Wolfgang K. Seiler

Höhere Mathematik I

Vorlesung an der Universität Mannheim
im Sommersemester 2006

Dieses Skriptum entsteht parallel zur Vorlesung und soll mit möglichst geringer Verzögerung erscheinen. Es ist daher in seiner Qualität auf keinen Fall mit einem Lehrbuch zu vergleichen; insbesondere sind Fehler bei dieser Entstehensweise nicht nur möglich, sondern **sicher**. Dabei handelt es sich wohl leider nicht immer nur um harmlose Tippfehler, sondern auch um Fehler bei den mathematischen Aussagen.

Das Skriptum sollte daher mit Sorgfalt und einem gewissen Mißtrauen gegen seinen Inhalt gelesen werden; falls Sie Fehler finden, teilen Sie mir dies bitte persönlich oder per e-mail (seiler@math.uni-mannheim.de) mit, oder informieren Sie Ihren Übungsgruppenleiter. Auch wenn Sie Teile des Skriptums unverständlich finden, bin ich für entsprechende Hinweise dankbar.

Falls genügend viele Hinweise eingehen, werde ich von Zeit zu Zeit Listen mit Berichtigungen und Verbesserungen zusammenstellen.

Einleitung

Die Vorlesung *Höhere Mathematik* soll Ihnen helfen, das für Ihren Studiengang (Technische Informatik *bzw.* Software- und Internettechnologie) notwendige mathematische Rüstzeug zu erwerben.

Im Vordergrund steht somit die Mathematik als Werkzeug.

Den Umgang mit einem Werkzeug lernt man nur durch dessen Gebrauch: Niemand wird zum Schlosser, indem er Bilder von Bohrmaschinen betrachtet und Abhandlungen über das Drehmoment liest, und niemand, der einfach mathematische Formeln und Sätze auswendig lernt, wird damit erfolgreich Probleme der Informatik lösen.

Zum einen beginnen Probleme der Informatik nie mit „$f : \mathbb{R}^3 \to \mathbb{R}$ sei eine mindestens zweimal stetig differenzierbare Funktion“ oder etwas ähnlichem; der Anwender muß sich stets zunächst überlegen, ob sich sein Problem überhaupt mit Mathematik lösen läßt, und wenn ja, mit welcher.

Die Antwort darauf wird selten eindeutig sein: Gelegentlich wird sich dasselbe Problem sowohl mit als auch ohne Mathematik modellieren lassen, und auch wenn man sich für eine mathematische Lösung entscheidet, steht selten eindeutig fest, wie es weiter geht:

Realistische Probleme (im Gegensatz zu Übungs- und Klausuraufgaben) sind fast immer zu komplex, als daß man sie vollständig formal beschreiben könnte. Vor ihrer Übersetzung in Mathematik muß man sie daher vereinfachen und dabei versuchen, die für die jeweilige Problemstellung wesentlichen Eigenschaften trotzdem zu erhalten. Beispielsweise wird man oft Größen, die ihrem Wesen nach ganzzahlig sind, mit reelle Zahlen modellieren, da die Mathematik der reellen Zahlen erheblich

einfacher ist als die der ganzen Zahlen und auch deutlich mehr Methoden zur Verfügung stellt. Bei der Informationsübertragung etwa ist die Anzahl übertragener Bits stets ganzzahlig, aber bei den Größenordnungen, die in einem typischen lokalen Netzwerk (oder auch im Internet) auftreten, macht man keinen großen Fehler, wenn man diese Anzahl als kontinuierliche Größe betrachtet.

Die mathematischen Werkzeuge, die man zur Lösung eines Problems benutzt, hängen wesentlich ab von solchen Modellierungsentscheidungen: Modellierung durch kontinuierliche Größen verlangt typischerweise analytische Methoden, oft Differentialgleichungen; beim Modellieren mit ganzen Zahlen ist man in der diskreten Mathematik, wo eher algebraische und zahlentheoretische Methoden im Vordergrund stehen – von denen zumindest ein Teil übrigens auch analytisch ist.

Selbst wenn die Übersetzung eines Problem in Mathematik (oder besser seine Annäherung an Mathematik) feststeht, gibt es im Allgemeinen verschiedene mathematische Ansätze, die theoretisch allesamt zur korrekten Lösung führen; in der Praxis kann sich aber der Rechenaufwand zweier Verfahren so stark unterscheiden, daß nur eines der beiden wirklich durchführbar ist, oder aber so, daß zwar beide durchführbar sind, das eine aber erheblich mehr kostet als das andere.

