positiv.

Positive Hauptminoren implizieren positive Definitheit. Nun nehmen wir an, dass

$$\det\left(A^{(r)}\right) > 0 \quad \text{für alle } r \in \{1, \dots, n\}$$

gilt. Wir zeigen per Induktion über n, dass b positiv definit ist.

Induktionsanfang $n = 1$**.** Dann ist $A = (a)$ mit $a = \det(A) > 0$. Für $z \in \mathbb{C}$ gilt

$$b(z, z) = \bar{z} a z = a\,|z|^2.$$

Ist $z \neq 0$, dann ist $a\,|z|^2 > 0$. Also ist b positiv definit.

Induktionsschritt. Sei nun $n > 1$, und nehmen wir die Aussage für $(n-1)\times(n-1)$-Matrizen an. Setze

$$U := \mathrm{Span}(e_1, \dots, e_{n-1}).$$

Die Matrix der Einschränkung von b auf U bezüglich der Standardbasis von U ist

$$A^{(n-1)}.$$

Ihre oberen linken Blöcke sind genau die Matrizen $A^{(r)}$ für $r < n$. Da A hermitesch ist, ist auch $A^{(n-1)}$ hermitesch. Ihre oberen linken Blöcke sind genau die Matrizen $A^{(r)}$ für $r < n$. Nach Induktionsannahme ist die Einschränkung von b auf U positiv definit. Also ist sie ein Skalarprodukt auf U.
Wir wählen eine Orthonormalbasis

$$q_1, \dots, q_{n-1}$$

von U bezüglich dieses Skalarprodukts. Wir betrachten diese Vektoren nun als Vektoren in $\mathbb{C}^n$. Dann gilt

$$b(q_i, q_j) = \delta_{i,j} \quad \text{für alle } i, j < n.$$

Nun definieren wir wie bei Gram-Schmidt

$$q_n := e_n - \sum_{i=1}^{n-1} b(e_n, q_i) q_i.$$

Dieser Vektor ist nicht Null. Denn die Summe liegt in U, aber $e_n \notin U$.
Wir zeigen nun, dass q_n zu allen q_j mit $j < n$ „orthogonal“ ist.[1] Für $j < n$ gilt

$$\begin{aligned} b(q_n, q_j) &= b\left(e_n - \sum_{i=1}^{n-1} b(e_n, q_i) q_i, q_j\right) \\ &= b(e_n, q_j) - \sum_{i=1}^{n-1} b(e_n, q_i) b(q_i, q_j) \\ &= b(e_n, q_j) - b(e_n, q_j) = 0. \end{aligned}$$

Da b hermitesch ist, folgt auch

$$b(q_j, q_n) = 0 \quad \text{für alle } j < n.$$

Das System

$$Q = (q_1, \dots, q_n)$$

ist eine Basis von $\mathbb{C}^n$. Denn $q_1, \dots, q_{n-1}$ ist eine Basis von U, und $q_n \notin U$.
Sei D die Matrix von b bezüglich der Basis Q. Nach Konstruktion ist D diagonal. Genauer gilt

$$D = \mathrm{diag}(1, \dots, 1, d_n)$$

mit

$$d_n = b(q_n, q_n) \in \mathbb{R}.$$

[1] Die Verwendung des Wortes „orthogonal“ hier ist sogenannte *abuse of notation*. Formal ist es natürlich falsch ein System als orthogonal zu bezeichnen, wenn noch gar nicht geklärt ist, ob die zugrundeliegende Sesquilinearform ein Skalarprodukt ist. An dieser Stelle bedeutet es also einfach nur, dass $b(q_j, q_n) = 0$. *Abuse of notation* tritt in der Mathematik häufiger auf, wenn es zu umständlich wäre alles formal korrekt zu formulieren. Dabei ist natürlich darauf zu achten, dass es für die Zielgruppe dennoch eindeutig verständlich ist.

Hier ist $\operatorname{diag}(a_1, \dots, a_n)$ die Diagonalmatrix mit Diagonaleinträgen $a_1, \dots, a_n$. Nach dem Vorzeichen-Lemma für Basiswechsel haben D und A Determinanten mit demselben Vorzeichen. Da $\det(A) = \det\left(A^{(n)}\right) > 0$ gilt, folgt

$$\det(D) > 0.$$

Weil D diagonal ist, ist

$$\det(D) = 1 \cdots 1 \cdot d_n = d_n.$$

Also ist $d_n > 0$.

Damit sind alle Diagonaleinträge von D positiv. Nach dem Lemma über diagonale Darstellungen ist b positiv definit. Damit ist der Induktionsschritt bewiesen.

Zusammen ergibt das das Hurwitz-Kriterium. □

Leitbeispiel 9.6.7 (Der Trägheitstensor: ist es ein echter Körper?)**.** Für den Trägheitstensor Leitbeispiel 9.1.14 beantwortet das Hurwitz-Kriterium eine handfeste Frage: Gehört eine gegebene symmetrische Matrix überhaupt zu einem echten dreidimensionalen Körper, kostet also jede Drehung positive Energie? Man muss dafür nicht alle Richtungen ω durchprobieren; es genügt, die drei oberen linken Hauptminoren anzusehen. Für

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

sind das

$$\det\left(I^{(1)}\right) = 2 > 0, \qquad \det\left(I^{(2)}\right) = \det\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} = 3 > 0, \qquad \det\left(I^{(3)}\right) = \det(I) = 6 > 0.$$

Alle drei sind positiv, also ist I positiv definit: Jede Drehung kostet Energie, der Körper ist genuin dreidimensional.

Der obere 2×2-Block ist übrigens ein alter Bekannter: die Pendelmatrix K aus Leitbeispiel 8.1.4 — sein Hauptminor 3 ist genau $\det K$. Und wie beim Pendel die Feder, so verrät hier der Eintrag -1 außerhalb der Diagonale eine *Kopplung*: Für $\omega = (\omega_x, \omega_y, 0)$ ist

$$T(\omega) = \tfrac{1}{2}\left(2\omega_x^2 + 2\omega_y^2 - 2\,\omega_x\omega_y\right),$$

und der gemischte Term $-2\,\omega_x\omega_y$ bedeutet: Die Drehungen um die x- und die y-Achse sind energetisch gekoppelt — unsere Koordinatenachsen sind *nicht* die Hauptachsen des Körpers. Diese Kopplung werden wir mit der Hauptachsentransformation beseitigen.

9.7 Der Spektralsatz für selbstadjungierte Endomorphismen

Wir arbeiten in diesem Abschnitt immer in einem endlich-dimensionalen euklidischen oder unitären Vektorraum. Das Skalarprodukt wird dabei einmal gewählt und dann festgesetzt. Alle vorkommenden Begriffe wie

„adjungiert“, „selbstadjungiert“, „orthogonal“ und „orthonormal“

beziehen sich auf dieses fest gewählte Skalarprodukt. Im unitären Fall verwenden wir weiterhin die Konvention, dass das Skalarprodukt im ersten Argument linear und im zweiten Argument antilinear ist. Wenn stärkere Voraussetzungen notwendig sind, weisen wir ausdrücklich darauf hin.

9.7.1 Isometrien und Standardräume

Definition 9.7.1 (Isometrie)**.** Seien V und W zwei euklidische oder zwei unitäre Vektorräume. Eine lineare Abbildung

$$F : V \to W$$

heißt eine *Isometrie*, wenn für alle $v, w \in V$ gilt

$$\langle F(v), F(w)\rangle = \langle v, w\rangle.$$

Ist F zusätzlich bijektiv, dann heißt F ein *isometrischer Isomorphismus*.

Bemerkung 9.7.2. Eine Isometrie erhält insbesondere Normen, denn

$$\|F(v)\|^2 = \langle F(v), F(v)\rangle = \langle v, v\rangle = \|v\|^2 .$$

Umgekehrt folgt mit Korollar 9.4.7 die Erhaltung des Skalarprodukts aus der Erhaltung der Normen.

Bemerkung 9.7.3. Wegen Bemerkung 9.4.5 muss man in Definition 9.7.1 nicht überprüfen, ob F eine lineare Abbildung ist, es folgt aus der Erhaltung des Skalarprodukts.

Theorem 9.7.4 (Alle Räume haben Geometrie wie Standardräume)**.** *Jeder n-dimensionale euklidische Vektorraum ist isometrisch isomorph zu $\mathbb{R}^n$ mit dem Standardskalarprodukt. Jeder n-dimensionale unitäre Vektorraum ist isometrisch isomorph zu $\mathbb{C}^n$ mit dem Standardskalarprodukt.*

Beweis. Wir schreiben den Beweis gleichzeitig für beide Fälle. Im euklidischen Fall ist $k = \mathbb{R}$, im unitären Fall ist $k = \mathbb{C}$. Nach Gram-Schmidt gibt es eine Orthonormalbasis

$$(v_1, \dots, v_n)$$

von V. Sei $(e_1, \dots, e_n)$ die Standardbasis von k^n. Nach linearer Fortsetzung gibt es genau eine lineare Abbildung

$$F : V \to k^n$$

mit

$$F(v_i) = e_i \quad \text{für alle } i \in \{1, \dots, n\}.$$

Die Abbildung F ist surjektiv, denn die Standardbasis $(e_1, \dots, e_n)$ liegt im Bild. Da V und k^n beide Dimension n haben, ist F nach Lemma 6.4.3 ein Isomorphismus. Es bleibt zu zeigen, dass F das Skalarprodukt erhält. Seien

$$v = \sum_{i=1}^{n} \lambda_i v_i \quad \text{und} \quad w = \sum_{i=1}^{n} \mu_i v_i.$$

Dann ist

$$F(v) = \sum_{i=1}^{n} \lambda_i e_i \quad \text{und} \quad F(w) = \sum_{i=1}^{n} \mu_i e_i.$$

Da beide Basen orthonormal sind, gilt in beiden Räumen

$$\langle v, w\rangle = \sum_{i=1}^{n} \lambda_i \overline{\mu_i} = \langle F(v), F(w)\rangle.$$

Im reellen Fall ist die komplexe Konjugation hier natürlich wirkungslos. Also ist F ein isometrischer Isomorphismus. □

9.7.2 Adjungierte und selbstadjungierte Endomorphismen

Definition 9.7.5 (Adjungierter Endomorphismus)**.** Sei V ein euklidischer oder unitärer Vektorraum, und sei $F : V \to V$ ein Endomorphismus. Ein Endomorphismus $F^* : V \to V$ heißt *adjungiert* zu F, wenn für alle $v, w \in V$ gilt

$$\langle F(v), w\rangle = \langle v, F^*(w)\rangle.$$

Bemerkung 9.7.6. In endlich-dimensionalen euklidischen und unitären Vektorräumen existiert ein solcher adjungierter Endomorphismus und ist eindeutig.

Lemma 9.7.7 (Adjungieren ist involutiv)**.** *Sei V ein endlich-dimensionaler unitärer Vektorraum, und sei $F : V \to V$ ein Endomorphismus. Dann gilt*

$$(F^*)^* = F.$$

Beweis. Wir zeigen, dass F der adjungierte Endomorphismus zu F^* ist. Dann folgt die Behauptung aus der Eindeutigkeit des adjungierten Endomorphismus.

Seien also $v, w \in V$. Aus der Definition von F^* erhalten wir zunächst

$$\langle F(w), v\rangle = \langle w, F^*(v)\rangle.$$

Wir konjugieren beide Seiten. Wegen der hermiteschen Symmetrie des Skalarprodukts folgt

$$\langle v, F(w)\rangle = \langle F^*(v), w\rangle.$$

Also gilt für alle $v, w \in V$

$$\langle F^*(v), w\rangle = \langle v, F(w)\rangle.$$

Das heißt genau: F ist adjungiert zu F^*. Somit ist

$$(F^*)^* = F.$$

□

Wir brauchen hier vor allem die folgende Spezialbedingung.

Definition 9.7.8 (Selbstadjungierter Endomorphismus)**.** Sei V ein euklidischer oder unitärer Vektorraum, und sei $F : V \to V$ ein Endomorphismus. Dann heißt F *selbstadjungiert*, wenn für alle $v, w \in V$ gilt

$$\langle F(v), w\rangle = \langle v, F(w)\rangle.$$

Bemerkung 9.7.9. Das bedeutet: F ist sein eigener adjungierter Endomorphismus, also $F = F^*$.