In der Praxis eines Informatikers geht es somit nicht in erster Linie darum, ob die Voraussetzungen für einen bestimmten mathematischen Satz erfüllt sind: Die Frage stellt sich erst viel später. Als erstes muß geklärt werden, welche mathematischen Modelle in Frage kommen und welche davon zu Lösungen mit realistischem Aufwand führen.

Wer hier erfolgreich sein will, muß daher vor allem ein Gefühl für die Tragweite und den Aufwand mathematischer Methoden entwickeln; nur so kann er eine geeignete auswählen.

Dieses Gefühl kann man – wie auch die richtige Technik für den Umgang mit einem Hammer oder einer Feile – nur durch praktische Erfahrung erwerben. Ein wesentlicher Bestandteil dieser Vorlesung sind daher die Übungen, die – im Rahmen dessen, was mit Informatikkenntnissen des zweiten Semesters möglich ist – die notwendige Erfahrung dazu vermitteln sollen. Hauptziel der Vorlesung ist also, daß Sie praktische Fähig-

keiten entwickeln, und das ist nur möglich, indem Sie selbst praktische Erfahrung sammeln.

Die Übungen sind somit mindestens genauso wichtig wie die Vorlesung selbst. Es wird jede Woche zwei Übungsblätter für zwei Arten von Übungen geben:

Die wöchentlichen Übungen in kleinen Gruppen sollen Ihnen in erster Linie Gelegenheit geben, Fragen zur Vorlesung und zur konkreten Umsetzung des Vorlesungsstoffs zu stellen. Leider zeigt die Erfahrung, daß sich leider wahrscheinlich nur eine sehr kleine Minderheit von Ihnen getrauen wird, Fragen in der Vorlesung zu stellen oder Themenvorschläge für die Übungen zu machen. Deshalb gibt es jede Woche ein Blatt *Themenvorschläge für die kleinen Übungen*, das Ihnen mögliche Aufgaben vorschlägt. Diese Themenvorschläge sind selbstverständlich nicht verbindlich; in der idealen Übung spielt keiner von ihnen auch nur die geringste Rolle. Wieweit sich eine Übung diesem Idealbild nähert, hängt von Ihnen ab.

In den subidealen realen Übungen werden zunächst Ihre Fragen beantwortet und von Ihnen vorgeschlagene Probleme gelöst; in der (leider meist viel zu langen) Zeit, die noch übrig bleibt, sollten Sie die den Inhalt der Übungen wenigstens dadurch beeinflussen, daß Sie eine Auswahl unter den Themenvorschlägen treffen. Die Themenvorschläge sind im allgemeinen so umfangreich, daß unmöglich alle in einer kleinen Übung behandelt werden können; es liegt an Ihnen, diejenigen auswählen, die Ihnen am ehesten helfen, den Umgang mit den noch nicht so gut verstandenen Konzepten der Vorlesung zu üben.

Als *Hausarbeit* erhalten Sie jede Woche das eigentliche Übungsblatt, das abgegeben und von Ihrem Tutor korrigiert wird. Eine Lösung werde ich jede Woche in den großen Übungen vorrechnen – wie bereits oben ausgeführt, wird dies nur selten die einzig mögliche richtige Lösung sein. Sowohl der Vergleich meiner Lösung mit der Ihrigen als auch vor allem die Rückmeldung durch die Korrektur sollen Ihnen noch vorhandene Schwächen zeigen und zu Fragen in den kleinen Übungen anregen.

Literaturhinweise

Das Angebot von Lehrbüchern zum Thema „Höhere Mathematik“ ist riesig, und fast jedes dieser Bücher kann zumindest für Teile dieser Vorlesung nützlich sein. Ich habe hier vor allem Bücher aufgeführt, die ich selbst schon irgendwann einmal benutzt habe und daher einigermaßen kenne. Die meisten davon sind in der Mathematischen Bibliothek zu finden, teils im allgemeinen Bestand, teils auch in der Lehrbuchsammlung. Die angegebenen Bücher sind in ihrer Art sehr verschieden; bevor Sie sich eines davon kaufen, sollten Sie es sich unbedingt vorher ein Bibliotheksexemplar genau anschauen, ob es Ihnen wirklich zusagt. Wenn Sie bei einen Versender ältere Auflagen zu reduzierten Preisen bekommen können (oft nur die Hälfte), können Sie diese unbesorgt kaufen; die Änderungen zwischen verschiedenen Auflagen sind im allgemeinen so gering, daß sie praktisch kaum ins Gewicht fallen. Die angegebenen Auflagen sind die letzten, die ich kenne; im Buchhandel sind wahrscheinlich bereits neuere zu finden.