Lemma 9.7.10 (Selbstadjungiertheit und Matrixsymmetrie)**.**

1. *Sei auf $\mathbb{R}^n$ das Standardskalarprodukt gewählt, und sei $A \in M_n(\mathbb{R})$. Dann gilt:*

$$L_A \text{ ist selbstadjungiert} \quad \Longleftrightarrow \quad A^\top = A.$$

2. *Sei auf $\mathbb{C}^n$ das Standardskalarprodukt gewählt, und sei $A \in M_n(\mathbb{C})$. Dann gilt:*

$$L_A \text{ ist selbstadjungiert} \quad \Longleftrightarrow \quad A^H = A.$$

Bemerkung 9.7.11. Später sehen wir in Lemma 9.8.3, dass für Orthonormalbasen B gilt, dass

$$M_{B\leftarrow B}(T^*) = M_{B\leftarrow B}(T)^H.$$

Im euklidischen Fall kann man das H natürlich durch ein $\top$ ersetzen.

Also gilt allgemein für jede Orthonormalbasis B:

$$T \text{ ist selbstadjungiert} \quad \Longleftrightarrow \quad M_{B\leftarrow B}(T)^H = M_{B\leftarrow B}(T).$$

Beweis. Wir beweisen den unitären Fall. Der euklidische Fall ist dieselbe Rechnung ohne komplexe Konjugation, also mit $A^\top$ statt A^H. Für $v, w \in \mathbb{C}^n$ gilt bezüglich des Standardskalarprodukts

$$\langle v, L_A(w)\rangle = (Aw)^H v = w^H A^H v$$

und

$$\langle L_A(v), w\rangle = w^H A v.$$

Ist $A^H = A$, dann sind diese beiden Ausdrücke für alle v, w gleich. Also ist L_A selbstadjungiert. Sei umgekehrt L_A selbstadjungiert. Dann gilt für alle $v, w \in \mathbb{C}^n$

$$w^H A v = w^H A^H v.$$

Also definieren A und A^H dieselbe Sesquilinearform

$$(v, w) \mapsto w^H A v = w^H A^H v.$$

Nach der Eindeutigkeit der darstellenden Matrix folgt

$$A = A^H.$$

Diese Eindeutigkeit sieht man auch direkt, indem man $v = e_j$ und $w = e_i$ einsetzt. Dann liest man den (i, j)-ten Matrixeintrag ab. □

Lemma 9.7.12 (Eigenwerte und Eigenvektoren selbstadjungierter Endomorphismen)**.** *Sei V ein euklidischer oder unitärer Vektorraum, und sei $F : V \to V$ selbstadjungiert. Dann gelten:*

1. *Jeder Eigenwert von F ist reell.*
2. *Eigenvektoren zu unterschiedlichen Eigenwerten sind orthogonal.*

Beweis. Seien u, v Eigenvektoren von F zu Eigenwerten λ und μ. Also gilt

$$F(u) = \lambda u \quad \text{und} \quad F(v) = \mu v.$$

Dann rechnen wir

$$\lambda\langle u, v\rangle = \langle \lambda u, v\rangle = \langle F(u), v\rangle = \langle u, F(v)\rangle = \langle u, \mu v\rangle = \overline{\mu}\langle u, v\rangle.$$

Also gilt

$$(\lambda - \overline{\mu})\langle u, v\rangle = 0.$$

Setzen wir nun $u = v$ und $\lambda = \mu$, dann erhalten wir

$$\left(\lambda - \overline{\lambda}\right)\langle u, u\rangle = 0.$$

Da u ein Eigenvektor ist, gilt $u \neq 0$, also $\langle u, u\rangle > 0$. Damit folgt

$$\lambda = \overline{\lambda}.$$

Also ist $\lambda \in \mathbb{R}$. Im euklidischen Fall war das ohnehin klar, weil die Skalare reell sind. Seien nun u und v Eigenvektoren zu unterschiedlichen Eigenwerten $\lambda \neq \mu$. Nach dem ersten Teil sind beide Eigenwerte reell. Also ist

$$\lambda - \overline{\mu} = \lambda - \mu \neq 0.$$

Aus

$$(\lambda - \overline{\mu})\langle u, v\rangle = 0$$

folgt daher

$$\langle u, v\rangle = 0.$$

Also sind u und v orthogonal. □

Bemerkung 9.7.13 (Warum Physikerinnen und Physiker das mögen)**.** In der Quantenmechanik werden mögliche Messergebnisse durch Eigenwerte geeigneter Operatoren beschrieben. Dass selbstadjungierte Operatoren nur reelle Eigenwerte haben, ist daher nicht bloß ein nettes Rechenphänomen. Es passt dazu, dass Messergebnisse reelle Zahlen sein sollen. In der endlichdimensionalen linearen Algebra sehen wir hier die algebraische Grundform dieses Prinzips.

Definition 9.7.14. Eine orthonormale Basis aus Eigenvektoren (eines gegebenen Endomorphismus F) heißt (F-)ON-Eigenbasis.

Theorem 9.7.15 (Diagonalisierbar und selbstadjungiert liefert ON-Eigenbasis)**.** *Sei $F : V \to V$ selbstadjungiert. Ist F diagonalisierbar, dann besitzt V eine Orthonormalbasis aus Eigenvektoren von F.*

Beweis. Da F diagonalisierbar ist, ist, nach Theorem 8.3.11, V die direkte Summe der Eigenräume:

$$V = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_r}.$$

Nach dem vorherigen Lemma sind verschiedene Eigenräume orthogonal zueinander. Auf jedem Eigenraum E_{λ_j} wählen wir irgendeine Basis und wenden Gram-Schmidt an. So erhalten wir eine Orthonormalbasis von E_{λ_j}. Gram-Schmidt zerstört die Eigenschaft, im Eigenraum zu liegen, nicht: Es werden nur Linearkombinationen von Vektoren aus demselben Eigenraum gebildet. Die Vereinigung dieser Orthonormalbasen über alle Eigenräume ist daher ein orthonormales System. Sie erzeugt ganz V, weil die Eigenräume zusammen V erzeugen. Also ist sie eine Orthonormalbasis von V, und alle ihre Vektoren sind Eigenvektoren. □

Algorithmus 9.7.16 (ON-Eigenbasis im diagonalisierbaren selbstadjungierten Fall)**.** *Angenommen, F ist selbstadjungiert und diagonalisierbar. Eine ON-Eigenbasis erhält man so:*

1. *Bestimme die Eigenwerte von F.*
2. *Bestimme zu jedem Eigenwert λ den Eigenraum*
$$E_\lambda = \operatorname{Kern}(F - \lambda \operatorname{Id}).$$
3. *Wähle in jedem Eigenraum irgendeine Basis.*
4. *Wende Gram-Schmidt getrennt auf jede dieser Basen an. So erhältst du in jedem Eigenraum eine ONB.*
5. *Setze diese ONBs zusammen. Da verschiedene Eigenräume orthogonal sind, ist das Ergebnis eine ON-Eigenbasis von V.*

9.7.3 Existenz von Eigenwerten

Theorem 9.7.17 (Fundamentalsatz der Algebra)**.** *Sei $p \in \mathbb{C}[X]$ ein nicht-konstantes Polynom. Betrachtet man p als Funktion*

$$f_p : \mathbb{C} \to \mathbb{C}, \quad z \mapsto p(z),$$

dann besitzt f_p mindestens eine Nullstelle. Das heißt: Es gibt ein $\lambda \in \mathbb{C}$ mit

$$p(\lambda) = 0.$$

Bemerkung 9.7.18. Wir beweisen den Fundamentalsatz der Algebra hier nicht. Ein Beweis benutzt typischerweise Analysis, zum Beispiel Methoden der komplexen Funktionen und komplexer Differenzierbarkeit. Für den Spektralsatz verwenden wir den Satz als externes Werkzeug.

Lemma 9.7.19 (Selbstadjungierte Endomorphismen haben Eigenwerte)**.** *Sei V ein endlich-dimensionaler euklidischer oder unitärer Vektorraum mit $\dim(V) > 0$, und sei $F : V \to V$ selbstadjungiert. Dann besitzt F mindestens einen Eigenwert. Dieser Eigenwert ist notwendig reell.*

Beweis. Wir unterscheiden den unitären und den euklidischen Fall.

Unitärer Fall. Hier brauchen wir die Selbstadjungiertheit zunächst gar nicht. Das charakteristische Polynom von F ist ein nicht-konstantes Polynom über $\mathbb{C}$. Es ist nicht-konstant, da wir wissen, dass der Grad des Polynoms genau die Dimension des Raumes ist und es gilt $\dim(V) > 0$. Nach dem Fundamentalsatz der Algebra besitzt es eine Nullstelle $\lambda \in \mathbb{C}$. Da wir über dem Körper $\mathbb{C}$ arbeiten, ist λ nach dem bereits bewiesenen Eigenwertkriterium tatsächlich ein Eigenwert von F. Weil F selbstadjungiert ist, ist dieser Eigenwert nach dem vorherigen Lemma reell.

Euklidischer Fall. Wir wählen eine Orthonormalbasis von V. Bezüglich dieser Basis identifizieren wir V isometrisch mit $\mathbb{R}^n$ mit dem Standardskalarprodukt. Die Matrix von F bezüglich dieser ONB sei $A \in M_n(\mathbb{R})$. Da F selbstadjungiert ist, ist A symmetrisch. Nun betrachten wir dieselbe Matrix A, aber als komplexe Matrix. Sie definiert eine $\mathbb{C}$-lineare Abbildung

$$F_{\mathbb{C}} : \mathbb{C}^n \to \mathbb{C}^n, \quad z \mapsto Az.$$

Diese Abbildung ist die eindeutige komplexe Fortsetzung von F: Auf dem eingebetteten $\mathbb{R}^n \subseteq \mathbb{C}^n$ stimmt sie mit F überein. Das charakteristische Polynom von $F_{\mathbb{C}}$ ist dasselbe Polynom wie das charakteristische Polynom von A über $\mathbb{R}$. Denn in beiden Fällen ist es durch dieselbe Leibnizformel (die ja für alle Körper gilt)

$$\det(X1_n - A) = \sum_{\sigma \in S_n} \operatorname{signum}(\sigma) \prod_{i=1}^{n} \left(X \cdot \delta_{i,\sigma} - A_{i,\sigma(i)} \right) .$$

gegeben, mit denselben reellen Koeffizienten. Nach dem Fundamentalsatz der Algebra besitzt dieses Polynom eine komplexe Nullstelle $\lambda \in \mathbb{C}$. Über $\mathbb{C}$ ist diese Nullstelle ein Eigenwert von $F_{\mathbb{C}}$. Da A reell symmetrisch ist, gilt als komplexe Matrix

$$A^H = A.$$

Also ist $F_{\mathbb{C}}$ selbstadjungiert bezüglich des Standardskalarprodukts auf $\mathbb{C}^n$. Nach dem vorherigen Lemma ist jeder Eigenwert von $F_{\mathbb{C}}$ reell. Also gilt

$$\lambda \in \mathbb{R}.$$

Damit ist λ eine reelle Nullstelle von $\det(X1_n - A)$. Also gilt

$$\det(\lambda 1_n - A) = 0$$

als Gleichung über $\mathbb{R}$. Nach dem Eigenwertkriterium über $\mathbb{R}$ ist λ ein Eigenwert der ursprünglichen reellen Abbildung. □

Bemerkung 9.7.20 (Warum der Umweg über $\mathbb{C}^n$ nötig ist)**.** Der schnelle Slogan lautet: Das charakteristische Polynom hat über $\mathbb{C}$ eine Nullstelle, und bei selbstadjungierten Matrizen muss diese Nullstelle reell sein. Dieser Slogan ist richtig, aber er versteckt einen wichtigen Punkt. Das Kriterium

$$\lambda \text{ ist Eigenwert} \quad \Longleftrightarrow \quad \det(\lambda 1_n - A) = 0$$

setzt voraus, dass λ im zugrunde liegenden Körper liegt. Für eine reelle Matrix ist eine komplexe Nullstelle des charakteristischen Polynoms also im Allgemeinen kein Eigenwert der reellen Abbildung. Ein reeller Endomorphismus darf ja keine komplexen Vielfachen seiner Vektoren verwenden. Darum konstruieren wir im euklidischen Fall zuerst die komplexe Fortsetzung $F_{\mathbb{C}}$. Für diese komplexe Abbildung ist die komplexe Nullstelle wirklich ein Eigenwert. Dann nutzen wir die Selbstadjungiertheit, um zu zeigen, dass dieser Eigenwert sogar reell ist. Erst dann dürfen wir wieder zur ursprünglichen reellen Abbildung zurückkehren.