Die beiden erstgenannten Bücher **[MV]** und **[D]** verfolgen wohl am ehesten den gleichen Zweck wie diese Vorlesung:

[MV1] K. MEYBERG, P. VACHENAUER: *Höhere Mathematik I, Differential- und Integralrechnung, Vektor- und Matrizenrechnung,* Springer, ^{6}2001

[MV2] K. MEYBERG, P. VACHENAUER: *Höhere Mathematik II, Differentialgleichungen, Funktionentheorie, Fourier-Analyse, Variationsrechnung,* Springer, ^{4}2001

Dieses zweibändige Werk enthält den gesamten Stoff der *Höheren Mathematik* sowie die dafür relevanten Teile der *Analysis I.* Die Darstellung ist recht kompakt

mit fast vollständigen Beweisen; zu einigen Grundalgorithmen sind Programme angegeben. Für die *Höhere Mathematik I* reicht der erste Band.

[D] H.J. DIRSCHMID: *Mathematische Grundlagen der Elektrotechnik,* Vieweg, 1992

Etwa fünf Pfund Mathematik, die nicht nur diese Vorlesung mehr als abdecken, sondern für viele Studenten für deren gesamtes Berufsleben ausreichen dürften. Der Schwerpunkt liegt eindeutig auf dem Gebiet der Analysis; numerische Mathematik und Statistik sind (wie auch in der Vorlesung) so gut wie nicht vorhanden. Interessant vor allem für Technische Informatiker; für Software- und Internettechnologen, die keine *Höhere Mathematik II* hören, etwas zu viel des Guten. Leider auch sehr teuer, falls überhaupt noch erhältlich.

[P] L. PAPULA: *Mathematik für Ingenieure und Naturwissenschaftler,* Vieweg,
Band 1 ^{10}2001, Band 2 ^{10}2001, Band 3 ^{4}2001, Anwendungsorientierte Übungsaufgaben aus Naturwissenschaft und Technik ^{4}2000, Mathematische Formelsammlung für Ingenieure und Naturwissenschaftler, ^{7}2001

Sehr beliebtes und erfolgreiches Lehrbuch mit ausführlicher Darstellung einer beschränkten, aber im wesentlichen ausreichenden Stoffauswahl. Gelegentlich wird mehr Wert auf Anschaulichkeit als auf mathematische Exaktheit gelegt. Der erste Band behandelt vor allem Stoff der Analysis I, lediglich bei der elementaren Vektorrechnung gibt es eine kleine Überschneidung mit dieser Vorlesung. Der größte Teil des HM I-Stoffs ist in Band 2 zu finden, lediglich für die Vektoranalysis braucht man auch Band 3. Auch für die HM II reicht größtenteils Band 2; die in Band 3 sehr ausführlich behandelte Wahrscheinlichkeitstheorie und Statistik wird in der HM II nur am Ende und sehr viel kürzer behandelt. Die „Übungsaufgaben“ setzen einiges an Kenntnissen aus Physik und Technik voraus; ein Anhang stellt das notwendige Grundwissen kurz zusammen.

[BHW] BURG/HAF/WILLE: *Höhere Mathematik für Ingenieure,* Teubner 1. Analysis, ^{6}2003, 2. Lineare Algebra, ^{4}2002, 3. Gewöhnliche Differentialgleichungen, Distributionen, Integraltransformationen, ^{4}2002, 4. Vektoranalysis und Funktionentheorie, ^{2}1994, 5. Funktionalanalysis und Partielle Differentialgleichungen, ^{2}1993

Enthält deutlich mehr Stoff als **[P]** und geht mathematisch deutlich tiefer; leider ist die Verteilung des Stoffs auf die einzelnen Bände sehr verschieden vom Aufbau dieser Vorlesung: Schon die HM I behandelt Stoff aus den Bänden 1, 2 und 4; in der HM II kommt noch Stoff aus Band 3 dazu.

[BDH] BRAUCH/DREYER/HAACKE: *Mathematik für Ingenieure,* Teubner ^{9}1995

Dieses Buch richtet sich an Studenten von Fachhochschulen und ist somit nach Ansicht mancher Kollegen nicht für eine Vorlesung an der Universität geeignet. Wer sich allerdings eher für höhere Mathematik als für höheren Dünkel interessiert, findet hier ziemlich kompakt und relativ preisgünstig fast den gesamten Stoff zumindest der HM I; lediglich die Darstellung der Vektoranalysis ist etwas zu knapp.