9.7.4 Invariante Unterräume

Definition 9.7.21 (Invarianter Unterraum)**.** Sei V ein Vektorraum, und sei $F : V \to V$ ein Endomorphismus. Ein Untervektorraum $U \subseteq V$ heißt *F-invariant*, wenn

$$F(U) \subseteq U$$

gilt. Das heißt: Für jedes $u \in U$ liegt auch $F(u)$ wieder in U.

Bemerkung 9.7.22 (Warum Invarianz hilft)**.** Ist $U \subseteq V$ invariant, dann kann man F auf U einschränken. Man erhält also einen Endomorphismus

$$F|_U : U \to U.$$

Sind sogar zwei Unterräume $U, W \subseteq V$ invariant und gilt

$$V = U \oplus W,$$

dann zerfällt die Untersuchung von F in zwei kleinere Untersuchungen: auf U und auf W. In einer Basis, die zuerst aus einer Basis von U und dann aus einer Basis von W besteht, hat die Matrix von F Blockdiagonalgestalt. Das ist der lineare Algebra-Modus von: „Ein großes Problem in kleinere Probleme zerlegen."

Lemma 9.7.23 (Orthogonale Komplemente invariant)**.** *Sei $F : V \to V$ selbstadjungiert, und sei $U \subseteq V$ ein F-invarianter Unterraum. Dann ist auch das orthogonale Komplement*

$$U^{\perp}$$

F-invariant.

Beweis. Sei $v \in U^\perp$. Wir müssen zeigen, dass $F(v) \in U^\perp$ gilt. Sei also $u \in U$. Dann gilt

$$\langle F(v), u\rangle = \langle v, F(u)\rangle.$$

Da U invariant ist, liegt $F(u)$ wieder in U. Da $v \in U^\perp$ ist, folgt

$$\langle v, F(u)\rangle = 0.$$

Also gilt

$$\langle F(v), u\rangle = 0$$

für alle $u \in U$. Damit liegt $F(v)$ in $U^\perp$. □

9.7.5 Der Spektralsatz

Theorem 9.7.24 (Spektralsatz für selbstadjungierte Endomorphismen)**.** *Sei V ein endlich-dimensionaler euklidischer oder unitärer Vektorraum, und sei $F : V \to V$ selbstadjungiert. Dann besitzt V eine Orthonormalbasis aus Eigenvektoren von F. Insbesondere ist F diagonalisierbar.*

Beweis. Wir geben den Beweis als iteratives Verfahren. Formal ist das eine Induktion über die Dimension. Setze zunächst

$$W_0 := V.$$

Falls $W_0 = \{0\}$ ist, ist nichts zu zeigen. Andernfalls besitzt $F|_{W_0} = F$ nach Lemma 9.7.19 einen Eigenwert. Sei λ_1 ein solcher Eigenwert, und sei

$$U_1 := \operatorname{Kern}(F - \lambda_1 \operatorname{Id})$$

der zugehörige Eigenraum. Dann ist $U_1 \neq \{0\}$, und U_1 ist F-invariant. Setze

$$W_1 := U_1^\perp.$$

Nach der orthogonalen Zerlegung gilt

$$W_0 = U_1 \oplus W_1.$$

Nach Lemma 9.7.23 ist W_1 wieder F-invariant. Falls es Eigenvektoren zu anderen Eigenwerten gibt, liegen sie automatisch in W_1. Das folgt aus der Orthogonalität von Eigenvektoren zu unterschiedlichen Eigenwerten. Wir haben also den ersten Eigenraum abgespalten, ohne die anderen Eigenrichtungen zu beschädigen. Nun wiederholen wir dasselbe Argument auf W_1. Nach Korollar 3.3.28 reduziert sich die Dimension dabei um $\dim(U_1)$, denn es gilt

$$\dim(W_0) = \dim(U_1) + \dim(W_1)\,.$$

Die Einschränkung

$$F|_{W_1} : W_1 \to W_1$$

ist wieder selbstadjungiert bezüglich des eingeschränkten Skalarprodukts, denn für $v, w \in W_1$ gilt

$$\langle F|_{W_1}(v), w\rangle = \langle F(v), w\rangle = \langle v, F(w)\rangle = \langle v, F|_{W_1}(w)\rangle.$$

Wenn $W_1 \neq \{0\}$ ist, besitzt diese Einschränkung also wieder einen Eigenwert.

Wir erhalten einen Eigenraum $U_2 \subseteq W_1$ und das orthogonale Komplement

$$W_2 := U_2^\perp \quad \text{innerhalb von } W_1.$$

Dann gilt

$$W_1 = U_2 \oplus W_2.$$

So fahren wir fort. In jedem Schritt ist $U_j \neq \{0\}$, also gilt

$$\dim(W_j) = \dim(W_{j-1}) - \dim(U_j) < \dim(W_{j-1}).$$

Die Dimension wird also in jedem Schritt echt kleiner. Irgendwann muss daher

$$W_m = \{0\}$$

gelten. Negativ kann eine Dimension nicht werden. Zusammengesetzt erhalten wir eine orthogonale direkte Summe

$$V = U_1 \oplus U_2 \oplus \cdots \oplus U_m.$$

Jeder Raum U_j besteht aus Eigenvektoren von F zu einem Eigenwert λ_j. Außerdem ist

$$\dim(V) = \dim(U_1) + \cdots + \dim(U_m).$$

Die Summe der Dimensionen der gefundenen Eigenräume ist also die ganze Dimension von V. Das ist genau die Diagonalisierbarkeit. Wählen wir nun in jedem U_j eine ONB, dann ist die Vereinigung dieser Basen eine ONB von V. Da alle Vektoren in den U_j Eigenvektoren von F sind, erhalten wir eine Orthonormalbasis aus Eigenvektoren. □

Bemerkung 9.7.25 (Was der Spektralsatz sagt)**.** Der Spektralsatz ist stark. Er sagt: Sobald ein Endomorphismus selbstadjungiert ist, gibt es nicht nur genug Eigenvektoren, sondern sogar eine orthonormale Eigenbasis. In Matrixsprache heißt das: Eine reelle symmetrische Matrix ist automatisch diagonalisierbar. Nicht „vielleicht nach Glück“, nicht „wenn die Eigenwerte verschieden sind“, sondern immer. Das ist erstaunlich und sehr nützlich. Über $\mathbb{C}$ muss man allerdings vorsichtig sein. Die richtige Bedingung ist nicht $A^\top = A$, sondern

$$A^H = A.$$

Komplexe Hermiteschheit ist die Matrixform von Selbstadjungiertheit bezüglich des unitären Standardskalarprodukts.

9.7.6 Die Hauptachsentransformation

Bemerkung 9.7.26 (Orthogonale und unitäre Basiswechselmatrizen)**.** Sei $A \in M_n(\mathbb{R})$ symmetrisch, und seien $s_1, \ldots, s_n$ eine ONB aus Eigenvektoren. Setzen wir diese Vektoren als Spalten in eine Matrix

$$S = \begin{pmatrix} | & & | \\ s_1 & \cdots & s_n \\ | & & | \end{pmatrix},$$

dann ist S orthogonal. Also gilt

$$S^{-1} = S^\top.$$

Die Diagonalisierung hat daher die besonders einfache Form

$$S^\top A S = D.$$

Im komplexen Fall ist S unitär, also

$$S^{-1} = S^H,$$

und die Diagonalisierung lautet

$$S^H AS = D.$$

Die Diagonaleinträge von D sind die Eigenwerte, also im selbstadjungierten Fall reell. Im reellen Fall kann man die Determinante von S auf 1 bringen, indem man das Vorzeichen eines Eigenvektors ändert. Dann liegt S sogar in $SO(n)$. Im komplexen Fall kann man eine Spalte mit einer komplexen Zahl vom Betrag 1 multiplizieren, um die Determinante auf 1 zu bringen. Dann liegt S sogar in $SU(n)$. Die Diagonalgestalt ändert sich dabei nicht.

Korollar 9.7.27 (Hauptachsentransformation)**.** *Die folgenden Resultate gelten für symmetrische bzw. hermitesche Matrizen im $\mathbb{R}^n$ bzw. $\mathbb{C}^n$. Das heißt für selbstadjungierte Operatoren bzgl. des Standardskalarprodukts.*

1. *Ist $A \in M_n(\mathbb{R})$ symmetrisch, dann gibt es ein $S \in SO(n)$, so dass*

   $$S^\top AS$$

   Diagonalgestalt hat.

2. *Ist $A \in M_n(\mathbb{C})$ hermitesch, dann gibt es ein $S \in SU(n)$, so dass*

   $$S^H AS$$

   eine reelle Diagonalmatrix ist.

Beweis. Wir beweisen beide Aussagen gleichzeitig. Im reellen Fall verwenden wir das Standardskalarprodukt auf $\mathbb{R}^n$, im komplexen Fall das Standardskalarprodukt auf $\mathbb{C}^n$. Ist A symmetrisch beziehungsweise hermitesch, dann ist L_A nach dem Lemma über selbstadjungierte Matrizen selbstadjungiert. Nach dem Spektralsatz gibt es eine ONB aus Eigenvektoren von L_A. Wir schreiben diese Eigenvektoren als Spalten in eine Matrix S. Im reellen Fall ist $S \in O(n)$, und im komplexen Fall ist $S \in U(n)$. Bezüglich der Eigenbasis ist die Matrix von L_A diagonal. Daher gilt im reellen Fall $S^\top = S^{-1}$ und damit

$$S^\top AS = D.$$

Im komplexen Fall gilt $S^H = S^{-1}$ und damit

$$S^H AS = D.$$

In beiden Fällen ist D diagonal. Die Diagonaleinträge sind die Eigenwerte von L_A. Diese sind nach dem Eigenwert-Lemma reell. Es bleibt nur die Zusatzbedingung an die Determinante. Im reellen Fall gilt für $S \in O(n)$

$$\det(S) = \pm 1.$$

Falls $\det(S) = -1$ ist, multiplizieren wir eine Spalte von S mit -1. Das ändert weder die Orthonormalität noch die Eigenschaft, Eigenvektor zu sein. Es ändert auch die Diagonalmatrix D nicht. Danach gilt $S \in SO(n)$. Im komplexen Fall gilt für $S \in U(n)$

$$|\det(S)| = 1.$$

Multiplizieren wir eine Spalte von S mit $\det(S)^{-1}$, dann bleibt diese Spalte normiert, bleibt Eigenvektor, und die Determinante der neuen Matrix wird 1. Auch hier ändert sich die Diagonalmatrix D nicht. Also können wir $S \in SU(n)$ erreichen. □

Bemerkung 9.7.28. Die Hauptachsentransformation ist also kein neues Wunder zusätzlich zum Spektralsatz. Sie ist der Spektralsatz in Matrixsprache, mit der Zusatzinformation, dass die Basiswechselmatrix wegen der Orthonormalität orthogonal beziehungsweise unitär gewählt werden kann.

Leitbeispiel 9.7.29 (Der Trägheitstensor: die Hauptachsentransformation)**.** Jetzt der Höhepunkt für unseren Körper Leitbeispiel 9.1.14. Der Trägheitstensor

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

ist symmetrisch, also selbstadjungiert bezüglich des Standardskalarprodukts. Nach dem Spektralsatz gibt es daher eine Orthonormalbasis aus Eigenvektoren. Und wir müssen sie nicht einmal neu ausrechnen: Der Block oben links ist unsere Pendelmatrix K aus Leitbeispiel 8.1.4! Deren Eigenvektoren kennen wir seit dem Eigenwertkapitel — Gleichtakt $(1,1)$ zum Eigenwert 1 und Gegentakt $(1,-1)$ zum Eigenwert 3. In die xy-Ebene gelegt und normiert sind sie (zusammen mit der unberührten z-Achse) genau die gesuchten Hauptachsen:

$$s_1 = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \quad s_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \quad s_3 = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}$$

mit den Eigenwerten — den *Hauptträgheitsmomenten* —

$$\lambda_1 = 1, \qquad \lambda_2 = 2, \qquad \lambda_3 = 3.$$

Setzt man diese Vektoren als Spalten in

$$S = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & \sqrt{2} & 0 \end{pmatrix} \in SO(3),$$

so wird

$$S^\top I S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Das ist die Hauptachsentransformation: Die neuen Achsen sind die beiden Diagonalen der xy-Ebene und die alte z-Achse. Das Koordinatensystem wird also um 45° um die z-Achse gedreht — und die Achsen werden passend umnummeriert, damit die Hauptträgheitsmomente geordnet erscheinen. Im Hauptachsensystem des Körpers verschwindet die störende Kopplung -1.