[W1] T. WESTERMANN: *Mathematik für Ingenieure mit MAPLE I,* Springer ^{2}2000

[W2] T. WESTERMANN: *Mathematik für Ingenieure mit MAPLE II,* Springer ^{2}2001

Auch diese beiden Bände wenden sich eher an Studenten von Fachhochschulen; sie passen vom Aufbau her nicht sonderlich gut zur Vorlesung, haben aber den Vorteil, daß sie parallel zum Stoff auch das Computeralgebrasystem MAPLE behandeln und anwenden. Eine CD mit entsprechenden *worksheets* sowie einer eingeschränkten Version von MAPLE V.0 liegt jedem der beiden Bände bei. Interessant vor allem für Studenten, die parallel zur Vorlesung auch den Umgang mit einem Computeralgebrasystem üben wollen und noch keinerlei entsprechende Erfahrung haben. Die *Höhere Mathematik I* behandelt Stoff aus beiden Bänden.

[F] P. FURLAN: *Das gelbe Rechenbuch 1–3,* Verlag Martina Furlan, Dortmund, *o.J.*

Wer vor allem auf Drill und durchgerechnete Beispiele Wert legt, findet hier laut Untertitel „Rechenverfahren der Höheren Mathematik in Einzelschritten erklärt. Mit vielen ausführlich gerechneten Beispielen“. Mit den dort vorexerzierten Kochrezepten lassen sich die gängigen Typen von Standardaufgaben lösen; wenn auch nicht immer optimal: Wie immer beim sturen Nachexerzieren von Kochrezepten läuft man Gefahr, sich oftmals zuviel Arbeit zu machen, da sich

konkrete Probleme oft mit etwas Theorie beträchtlich vereinfachen lassen (und, bei realen Problemen, teilweise auch erst dadurch mit vertretbarem Aufwand lösbar werden).

Als Ergänzung zur *Höheren Mathematik I* können, mit diesen Einschränkungen, die ersten beiden Bände nützlich sein – insbesondere auch in der Endphase der Klausurvorbereitung.

Zumindest für *Technische Informatiker,* die im weiteren Verlauf ihres Studiums (und Berufslebens) immer wieder mit mathematischen Problemen konfrontiert werden, empfiehlt sich über kurz oder lang die Anschaffung einer Formelsammlung. Zu einigen der bereits zitierten Werke gibt es einen entsprechenden Band, der in seinen Bezeichnungen und der Stoffauswahl auf das Gesamtwerk abgestimmt ist; ansonsten ist vor allem ein Klassiker zu nennen, der seit Jahrzehnten in immer neuen Auflagen erscheint und mit dem schon Generationen von Naturwissenschaftlern und Ingenieuren gearbeitet haben: „Der BRONSTEIN", der seit einigen Jahren in zwei konkurrierenden Neubearbeitungen angeboten wird, wobei die erste wahlweise mit oder ohne CD-ROM erhältlich ist.

[BSM] I.N. BRONSTEIN, K.A. SEMENDJAJEW, G. MUSIOL: *Taschenbuch der Mathematik,* Verlag Harri Deutsch, 2000

[BGZ] I.N. BRONSTEIN, G. GROSCHE, E. ZEIDLER: *Teubner-Taschenbuch der Mathematik,* Teubner, 1996

Deutlich weniger ambitioniert und auch billiger ist

[MMWW] G. MERZINGER, G. MÜHLBACH, D. WILLE, T. WIRTH: *Formeln + Hilfen zur Höheren Mathematik,* Binomi ^{4}2001,

eine Formelsammlung die zur HM I und – mit Ausnahme der nicht behandelten FOURIER-Transformation – auch zur HM II ausreicht, vielleicht aber nicht für spätere Anwendungen.

Auch bei den Lehrbüchern seien noch einige „Klassiker" genannt, die seit Jahrzehnten in immer neuen Auflagen erscheinen und auch heute noch interessant sind. Es handelt sich um Werke aus meist recht vielen Bänden, wobei selbst der Stoff der Vorlesung *Höhere Mathematik I* je

nach Organisation des Gesamtwerks auf bis zu drei Bände verteilt sein kann. Wegen der Vielzahl von Auflagen und Bänden verzichte ich auf die Angabe von Erscheinungsjahren.