Und jetzt zahlen sich die beiden Rollen der Matrix I aus. Weil S orthogonal ist, ist $S^\top I S$ zugleich

- die *Diagonalisierung des Operators* I, denn $S^\top = S^{-1}$, also $S^\top I S = S^{-1} I S$, und
- die *Diagonalgestalt der Energieform* $\langle \cdot, \cdot \rangle_I$, deren Matrix sich bei einem Basiswechsel gerade als $S^\top I S$ transformiert.

In Hauptachsenkoordinaten $\omega = (\omega_1, \omega_2, \omega_3)$ entkoppelt die Rotationsenergie vollständig:

$$T(\omega) = \tfrac{1}{2}\left(\lambda_1 \omega_1^2 + \lambda_2 \omega_2^2 + \lambda_3 \omega_3^2\right).$$

Das ist dieselbe entkoppelte Gestalt wie bei den zwei gekoppelten Pendeln: Diagonalisieren heißt, Koordinaten zu finden, in denen das System in unabhängige Achsen zerfällt.

9.7.7 Hauptachsentransformation und Skalarprodukte

In den letzten Abschnitten sind zwei verschiedene Arten von Basiswechseln aufgetreten. Bei linearen Abbildungen wechselt man die Beschreibung eines Endomorphismus. Bei Sesquilinearformen wechselt man die Beschreibung einer Form. Diese beiden Situationen sind nicht dasselbe. Gerade bei orthonormalen Basiswechseln sehen die Formeln aber plötzlich gleich aus. Das ist der Grund, warum die Hauptachsentransformation so elegant formuliert werden kann.

Bemerkung 9.7.30 (Zwei Basiswechsel, zwei Bedeutungen)**.** Sei zunächst $F : V \to V$ ein Endomorphismus, und seien B und C zwei Basen von V. Schreiben wir

$$P := M_{B\leftarrow C}(\mathrm{Id}),$$

dann gilt

$$[x]_B = P[x]_C.$$

Sind M_B und M_C die Matrizen von F bezüglich B und C, dann gilt

$$M_C = P^{-1}M_BP.$$

Das ist ein Basiswechsel für eine lineare Abbildung.

Ist dagegen $b : V \times V \to \mathbb{C}$ eine Sesquilinearform, und sind A_B und A_C die Matrizen von b bezüglich B und C, dann gilt

$$A_C = P^HA_BP.$$

Das ist ein Basiswechsel für eine Sesquilinearform. Die Formel ist anders: Es steht nicht P^{-1} links, sondern P^H.

Lemma 9.7.31 (Warum die Formeln bei ON-Basiswechseln zusammenfallen)**.** *Sei V ein euklidischer oder unitärer Vektorraum, und seien B und C zwei Orthonormalbasen. Sei*

$$P := M_{B\leftarrow C}(\mathrm{Id}).$$

Dann ist P orthogonal im euklidischen Fall und unitär im unitären Fall. Insbesondere gilt

$$P^{-1} = P^\top \quad \textit{im euklidischen Fall}$$

und

$$P^{-1} = P^H \quad \textit{im unitären Fall.}$$

Daher haben der Endomorphismen-Basiswechsel und der Form-Basiswechsel bei ON-Basiswechseln dieselbe sichtbare Form. Im euklidischen Fall ist

$$P^{-1}MP = P^\top MP,$$

und im unitären Fall ist

$$P^{-1}MP = P^HMP.$$

Beweis. Die Spalten von P sind die Koordinaten der Vektoren aus C bezüglich der ONB B. Da C selbst eine ONB ist, bilden diese Spalten im Standardraum wieder eine ONB. Nach der Charakterisierung orthogonaler beziehungsweise unitärer Matrizen ist P daher orthogonal beziehungsweise unitär. Also gilt im euklidischen Fall $P^\top P = 1_n$, und im unitären Fall $P^HP = 1_n$. Das ist äquivalent zu

$$P^{-1} = P^\top \quad \text{beziehungsweise} \quad P^{-1} = P^H.$$

□

Bemerkung 9.7.32 (Was die Hauptachsentransformation gleichzeitig tut)**.** Sei $A \in M_n(\mathbb{C})$ hermitesch, also $A^H = A$. Dann definiert A einerseits einen selbstadjungierten Endomorphismus

$$L_A : \mathbb{C}^n \to \mathbb{C}^n, \quad v \mapsto Av.$$

Andererseits definiert A eine hermitesche Sesquilinearform

$$b_A(v, w) := \langle L_A(v), w \rangle = w^H A v.$$

Wählt man nun nach dem Spektralsatz eine ONB aus Eigenvektoren von L_A, und ist S die Matrix, deren Spalten diese ONB sind, dann ist S unitär. Also gilt

$$S^{-1} = S^H.$$

Für den Endomorphismus gilt daher

$$S^{-1}AS = S^H AS = D,$$

wobei D eine reelle Diagonalmatrix ist.

Dieselbe Matrix $S^H AS$ ist aber zugleich die Basiswechselmatrix der Sesquilinearform b_A in die neue Basis. Die Hauptachsentransformation diagonalisiert also gleichzeitig

1. den selbstadjungierten Endomorphismus L_A durch einen ON-Basiswechsel,
2. und die hermitesche Sesquilinearform b_A durch denselben Basiswechsel.

Dass dieselbe Formel erscheint, liegt nicht daran, dass Endomorphismen und Formen dasselbe wären. Es liegt daran, dass die Basiswechselmatrix unitär ist.

Bemerkung 9.7.33 (Jedes Skalarprodukt ist als Form diagonalisierbar)**.** Sei b ein Skalarprodukt auf $\mathbb{C}^n$, und sei A seine Matrix bezüglich der Standardbasis. Dann ist A hermitesch und positiv definit. Wendet man Gram-Schmidt bezüglich des Skalarprodukts b auf die Standardbasis an, erhält man eine b-Orthonormalbasis $(q_1, \dots, q_n)$. Ist P die Matrix mit Spalten $q_1, \dots, q_n$, dann gilt

$$P^H AP = 1_n.$$

Also ist jedes Skalarprodukt durch einen Basiswechsel der Sesquilinearform sogar auf die Einheitsmatrix bringbar. Insbesondere ist jedes Skalarprodukt als hermitesche Form diagonalisierbar.

Im reellen Fall gilt dieselbe Aussage mit $P^\top AP = 1_n$.

Bemerkung 9.7.34 (Warum das kein alternativer Spektralsatz-Beweis ist)**.** Die letzte Bemerkung ist sehr nützlich, aber sie beweist nicht den Spektralsatz für positiv definite selbstadjungierte Matrizen. Der Grund ist die Art des Basiswechsels.

Aus einer b_A-ONB folgt

$$P^H AP = 1_n.$$

Das ist eine Kongruenztransformation der Form b_A. Für die Matrix des Endomorphismus L_A bräuchte man aber

$$P^{-1}AP.$$

Diese beiden Ausdrücke sind nur dann gleich, wenn P bezüglich des ursprünglichen Standardskalarprodukts unitär ist, also wenn $P^{-1} = P^H$ gilt. Eine b_A-ONB ist aber im Allgemeinen keine Standard-ONB. Ihre Spalten erfüllen

$$q_j^H A q_i = \delta_{ij},$$

nicht notwendig

$$q_j^H q_i = \delta_{ij}.$$

Daher ist P im Allgemeinen nicht unitär.

Kurz gesagt: Gram-Schmidt bezüglich b_A diagonalisiert die Form. Der Spektralsatz diagonalisiert den selbstadjungierten Endomorphismus durch eine ONB bezüglich des fest gewählten ursprünglichen Skalarprodukts. Das sind verschiedene Aussagen. Sie berühren sich genau dann in derselben Formel, wenn der Basiswechsel orthogonal beziehungsweise unitär ist.

Korollar 9.7.35 (Positive Definitheit und Eigenwerte)**.** *Sei $A \in M_n(\mathbb{R})$ symmetrisch oder $A \in M_n(\mathbb{C})$ hermitesch. Dann sind äquivalent:*

1. *A ist positiv definit, das heißt*

$$v^H A v > 0 \quad \text{für alle } v \neq 0.$$

   Im reellen Fall steht hier entsprechend $v^\top A v > 0$.

2. *Alle Eigenwerte von A sind positiv.*

Beweis. Nach dem Spektralsatz gibt es im unitären Fall eine Matrix $S \in U(n)$ mit

$$S^H A S = D,$$

und im euklidischen Fall eine Matrix $S \in O(n)$ mit

$$S^\top A S = D.$$

Dabei ist D jeweils eine reelle Diagonalmatrix. Ihre Diagonaleinträge sind die Eigenwerte von A.

Sei zunächst A positiv definit. Ist q_i ein Eigenvektor zum Eigenwert λ_i mit $\|q_i\| = 1$, dann gilt

$$0 < q_i^H A q_i = q_i^H \lambda_i q_i = \lambda_i q_i^H q_i = \lambda_i.$$

Also ist jeder Eigenwert positiv.

Seien nun umgekehrt alle Eigenwerte positiv. Sei $v \neq 0$. Im unitären Fall setzen wir $x := S^H v$, im euklidischen Fall setzen wir $x := S^\top v$. Da S unitär beziehungsweise orthogonal ist, ist $x \neq 0$. Dann gilt im unitären Fall

$$v^H A v = x^H D x = \sum_{i=1}^{n} \lambda_i |x_i|^2 .$$

Im euklidischen Fall gilt dieselbe Rechnung mit transponierten statt hermitesch transponierten Vektoren. Da mindestens ein $x_i \neq 0$ ist und alle $\lambda_i > 0$ sind, ist diese Summe positiv. Also ist A positiv definit. □

9.8 Der Spektralsatz für normale Endomorphismen

Wir betrachten nun eine Erweiterung des Spektralsatzes. In diesem Abschnitt arbeiten wir ausschließlich in endlich-dimensionalen unitären Vektorräumen. Das Skalarprodukt ist fest gewählt. Insbesondere beziehen sich die Begriffe

„adjungiert“, „orthogonal“ und „orthonormal“

immer auf dieses Skalarprodukt.

Der euklidische Fall steht hier bewusst nicht im Mittelpunkt. Über $\mathbb{R}$ sind normale Endomorphismen im Allgemeinen nicht orthogonal diagonalisierbar. Eine Drehung der Ebene ist zum Beispiel normal, hat aber über $\mathbb{R}$ im Allgemeinen keine Eigenwerte. Über $\mathbb{C}$ ist die Lage sauberer: Normale Endomorphismen sind genau die Endomorphismen, die durch eine Orthonormalbasis diagonalisiert werden können.

9.8.1 Normale Endomorphismen

Definition 9.8.1 (Normaler Endomorphismus)**.** Sei V ein unitärer Vektorraum, und sei $F : V \to V$ ein Endomorphismus. Dann heißt F *normal*, wenn F mit seinem adjungierten Endomorphismus (Definition 9.7.5) kommutiert, das heißt, wenn

$$F^*F = FF^*$$

gilt.

Bemerkung 9.8.2. Jeder selbstadjungierte Endomorphismus ist normal. Denn aus $F = F^*$ folgt sofort

$$F^*F = F^2 = FF^*.$$

Normale Endomorphismen sind also eine Verallgemeinerung selbstadjungierter Endomorphismen. Der Preis ist: Die Eigenwerte müssen nicht mehr reell sein.

9.8.2 Adjungierte und Matrizen in Orthonormalbasen

Lemma 9.8.3 (Matrix des adjungierten Endomorphismus)**.** *Sei V ein endlich-dimensionaler unitärer Vektorraum, sei $F : V \to V$ ein Endomorphismus, und sei B eine Orthonormalbasis von V. Setze*

$$A := M_{B \leftarrow B}(F) \quad \textit{und} \quad C := M_{B \leftarrow B}(F^*).$$

Dann gilt

$$C = A^H.$$

Beweis. Seien $v, w \in V$. Da B eine Orthonormalbasis ist, wird das Skalarprodukt in Koordinaten durch das Standardskalarprodukt beschrieben:

$$\langle v, w \rangle = [w]_B^H [v]_B.$$

Wir berechnen beide Seiten der Adjungiertheitsbedingung. Einerseits gilt

$$\langle F(v), w \rangle = [w]_B^H A [v]_B.$$

Andererseits gilt

$$\langle v, F^*(w) \rangle = [C[w]_B]^H [v]_B = [w]_B^H C^H [v]_B.$$

Da F^* adjungiert zu F ist, sind diese beiden Ausdrücke für alle $v, w \in V$ gleich. Also gilt

$$[w]_B^H A [v]_B = [w]_B^H C^H [v]_B$$

für alle Koordinatenvektoren $[v]_B, [w]_B \in \mathbb{C}^n$. Nach der Eindeutigkeit der darstellenden Matrix folgt

$$A = C^H.$$

Also gilt $C = A^H$. □

Bemerkung 9.8.4 (Warum hier Orthonormalbasen stehen)**.** Die Aussage des Lemmas gilt im Allgemeinen nicht für beliebige Basen. In einer beliebigen Basis $(c_1, \ldots, c_n)$ muss zusätzlich die sogenannte Gram-Matrix des Skalarprodukts berücksichtigt werden. Diese ist die Matrix die an Stelle (i, j) den Eintrag $\langle c_i, c_j \rangle$ hat. Für Orthonormalbasen ist diese Gram-Matrix die Einheitsmatrix. Genau deshalb ist für den Spektralsatz die Sprache der Orthonormalbasen natürlich.

Lemma 9.8.5 (Kommutieren und Matrixdarstellungen)**.** *Seien $F, G : V \to V$ Endomorphismen eines endlich-dimensionalen Vektorraums, und sei B eine Basis von V. Setze*

$$A := M_{B \leftarrow B}(F) \quad \textit{und} \quad D := M_{B \leftarrow B}(G).$$

Dann gilt

$$FG = GF \quad \Longleftrightarrow \quad AD = DA.$$

Beweis. Die Matrix von FG bezüglich B ist AD. Die Matrix von GF bezüglich B ist DA. Da eine Matrixdarstellung bezüglich einer festen Basis eindeutig ist, folgt die Behauptung. □

Korollar 9.8.6 (Matrixform normaler Endomorphismen)**.** *Sei $F : V \to V$ ein Endomorphismus eines endlich-dimensionalen unitären Vektorraums, und sei B eine Orthonormalbasis von V. Setze*

$$A := M_{B \leftarrow B}(F).$$

Dann gilt

$$F \textit{ ist normal} \quad \Longleftrightarrow \quad A^H A = A A^H.$$

Beweis. Nach Lemma 9.8.3 hat F^* bezüglich B die Matrix A^H. Die Matrix von F^*F bezüglich B ist also $A^H A$. Die Matrix von FF^* bezüglich B ist AA^H. Die Behauptung folgt also aus Lemma 9.8.5. □

Lemma 9.8.7 (Konjugation erhält Kommutativität)**.** *Seien $A, D \in M_n(\mathbb{C})$, und sei $S \in \mathrm{GL}(n, \mathbb{C})$. Gilt*

$$AD = DA,$$

dann gilt auch

$$(S^{-1}AS)(S^{-1}DS) = (S^{-1}DS)(S^{-1}AS).$$

Beweis. Wir rechnen direkt:

$$(S^{-1}AS)(S^{-1}DS) = S^{-1}ADS = S^{-1}DAS = (S^{-1}DS)(S^{-1}AS). \qquad \square$$

Definition 9.8.8 (Unitäre Äquivalenz)**.** Zwei Matrizen $A, D \in M_n(\mathbb{C})$ heißen *unitär äquivalent*, wenn es eine unitäre Matrix $S \in U(n)$ gibt mit

$$D = S^H A S.$$

Da für unitäre Matrizen $S^{-1} = S^H$ gilt, ist dies die gewöhnliche Basiswechselformel für Endomorphismen, aber eingeschränkt auf Orthonormalbasen.

9.8.3 Eigenräume normaler Endomorphismen

Lemma 9.8.9 (Normgleichheit für normale Endomorphismen)**.** *Sei $F : V \to V$ normal. Dann gilt für alle $v \in V$*

$$\|F(v)\| = \|F^*(v)\|.$$

Beweis. Wir vergleichen die Quadrate der beiden Normen. Mit der Definition des adjungierten Endomorphismus gilt

$$\|F(v)\|^2 = \langle F(v), F(v)\rangle = \langle v, F^*F(v)\rangle.$$

Da F normal ist, gilt $F^*F = FF^*$. Also

$$\|F(v)\|^2 = \langle v, FF^*(v)\rangle.$$

Noch einmal mit der Definition des adjungierten Endomorphismus und $(T^*)^* = T$ (Lemma 9.7.7) erhalten wir

$$\langle v, FF^*(v)\rangle = \langle F^*(v), F^*(v)\rangle = \|F^*(v)\|^2.$$

Damit sind die Normen gleich. □

Lemma 9.8.10 (Eigenvektoren normaler Endomorphismen)**.** *Sei $F : V \to V$ normal, und sei $v \neq 0$ ein Eigenvektor von F zum Eigenwert λ. Dann ist v auch ein Eigenvektor von F^*, und zwar zum Eigenwert $\overline{\lambda}$:*

$$F^*(v) = \overline{\lambda} v.$$

Beweis. Setze

$$G := F - \lambda \operatorname{Id}.$$

Dann gilt

$$G^* = F^* - \overline{\lambda} \operatorname{Id}.$$

Außerdem ist G normal. Denn beim Ausmultiplizieren von G^*G und GG^* unterscheiden sich nur die Terme F^*F und FF^*, und diese sind gleich, weil F normal ist.

Da v ein Eigenvektor zum Eigenwert λ ist, gilt

$$G(v) = 0.$$

Nach dem vorherigen Lemma gilt für den normalen Endomorphismus G

$$\|G^*(v)\| = \|G(v)\| = 0.$$

Also ist $G^*(v) = 0$. Damit folgt

$$(F^* - \overline{\lambda} \operatorname{Id})(v) = 0,$$

also

$$F^*(v) = \overline{\lambda} v.$$

□

Korollar 9.8.11 (Orthogonalität verschiedener Eigenräume)**.** *Sei $F : V \to V$ normal. Eigenvektoren zu verschiedenen Eigenwerten sind orthogonal.*

Beweis. Seien u, v Eigenvektoren zu Eigenwerten λ und μ, wobei $\lambda \neq \mu$ gilt. Dann gilt

$$F(u) = \lambda u \quad \text{und} \quad F(v) = \mu v.$$

Nach dem vorherigen Lemma gilt außerdem

$$F^*(v) = \overline{\mu} v.$$

Damit rechnen wir

$$\lambda\langle u, v\rangle = \langle \lambda u, v\rangle = \langle F(u), v\rangle = \langle u, F^*(v)\rangle = \langle u, \overline{\mu} v\rangle = \mu\langle u, v\rangle.$$

Also gilt

$$(\lambda - \mu)\langle u, v\rangle = 0.$$

Da $\lambda \neq \mu$, folgt $\langle u, v\rangle = 0$. □

Lemma 9.8.12 (Orthogonales Komplement eines Eigenraums)**.** *Sei $F : V \to V$ normal, und sei λ ein Eigenwert von F. Setze*

$$U := \operatorname{Kern}(F - \lambda \operatorname{Id}).$$

Dann ist $U^\perp$ sowohl unter F als auch unter F^* invariant.

Beweis. Sei $v \in U^\perp$. Wir zeigen zuerst, dass $F(v) \in U^\perp$ gilt. Sei dazu $u \in U$. Dann ist u ein Eigenvektor von F zum Eigenwert λ, oder $u = 0$. In beiden Fällen gilt nach dem vorherigen Lemma

$$F^*(u) = \overline{\lambda} u.$$

Also

$$\langle F(v), u\rangle = \langle v, F^*(u)\rangle = \langle v, \overline{\lambda} u\rangle = \lambda\langle v, u\rangle = 0.$$

Da dies für alle $u \in U$ gilt, liegt $F(v)$ in $U^\perp$.

Nun zeigen wir, dass auch $F^*(v) \in U^\perp$ gilt. Sei wieder $u \in U$. Dann gilt

$$\langle F^*(v), u\rangle = \langle v, F(u)\rangle = \langle v, \lambda u\rangle = \overline{\lambda}\langle v, u\rangle = 0.$$

Also liegt auch $F^*(v)$ in $U^\perp$. □

Lemma 9.8.13 (Einschränkung auf das orthogonale Komplement)**.** *Sei $F : V \to V$ normal, sei λ ein Eigenwert von F, und sei*

$$U := \operatorname{Kern}(F - \lambda \operatorname{Id}), \quad O := U^\perp.$$

Dann ist die Einschränkung

$$F|_O : O \to O$$

wieder normal bezüglich des eingeschränkten Skalarprodukts.

Beweis. Nach dem vorherigen Lemma sind O sowohl unter F als auch unter F^* invariant. Damit sind

$$F|_O : O \to O \quad \text{und} \quad F^*|_O : O \to O$$

Endomorphismen von O. Für $x, y \in O$ gilt

$$\langle F|_O(x), y\rangle = \langle F(x), y\rangle = \langle x, F^*(y)\rangle = \langle x, F^*|_O(y)\rangle.$$

Also ist

$$(F|_O)^* = F^*|_O.$$

Für $x \in O$ folgt daher

$$(F|_O)^*(F|_O)(x) = F^*F(x) = FF^*(x) = (F|_O)(F|_O)^*(x).$$

Also ist $F|_O$ normal. □

9.8.4 Der Spektralsatz für normale Endomorphismen

Theorem 9.8.14 (Spektralsatz für normale Endomorphismen)**.** *Sei V ein endlich-dimensionaler unitärer Vektorraum, und sei $F : V \to V$ ein Endomorphismus. Dann sind äquivalent:*

1. *F ist normal.*
2. *V besitzt eine Orthonormalbasis aus Eigenvektoren von F.*

Beweis. Wir zeigen beide Richtungen.

ON-Eigenbasis impliziert Normalität. Angenommen, V besitzt eine Orthonormalbasis B aus Eigenvektoren von F. Dann ist die Matrix von F bezüglich B diagonal, also von der Form

$$D = \operatorname{diag}(\lambda_1, \dots, \lambda_n).$$

Hier bezeichnet $\operatorname{diag}(\lambda_1, \dots, \lambda_n)$ wieder die Matrix D mit $D_{i,i} = \lambda_i$ und $D_{i,j} = 0$ für $i \neq j$.

Nach Lemma 9.8.3 hat F^* bezüglich derselben Basis die Matrix

$$D^H = \operatorname{diag}(\overline{\lambda_1}, \dots, \overline{\lambda_n}).$$

Diagonale Matrizen kommutieren miteinander. Also gilt

$$D^H D = D D^H.$$

Nach Korollar 9.8.6 ist F normal.

Normalität impliziert ON-Eigenbasis. Wir beweisen die Aussage per Induktion über $n := \dim V$. Für $n = 0$ gibt es nichts zu zeigen. Sei also $n \geq 1$, und sei F normal.

Da V ein komplexer endlich-dimensionaler Vektorraum ist, besitzt das charakteristische Polynom von F nach dem Fundamentalsatz der Algebra eine Nullstelle. Da wir über dem zugrunde liegenden Körper $\mathbb{C}$ arbeiten, ist diese Nullstelle nach dem Eigenwertkriterium tatsächlich ein Eigenwert von F. Sei dieser Eigenwert λ. Setze

$$U := \operatorname{Kern}(F - \lambda \operatorname{Id}).$$

Dann ist $U \neq \{0\}$, und jeder Vektor in U ist ein Eigenvektor von F zum Eigenwert λ.

Wir wählen mit Gram-Schmidt eine Orthonormalbasis von U. Setze außerdem

$$O := U^\perp.$$

Nach dem vorherigen Lemma ist $F|_O : O \to O$ wieder normal. Da $U \neq \{0\}$ gilt, ist

$$\dim O < \dim V.$$

Nach Induktionsannahme besitzt O eine Orthonormalbasis aus Eigenvektoren von $F|_O$. Diese Vektoren sind zugleich Eigenvektoren von F.

Die Orthonormalbasis von U zusammen mit der Orthonormalbasis von O ist eine Orthonormalbasis von

$$V = U \oplus U^\perp.$$

Alle ihre Vektoren sind Eigenvektoren von F. Damit besitzt V eine Orthonormalbasis aus Eigenvektoren von F.

□

Korollar 9.8.15 (Matrixform des normalen Spektralsatzes)**.** *Für $A \in M_n(\mathbb{C})$ sind äquivalent:*

1. *A ist normal, das heißt*
$$A^H A = A A^H.$$
2. *A ist unitär äquivalent zu einer Diagonalmatrix. Das heißt: Es gibt ein $S \in U(n)$ mit*
$$S^H A S$$
diagonal.

Beweis. Wir betrachten den Endomorphismus

$$L_A : \mathbb{C}^n \to \mathbb{C}^n, \quad v \mapsto Av,$$

bezüglich des Standardskalarprodukts. Nach der Matrixform normaler Endomorphismen ist L_A genau dann normal, wenn $A^H A = A A^H$ gilt. Nach dem Spektralsatz besitzt L_A genau dann eine Orthonormalbasis aus Eigenvektoren, wenn L_A normal ist. Schreiben wir diese Orthonormalbasis als Spalten einer Matrix S, dann ist S unitär. Der Basiswechsel in diese ONB liefert

$$S^{-1} A S = S^H A S.$$

Diese Matrix ist genau dann diagonal, wenn die gewählte ONB aus Eigenvektoren besteht. □

Bemerkung 9.8.16 (Einordnung)**.** Der selbstadjungierte Spektralsatz ist ein Spezialfall des normalen Spektralsatzes. Ist $F = F^*$, dann ist F normal, also gibt es eine Orthonormalbasis aus Eigenvektoren. Zusätzlich sind im selbstadjungierten Fall alle Eigenwerte reell.

Normale Endomorphismen sind also die richtige komplexe Klasse für unitäre Diagonalisierbarkeit. Selbstadjungierte Endomorphismen sind die normale Klasse mit reellen Eigenwerten. Unitäre Endomorphismen bilden eine weitere wichtige Unterklasse: Ihre Eigenwerte liegen auf dem Einheitskreis.

Beispiel 9.8.17 (Eine nicht-normale Matrix)**.** Die Matrix

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{C})$$

ist nicht normal. Es ist

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

Daher gilt

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

Also ist

$$A^H A \neq A A^H.$$

Die Matrix A ist also nicht normal. Sie ist das kleinste typische Beispiel: Sie schiebt den ersten Basisvektor auf Null und den zweiten auf den ersten. Dieses einseitige Schieben passt nicht zu einer orthonormalen Diagonalisierung.

Bemerkung 9.8.18 (Wie normal ist „normal“?)**.** Der Begriff „normal“ klingt zunächst harmlos, ist aber eine starke Bedingung. Wählt man eine Matrix $A \in M_n(\mathbb{C})$ zufällig aus einer kontinuierlichen Verteilung, zum Beispiel indem man alle Real- und Imaginärteile der Einträge unabhängig und nach der Gleichverteilung aus $[0, 1]$ mit einer Dichte wählt, dann ist für $n \geq 2$ die Wahrscheinlichkeit

$$\mathbb{P}\,(A \text{ ist normal}) = 0.$$

Der Grund ist geometrisch: Normale Matrizen bilden nur eine dünne Teilmenge von $M_n(\mathbb{C})$. Nach dem Spektralsatz sind normale Matrizen genau die unitär diagonalisierbaren Matrizen. Eine solche Matrix wird also durch ihre Eigenwerte und eine orthonormale Eigenbasis beschrieben. Das sind deutlich weniger Freiheitsgrade als bei einer beliebigen komplexen Matrix.

Genauer hat $M_n(\mathbb{C})$ reelle Dimension $2n^2$. Normale Matrizen mit paarweise verschiedenen Eigenwerten haben reelle Dimension

$$2n + (n^2 - n) = n^2 + n.$$

Hierbei kommen $2n$ Freiheitsgrade von den Eigenwerten in $\mathbb{C}$, und $n^2 - n$ Freiheitsgrade von einer unitären Eigenbasis, wobei die Phasen der einzelnen Eigenvektoren die Matrix nicht ändern. Für $n \geq 2$ gilt

$$n^2 + n < 2n^2.$$

Normale Matrizen liegen also in einer Teilmenge kleinerer Dimension. Solche Teilmengen haben bezüglich des üblichen Volumenbegriffs Wahrscheinlichkeit Null.

Das heißt nicht, dass normale Matrizen selten im mathematischen Alltag sind. Im Gegenteil: Hermitesche Matrizen, unitäre Matrizen und Diagonalmatrizen sind alle normal. Aber innerhalb aller Matrizen sind normale Matrizen nicht generisch. Eine beliebige Matrix ist also fast nie normal, aber die wichtigsten strukturierten Matrizen sind es sehr oft.

Anhang A

Noether, Mathematik und Geschichte

Die Mathematik und Physik trieb die politischen und gesellschaftlichen Umwälzungen im 19. und 20. Jahrhundert mit an und wurde von ihnen auch beeinflusst. Im Kaiserreich und der Weimarer Republik war Göttingen eines der Hauptzentren der mathematischen Welt. Dort machte weder der wissenschaftliche Fortschritt noch die Emanzipation der Frau halt. Aus dieser Zeit stammt auch eine oft zitierte Anekdote über David Hilbert. Als man ihn fragte, was er davon halte, dass Frauen zur Habilitation zugelassen werden sollten, antwortete er sinngemäß „*Meine Herren, eine Fakultät ist doch kein Badehaus.*“ um die willkürliche Diskriminierung deutlich zu machen.

Die gesellschaftlichen und wissenschaftlichen Entwicklungen jener Zeit wurden jedoch durch den Terror der nationalsozialistischen Herrschaft jäh unterbrochen. Durch die Verfolgung[1] , Vertreibung[2] und Vernichtung[3] insbesondere jüdischer Wissenschaftlerinnen und Wissenschaftler verlor die deutsche Mathematik innerhalb weniger Jahre einen erheblichen Teil ihrer Substanz. Die mathematische Gemeinschaft war aber nicht ausschließlich Opfer sondern umfasste auch Täter.[4]

Diese Zäsur wirkte weit über ihre Zeit hinaus und veränderte die internationale Wissenschaftslandschaft nachhaltig. Auch die moderne Mathematik und Physik selbst waren ideologischen Angriffen ausgesetzt, da die theoretischen Umwälzungen politisch diffamiert und abgelehnt wurden.[5]

[1] Zu nennen sind hier viele Namen, darunter Edmund Landau:
Er war eine der Größen der analytischen Zahlentheorie. 1933 wurde er Opfer eines (von dem Mathematiker Oswald Teichmüller angeführten) Boykotts. 1934 wurde er aufgrund antisemitscher Gesetze in den vorzeitigen Ruhestand versetzt. Sowohl der Name Landau (z.B. in der sogenannten Landau-Notation oder auch Groß-O-Notation) als auch der Name Teichmüller (in der sogenannten Teichmüller-Theorie) werden einer Physikerin im Laufe ihres Studiums mit hoher Wahrscheinlichkeit begegnen. Siehe https://de.wikipedia.org/wiki/Edmund_Landau.

[2] Auch hier sind viele Namen zu nennen, ich greife Hilda Geiringer heraus. Sie studierte Mathematik und wurde 1928 die erste deutsche Privatdozentin für angewandte Mathematik. 1933 wurde sie als Jüdin entlassen und ging zunächst nach Istanbul, dann in die USA. Dort forschte sie bis zu ihrem Tod 1973 erfolgreich in Statistik und Elastizitätstheorie. Siehe https://de.wikipedia.org/wiki/Hilda_Geiringer.

[3] Hier greife ich aus den vielen Namen Felix Hausdorff heraus. Er war Mitbegründer des Forschungsfeldes der allgemeinen Topologie, welches sowohl die Mathematik als auch die Physik revolutionierte. Unter dem Pseudonym Paul Mongré verfasste er auch literatische und philosophische Werke. Er versuchte vergeblich zu emigrieren und wurde 1942 von den Nazis in den Suizid getrieben. Er fand keinen anderen Ausweg, um der unmittelbar bevorstehenden Deportation in ein KZ zu entgehen. Siehe https://de.wikipedia.org/wiki/Felix_Hausdorff.

[4] Hier sind unter anderem der bereits genannte Oswald Teichmüller (bereits 1931 Mitglied in NSDAP und SA) als auch Ludwig Bieberbach zu nennen. Bieberbach engagierte sich insbesondere in der ideologisch und rassistisch begründeten Gegenüberstellung der sogenannten „Deutschen Mathematik“ (siehe https://de.wikipedia.org/wiki/Deutsche_Mathematik) und sogenannter „jüdischer Mathematik“. Im Rahmen dieser Gegenüberstellung wertete er große Teile des mathematischen Fortschritts (insbesondere in abstrakten Gebieten) als vermeintliches Zeichen von Schwäche und Degeneration ab.

[5] Siehe https://de.wikipedia.org/wiki/Deutsche_Physik und https://de.wikipedia.org/wiki/Deutsche_Mathematik.

Dies unterbrach, erschwerte und bremste den Fortschritt, konnte ihn aber nicht aufhalten. Ein bis heute spürbarer Effekt ist die Verschiebung der Zentren der mathematischen Entwicklung in die USA, Großbritannien und die ehemalige Sowjetunion.

Eine besonders eindrucksvolle Verbindung zwischen den physikalischen Revolutionen – sowohl der Quantenmechanik als auch der allgemeinen Relativitätstheorie – und der mathematischen Revolution der abstrakten Algebra findet sich in der Mathematikerin Emmy Noether (1882 bis 1935).

Noether trug nicht nur wesentlich zur Entstehung und Entwicklung der abstrakten Algebra bei, sondern bewies mit dem Noether-Theorem[6] ein tiefes Resultat der theoretischen Physik, das die fundamentale Verbindung zwischen Symmetrien und Erhaltungsgrößen offenlegt.

In der Hoffnung, dass die Biographie dieser bemerkenswerten Wissenschaftlerin – die trotz struktureller Hindernisse und unter schwierigen historischen Umständen Außergewöhnliches geleistet hat – als Inspiration dienen kann, sei hier auf einige Aspekte ihres Lebens hingewiesen.[7]

Im Kontext der Entwicklung der allgemeinen Relativitätstheorie wandten sich David Hilbert und Felix Klein mit einem strukturellen Problem an Emmy Noether: Die damals neu formulierten physikalischen Gleichungen schienen mit den klassischen Erhaltungssätzen (insbesondere der Energieerhaltung) in Spannung zu stehen. Noether erkannte, dass dieses Problem kein physikalischer Widerspruch, sondern Ausdruck einer tieferen mathematischen Struktur war. Ihre Antwort bestand in einem heute als Noether-Theorem bekannten allgemeinen Prinzip: Jede kontinuierliche Symmetrie eines physikalischen Systems führt zu einer Erhaltungsgröße und umgekehrt. Da die allgemeine Relativitätstheorie nicht die gleichen globalen Symmetrien besitzt wie etwa die Newtonsche Mechanik, nehmen die klassischen Erhaltungssätze dort eine verallgemeinerte Form an. Damit wurde nicht nur das konkrete Problem geklärt, sondern ein grundlegender Zusammenhang zwischen Symmetrie und Physik freigelegt.

Trotz ihrer Leistungen erhielt sie nie eine ordentliche Professur. Auch die Fürworte von damals etablierten und geschätzten Größen wie dem bereits genannten Hilbert konnten das nicht ändern. Noether öffnete aber die Tür für Frauen die ihr später folgen sollten: 1922 wurde ihr der Titel „nicht beamteter außerordentlicher Professor“ verliehen. Damit war sie die erste Frau in Deutschland, die überhaupt einen Professorentitel trug. Bezahlt wurde sie für ihre Professur nicht. Auch ihre Lehraufträge wurden nur sehr gering bezahlt.

Als Jüdin wurde sie während der nationalsozialistischen Herrschaft verfolgt und ihrer akademischen Position beraubt.

Sie galt als unprätentiös, warmherzig und zutiefst dem gemeinsamen Denken verpflichtet. Mathematik erschien bei ihr weniger als individuelles Prestigeprojekt, sondern als kollektives Unternehmen, das vom offenen Austausch lebt. Auch unter zunehmend schwierigen politischen Bedingungen blieb sie diesem Ideal treu. Nach ihrer Entlassung aus dem Universitätsdienst hielt sie weiterhin Vorlesungen in kleinerem Rahmen und unterstützte Studierende, die den Zugang zur akademischen Lehre verloren hatten. Diese Form der gelebten wissenschaftlichen Gemeinschaft zeugt von einem tiefen humanistischen Verständnis von Bildung und Wissenschaft. Sie emigrierte schließlich in die USA wo sie ihre Lehre und Forschung fortsetzte.

[6] https://de.wikipedia.org/wiki/Noether-Theorem

[7] Mehr findet man beispielsweise auf Wikipedia: https://de.wikipedia.org/wiki/Emmy_Noether

Anhang B

Kommutativität und Assoziativität

In algebraischen Strukturen definieren wir meistens nur sehr lokale Regeln. Das hat einen guten Grund. Eine Regel soll einfach überprüfbar sein. Es wäre zum Beispiel kaum praktikabel, in der Definition einer Verknüpfung zu verlangen, dass alle möglichen Klammerungen von fünf, zehn oder hundert Faktoren denselben Wert liefern. Ebenso wäre es unhandlich, in der Definition von Kommutativität direkt alle möglichen Umordnungen beliebig langer Produkte aufzunehmen.

Stattdessen macht man etwas Eleganteres. Man formuliert eine kleine lokale Regel, die leicht zu überprüfen ist. Danach beweist man einen Satz, der zeigt, dass aus dieser lokalen Regel die gewünschte globale Freiheit folgt. Genau dieser Übergang wird in Rechnungen oft verschluckt, weil er intuitiv plausibel wirkt. Mathematisch steckt darin aber eine kleine, sehr schöne Strukturgeschichte.

Für die Assoziativität ist die lokale Regel

$$(a * b) * c = a * (b * c).$$

Diese Regel betrifft nur drei benachbarte Blöcke. Daraus folgt nicht unmittelbar, dass man bei beliebig vielen Faktoren jede Klammerung weglassen darf. Dafür ist ein weiteres Argument nötig. Die entsprechende Aussage ist ein eigener Satz, der oft *allgemeines Assoziativgesetz* genannt wird.

Für die Kommutativität ist die lokale Regel

$$a * b = b * a.$$

Auch diese Regel betrifft zunächst nur zwei Faktoren. In einem langen Produkt ist damit zunächst nur klar, dass zwei benachbarte Faktoren vertauscht werden dürfen, sobald die Klammerungsfrage geklärt ist. Dass daraus jede beliebige Umordnung folgt, ist ebenfalls ein eigener kombinatorischer Satz.

Die beiden Situationen sind also parallel:

lokale Regel	erlaubter lokaler Schritt	globaler Satz
Assoziativität	drei Blöcke umklammern	jede Klammerung hat gleichen Wert
Kommutativität	zwei benachbarte Faktoren tauschen	jede Umordnung hat gleichen Wert

Wir behandeln zuerst die Kommutativität, weil der zugrunde liegende kombinatorische Mechanismus sehr anschaulich ist. Danach kehren wir zur Assoziativität zurück. Dort sind die Objekte nicht mehr bloß Listen, sondern kompliziertere Objekte: sogenannte Klammerungsbäume.

B.1 Benachbarte Vertauschungen

Wir betrachten zunächst nur Listen. Für ein $n \geqslant 1$ sei eine Liste im Folgenden eine Folge

$$L = (x_1, x_2, \dots, x_n),$$

in der jede Zahl aus $\{1, \dots, n\}$ genau einmal vorkommt. Dabei interpretieren wir $x_i = k$ als „An der i-ten Stelle steht nun das was an der ursprünglich k-ten Stelle stand“.

Die Frage ob aus dem lokalen Kommutativitätsgesetz die globale Freiheit die Reihenfolge beliebig zu wählen folgt können wir nun auch anders stellen:

- können wir beliebige Sortierungen durch das Vertauschen benachbarter Einträge erhalten?
- Oder noch präziser: Kann man jede solche Liste aus der sortierten Liste

$$(1, 2, \dots, n)$$

  durch Vertauschungen benachbarter Einträge herstellen?

Diese zur Frage stehende Aussage ist etwas stärker als die Tatsache, dass jede Permutation ein Produkt von Transpositionen ist. Eine Transposition darf zwei beliebige Stellen vertauschen. Hier erlauben wir zunächst nur die benachbarten Vertauschungen

$$\begin{pmatrix} 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 3 \end{pmatrix}, \dots, \begin{pmatrix} n-1 & n \end{pmatrix}.$$

Wichtig ist dabei: „benachbart“ bezieht sich auf die Positionen in der jeweils aktuellen Liste, nicht auf die Zahlenwerte der Einträge. Wenn also gerade die Liste

$$(3, 1, 4, 2)$$

vorliegt, dann dürfen wir zum Beispiel die benachbarten Einträge 3 und 1 vertauschen, oder die benachbarten Einträge 4 und 2. Nicht gemeint ist, dass nur Zahlenwerte wie 1 und 2 oder 2 und 3 vertauscht werden dürften.

Der folgende Satz sagt, dass selbst diese wenigen Vertauschungen ausreichen.

Theorem B.1.1 (Benachbarte Vertauschungen genügen)**.** *Jede Liste, in der jede Zahl aus* $\{1, \dots, n\}$ *genau einmal vorkommt, kann durch endlich viele Vertauschungen benachbarter Einträge in die sortierte Liste*

$$(1, 2, \dots, n)$$

gebracht werden. Umgekehrt kann jede solche Liste aus der sortierten Liste durch endlich viele Vertauschungen benachbarter Einträge hergestellt werden.

Beweis. Wir verwenden die Idee von `BubbleSort`.

Ist $n = 1$, so ist nichts zu zeigen. Sei also $n \geqslant 2$. Wir durchlaufen die Liste von links nach rechts. Dabei betrachten wir nacheinander die benachbarten Paare

$$(x_1, x_2), \dots, (x_{n-2}, x_{n-1}), (x_{n-1}, x_n).$$

Immer wenn das linke Element größer ist als das rechte, vertauschen wir diese beiden benachbarten Einträge.

Wir behaupten: Nach diesem Durchlauf steht der Eintrag mit dem Wert n an der letzten Stelle. Denn solange die n nicht ganz rechts steht, liegt rechts neben ihr ein kleinerer Eintrag. Wenn dieses Paar im Durchlauf erreicht wird, wird die n um eine Stelle nach rechts vertauscht. Da der Durchlauf von links nach rechts geht, kann die n dadurch Schritt für Schritt bis an das Ende wandern. Am Ende steht also die n ganz rechts.

Nun betrachten wir die restliche Teilliste links von der n. Sie enthält genau die Zahlen

$$1, 2, 3, \dots, n-1.$$

Wenden wir denselben Vorgang auf diese Teilliste an, so wandert die $n-1$ an die zweitletzte Stelle. Danach wenden wir denselben Vorgang auf die verbleibende Teilliste an, und so weiter. Nach endlich vielen Schritten erhalten wir die sortierte Liste

$$(1, 2, \dots, n).$$

Für die umgekehrte Richtung beachten wir: Jede benachbarte Vertauschung ist ihre eigene Umkehrung. Wenn also eine Folge benachbarter Vertauschungen eine Liste L in die sortierte Liste bringt, dann bringt dieselbe Folge rückwärts gelesen die sortierte Liste wieder in L. □

Bemerkung B.1.2. Dieser Beweis ist ein Terminierungsbeweis in verkleideter Form. Nach jedem vollständigen Durchlauf ist mindestens ein weiterer Endteil der Liste endgültig sortiert. Das Problem wird also immer kleiner.

Bemerkung B.1.3 (Permutationen und Listen)**.** An dieser Stelle ist es wichtig, zwei verschiedene Ebenen sauber zu unterscheiden.

Eine Permutation

$$\sigma \in S_n$$

ist zunächst keine Liste, sondern eine Bijektion

$$\sigma : \{1, \dots, n\} \to \{1, \dots, n\}.$$

Sie beschreibt also eine Umordnung der Positionen

$$1, \dots, n.$$

Eine Liste dagegen ist ein Tupel

$$L = (x_1, \dots, x_n).$$

Die symmetrische Gruppe S_n wirkt auf solchen Listen, indem die Positionen umgeordnet werden.

Genauer: Eine Permutation $\sigma \in S_n$ wirkt auf einer Liste

$$(x_1, \dots, x_n)$$

durch

$$(x_1, \dots, x_n) \mapsto (x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)}).$$

Die neue Liste entsteht also dadurch, dass die Einträge an den Positionen gemäß σ umgeordnet werden.

Das Inverse σ^{-1} erscheint hier aus technischen Gründen. Es sorgt dafür, dass die Hintereinanderausführung von Permutationen mit der Hintereinanderausführung ihrer Wirkungen auf Listen übereinstimmt. Ohne das Inverse würden sich die Reihenfolgen der Kompositionen vertauschen.

Die Transposition

$$\begin{pmatrix} 1 & 2 \end{pmatrix}$$

vertauscht deshalb nicht die Zahlenwerte 1 und 2, sondern die Einträge an den Positionen 1 und 2. So wird zum Beispiel

$$(7, 42, 99)$$

zu

$$(42, 7, 99).$$

Wichtig ist dabei: Die Transposition

$$\begin{pmatrix} i & i+1 \end{pmatrix}$$

tauscht immer die aktuell benachbarten Positionen i und $i+1$. Wir müssen also nicht verfolgen, wohin ein bestimmter Eintrag im Laufe vieler Vertauschungen gewandert ist. Die Operation bezieht sich immer nur auf die momentanen Positionen in der aktuellen Liste.

Die benachbarten Transpositionen

$$\begin{pmatrix}1 & 2\end{pmatrix}, \begin{pmatrix}2 & 3\end{pmatrix}, \ldots, \begin{pmatrix}n-1 & n\end{pmatrix}$$

erzeugen die ganze symmetrische Gruppe S_n. Unsere eigentliche Behauptung lautet also: Jede Permutation kann als Hintereinanderausführung benachbarter Transpositionen geschrieben werden.

Dadurch folgt, dass jede Umordnung einer Liste durch endlich viele Vertauschungen benachbarter Positionen erreicht werden kann. Dies ist die algebraische Struktur hinter Verfahren wie BubbleSort.

Man sagt: „Die Wirkung von S_n auf den Listen ist transitiv." Damit ist gemeint, dass man jede Liste aus jeder anderen durch geeignete Permutationen erreichen kann. Da die benachbarten Transpositionen bereits ganz S_n erzeugen, genügen dafür schon diese einfachen lokalen Vertauschungen.

Korollar B.1.4. *Jede Liste die genau aus den Zahlen $\{1, \ldots, n\}$ ohne Wiederholungen besteht, entsteht aus der Ausgangsreihenfolge*

$$(1, 2, \ldots, n)$$

durch endlich viele Vertauschungen benachbarter Einträge.

In anderen Worten: für jede Permutation $\sigma \in S_n$ entsteht die Liste $(\sigma(1), \ldots, \sigma(n))$ aus der nicht-permutierten Liste

$$(1, 2, \ldots, n)$$

durch endlich viele Vertauschungen benachbarter Einträge.

Beweis. Die Behauptung ist die zweite Aussage von Theorem B.1.1. □

Bemerkung B.1.5 (Gruppentheoretische Sprache)**.** In der Sprache der symmetrischen Gruppe sagt das Korollar: Die Gruppe S_n wird von den benachbarten Transpositionen

$$s_i = \begin{pmatrix}i & i+1\end{pmatrix}, \qquad 1 \leqslant i < n,$$

erzeugt. Hierbei sollte man s_i als Vertauschung der beiden benachbarten Positionen i und $i+1$ lesen. Nach einigen Vertauschungen können an diesen Positionen natürlich ganz andere Zahlenwerte stehen.

Hier sieht man einen ersten Zusammenhang zwischen elementarer Algebra und Kombinatorik. Die lokale Operation ist das Vertauschen zweier benachbarter Positionen in der jeweils aktuellen Liste. Die globale Aussage ist, dass daraus alle Permutationen entstehen.

B.2 Anwendung auf kommutative Produkte

Nun übertragen wir den kombinatorischen Satz zurück auf Produkte. Dafür nehmen wir vorläufig an, dass die Klammerungsfrage bereits durch das allgemeine Assoziativgesetz geklärt ist. Dieses Gesetz beweisen wir im nächsten Abschnitt.

Theorem B.2.1 (Reihenfolge in endlichen kommutativen Produkten)**.** *Sei M eine Menge mit einer assoziativen und kommutativen Verknüpfung $*$. Sei $n \geqslant 1$. Seien $a_1, \ldots, a_n \in M$ und sei $\pi \in S_n$. Dann gilt*

$$a_1 * a_2 * \ldots * a_n = a_{\pi(1)} * a_{\pi(2)} * \ldots * a_{\pi(n)}.$$

Beweis. Nach dem allgemeinen Assoziativgesetz dürfen wir die Klammerung weglassen. Wegen der Kommutativität dürfen wir zwei benachbarte Faktoren vertauschen, ohne den Wert des Produkts zu verändern. Genauer: In einem Produkt

$$a_1 * \ldots * a_i * a_{i+1} * \ldots * a_n$$

dürfen wir durch geeignete Klammerung die beiden benachbarten Faktoren a_i und a_{i+1} vertauschen. Genauer gesagt dürfen wir die folgende kombinierte Umformung machen.

$$\begin{aligned} & a_1 * \ldots * a_i * a_{i+1} * \ldots * a_n \\ \text{Assoziativität} \quad & = a_1 * \ldots * (a_i * a_{i+1}) * \ldots * a_n \\ \text{Kommutativität} \quad & = a_1 * \ldots * (a_{i+1} * a_i) * \ldots * a_n \\ \text{Assoziativität} \quad & = a_1 * \ldots * a_{i+1} * a_i * \ldots * a_n \,. \end{aligned}$$

Damit erhalten wir

$$a_1 * \ldots * a_i * a_{i+1} * \ldots * a_n = a_1 * \ldots * a_{i+1} * a_i * \ldots * a_n.$$

Nach dem vorherigen Korollar entsteht die Reihenfolge

$$\pi(1), \pi(2), \ldots, \pi(n)$$

aus der Reihenfolge

$$1, 2, \ldots, n$$

durch endlich viele Vertauschungen benachbarter Einträge. Jede einzelne dieser Vertauschungen ändert den Wert des Produkts nicht. Also ändert auch die ganze Umordnung den Wert des Produkts nicht. □

Bemerkung B.2.2. Die Aussage „In kommutativen Strukturen ist die Reihenfolge egal“ ist also kein zusätzliches Axiom für beliebig lange Produkte. Sie ist ein Satz. Sie folgt aus drei Bausteinen:

1. dem allgemeinen Assoziativgesetz, das das Weglassen von Klammern rechtfertigt;
2. der binären Kommutativität, die das Vertauschen zweier benachbarter Faktoren erlaubt;
3. dem kombinatorischen Satz, dass benachbarte Vertauschungen jede beliebige Umordnung erzeugen.

B.3 Das allgemeine Assoziativgesetz

Wir kommen nun zur Klammerungsfrage zurück. Die lokale Regel der Assoziativität lautet nur

$$(a * b) * c = a * (b * c).$$

Sie erlaubt also eine lokale Umklammerung von drei benachbarten Blöcken. Die globale Aussage, die wir im Alltag ständig verwenden, ist stärker: Alle vollständigen Klammerungen eines endlichen Ausdrucks sollen denselben Wert liefern.

Um diese Aussage präzise zu beweisen, wählen wir eine Normalform. Für $a_1, \ldots, a_n \in M$ sei die *linksassoziative Normalform* rekursiv definiert durch

$$L_1(a_1) = a_1$$

und

$$L_{n+1}(a_1, \dots, a_{n+1}) = L_n(a_1, \dots, a_n) * a_{n+1}.$$

Also ist zum Beispiel

$$L_4(a_1, a_2, a_3, a_4) = (((a_1 * a_2) * a_3) * a_4).$$

Die Idee des Beweises ist: Wir vergleichen nicht jede Klammerung direkt mit jeder anderen. Stattdessen zeigen wir, dass jede vollständige Klammerung denselben Wert wie die linksassoziative Normalform hat. Dann sind automatisch je zwei vollständige Klammerungen gleich, weil beide gleich derselben Normalform sind.

Dieses Normalformargument ist derselbe Denktyp wie oben bei den benachbarten Vertauschungen. Dort wurde jede Liste durch erlaubte lokale Schritte in die sortierte Liste gebracht. Hier wird jede Klammerung durch erlaubte lokale Umklammerungen in eine feste Klammerungsform gebracht. Die lokalen Schritte sind wieder invertierbar: Die Regel

$$(A * B) * C = A * (B * C)$$

kann in beide Richtungen verwendet werden. Nur operiert sie diesmal nicht auf der Reihenfolge der Blätter, sondern auf der Form der Klammerung.

Lemma B.3.1. *Sei M eine Menge mit einer assoziativen Verknüpfung $*$. Für alle $k, m \geqslant 1$ und alle $a_1, \dots, a_{k+m} \in M$ gilt*

$$L_k(a_1, \dots, a_k) * L_m(a_{k+1}, \dots, a_{k+m}) = L_{k+m}(a_1, \dots, a_{k+m}).$$

Beweis. Wir beweisen die Aussage durch Induktion über m. Für $m = 1$ ist die Aussage gerade die Definition der linksassoziativen Normalform:

$$L_k(a_1, \dots, a_k) * a_{k+1} = L_{k+1}(a_1, \dots, a_{k+1}).$$

Sei nun $m \geqslant 1$, und die Aussage sei für m bekannt. Dann gilt

$$\begin{aligned} &L_k(a_1, \dots, a_k) * L_{m+1}(a_{k+1}, \dots, a_{k+m+1}) \\ &\qquad = L_k(a_1, \dots, a_k) * \big(L_m(a_{k+1}, \dots, a_{k+m}) * a_{k+m+1}\big) \\ &\qquad = \big(L_k(a_1, \dots, a_k) * L_m(a_{k+1}, \dots, a_{k+m})\big) * a_{k+m+1} \\ &\qquad = L_{k+m}(a_1, \dots, a_{k+m}) * a_{k+m+1} \\ &\qquad = L_{k+m+1}(a_1, \dots, a_{k+m+1}). \end{aligned}$$

Dabei haben wir im zweiten Schritt die Assoziativität rückwärts verwendet. □

Theorem B.3.2 (Allgemeines Assoziativgesetz)**.** *Sei M eine Menge mit einer assoziativen Verknüpfung $*$. Dann haben alle vollständigen Klammerungen eines Ausdrucks*

$$a_1 * a_2 * \dots * a_n$$

denselben Wert. Insbesondere ist die Schreibweise

$$a_1 * a_2 * \dots * a_n$$

ohne Klammern wohldefiniert.

Beweis. Wir zeigen durch Induktion über n, dass jede vollständige Klammerung von $a_1, \dots, a_n$ den Wert

$$L_n(a_1, \dots, a_n)$$

hat. Für $n = 1$ ist nichts zu zeigen.

Sei nun $n \geqslant 2$, und die Aussage sei für kürzere Listen bekannt. Jede vollständige Klammerung von

$$a_1, \dots, a_n$$

hat außen die Form

$$P * Q,$$

wobei P eine vollständige Klammerung der ersten k Einträge

$$a_1, \dots, a_k$$

und Q eine vollständige Klammerung der restlichen $n - k$ Einträge

$$a_{k+1}, \dots, a_n$$

ist. Hierbei gilt $1 \leqslant k < n$.

Nach Induktionsvoraussetzung gilt

$$P = L_k(a_1, \dots, a_k)$$

und

$$Q = L_{n-k}(a_{k+1}, \dots, a_n).$$

Mit dem vorherigen Lemma folgt daher

$$P * Q = L_k(a_1, \dots, a_k) * L_{n-k}(a_{k+1}, \dots, a_n) = L_n(a_1, \dots, a_n).$$

Also ist jede vollständige Klammerung gleich der linksassoziativen Normalform. Damit sind je zwei vollständige Klammerungen gleich. □

B.4 Klammerungen als Bäume

Es gibt eine strukturelle Sicht, die die Parallele zur Kommutativität besonders gut sichtbar macht. Eine vollständige Klammerung kann man als binären Baum auffassen. Die Blätter sind die Faktoren. Jeder innere Knoten steht für eine Anwendung der Verknüpfung $*$.

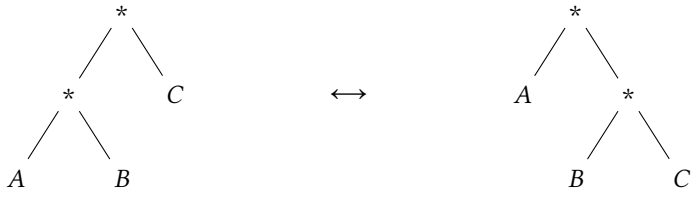
Zum Beispiel entspricht

$$(a * b) * c$$

einem Baum, bei dem zuerst a und b verknüpft werden, und danach das Ergebnis mit c verknüpft wird. Der Ausdruck

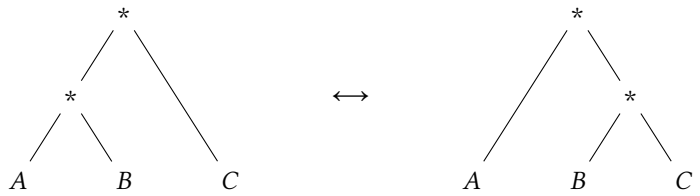
$$a * (b * c)$$

entspricht einem anderen Baum. Die Assoziativitätsregel sagt genau, dass die folgende lokale Baumrotation den Wert nicht ändert:

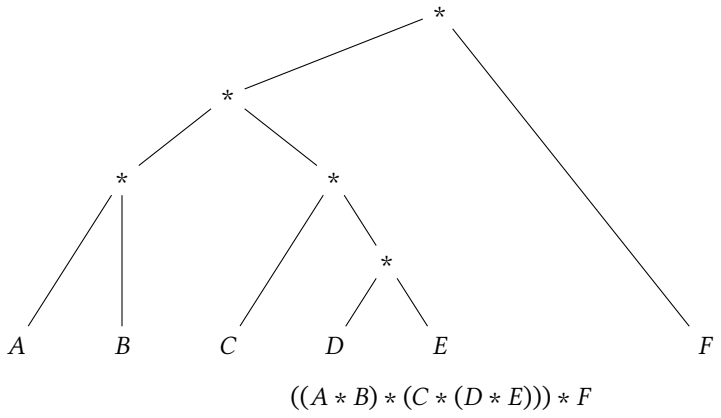


$(A * B) * C$ $\qquad$ $A * (B * C)$

Wir können die Blätter auch alle auf die selbe Höhe zeichnen und erhalten dann



Wir können auch größere Klammerungen so darstellen:



Das allgemeine Assoziativgesetz sagt dann: Alle binären Bäume mit denselben Blättern in derselben Reihenfolge liefern denselben Wert. Man kann also jede Klammerung durch lokale Baumrotationen in die linksassoziative Normalform bringen.

Damit entsteht die präzise Analogie:

Situation	Objekte	lokale Erzeug
Kommutativität	Listen der Blätter	benachbarte Vertaus
Assoziativität	binäre Klammerungsbäume	Baumrotation

Bei der Kommutativität betrachten wir also, wie die symmetrische Gruppe die Blätter umsortiert. Der Satz über benachbarte Vertauschungen sagt, dass diese Gruppe bereits durch sehr einfache lokale Vertauschungen erzeugt wird.

Bei der Assoziativität bleiben die Blätter in derselben Reihenfolge. Dafür ändern wir die Gestalt des Klammerungsbaums. Das allgemeine Assoziativgesetz sagt, dass alle diese Gestalten durch lokale Rotationen miteinander verbunden sind, und dass jede solche Rotation den Wert des Ausdrucks unverändert lässt.

Bemerkung B.4.1. Die Alltagssätze „Klammern sind egal“ und „die Reihenfolge ist egal“ sind also keine bloßen Konventionen. Sie sind globale Folgerungen aus lokalen Regeln.

In kurzer Form:

lokale Regel	globale Konsequenz
$(a * b) * c = a * (b * c)$	alle endlichen Klammerungen sind gleich
$a * b = b * a$	alle endlichen Umordnungen sind gleich

Die lokalen Regeln sind die Definitionen. Die globalen Freiheiten sind Sätze.