[S] W.I. SMIRNOW: *Lehrbuch der Höheren Mathematik,* VEB Deutscher Verlag der Wissenschaften

Ein Klassiker, nach dem Generationen von russischen und (nicht nur ost-)deutschen Naturwissenschaftlern und Ingenieuren ausgebildet wurden; enthält in vier Bänden (von denen die letzten beiden noch in Halbbände unterteilt sind) den gesamten klassischen Stoff der Mathematik für Naturwissenschaftler und Ingenieure (also erheblich mehr, als im zweisemestrigen Kurs *Höhere Mathematik* behandelt werden kann) und ist auch heute noch sehr gut zu lesen. Die HM I behandelt Stoff aus den Bänden I, II und III/1.

[R] R. ROTHE: *Höhere Mathematik,* Teubner

Sieben (dünne) Bände, zu denen allerdings auch Aufgaben- und Formelsammlung gehören, so daß die Darstellung insgesamt eher knapp ist. Für diese Vorlesung relevant sind die Bände II und III.

[Du] A. DUSCHEK: *Höhere Mathematik,* Springer Wien

Die österreichische Variante, vier recht ausführliche Bände, von denen hier vor allem die ersten beiden von Interesse sind.

[A] G. AUMANN: *Höhere Mathematik,* Bibliographisches Institut Mannheim

Drei relativ dünne Taschenbücher, deren erste beide trotzdem fast alles enthalten, was wir in dieser Vorlesung brauchen. Die Darstellung ist natürlich weniger ausführlich als in den dickleibigen Werken, aber das wird nicht jeder Student als Nachteil empfinden.

[C] R. COURANT: *Vorlesungen über Differential- und Integralrechnung I+II,* Springer

Ein Klassiker eines berühmten Mathematikers, auch heute noch sehr lesenswert. Trotz des Titels beschränkt sich das Buch nicht auf Analysis, sondern behandelt auch beispielsweise die Lineare Algebra in einem Umfang, der für diese Vorlesung völlig ausreicht.

Kapitel 1
Vektorräume und lineare Gleichungssysteme

Lineare Strukturen sind sowohl in der Mathematik als auch in ihren Anwendungen allgegenwärtig: Zwar sind die meisten Funktionen nichtlinear, aber fast alles, was man damit anstellt – Differenzieren, Integrieren, FOURIER- oder LAPLACE-transformieren *usw.* – wird sich als lineare Operation herausstellen. Vektorräume bieten einen gemeinsamen Rahmen für alle diese Operationen und sind daher wichtige Hilfsmittel nicht nur innerhalb der Mathematik, wie etwa für Analysis, Geometrie, Differentialgleichungen und Integraltransformationen, sondern auch beispielsweise in der Optimierung, der Signalverarbeitung (z.B. Kodierungstheorie, Kryptographie und Bildverarbeitung), der Optik, Elektrodynamik und Quantenphysik. Die anschaulichsten Vektorräume sind die, deren Elemente anschauliche Vektoren sind; der große Vorteil einer einheitlichen Behandlung dieser Vektoren und zahlreicher anderer Objekte unter dem gemeinsamen Dach des Begriffs „Vektorraum“ besteht darin, daß man viele für Vektoren anschaulich klare Aussagen mit geringem Aufwand so umformulieren kann, daß sie auch in den erheblich schwerer vorstellbaren Vektorräumen gelten, mit denen man es in schwierigeren Anwendungen zu tun hat. Dies ist Teil einer sehr viel allgemeineren Strategie der Mathematik: Abstrakte Mathematik lebt davon, daß anschauliche Phänomene formalisiert werden, um die so entstehende formale Struktur auf andere, weniger anschauliche Phänomene anzuwenden.

Gerade für Anwendungen in der Informationstechnik brauchen wir allerdings nicht nur einen allgemeineren Rahmen für Vektoren:

Physikalische und auch sonstige Größen lassen sich bekanntlich (mit wenigen Ausnahmen) bezüglich ihrer mathematischen Behandlung in

zwei Klassen einteilen: Temperaturen, Stromstärken, Bevölkerungszahlen, Geldmengen *usw.* werden (bezüglich einer festzulegenden Einheit) durch Zahlen beschrieben; Geschwindigkeiten, Kräfte, Bevölkerungswanderungen *usw.* durch Zahlen zusammen mit einer Richtung. Im ersten Fall reden wir von *Skalaren,* im zweiten von *Vektoren.*

Bei den gerade aufgeführten Beispiele handelt es sich bei den Zahlen jeweils um reelle Zahlen oder Teilmengen davon. Wenn wir praktisch rechnen, egal ob mit oder ohne Computer, müssen wir uns allerdings immer auf Teilmengen der reellen Zahlen beschränken, schon weil kein Computer sämtliche Elemente einer überabzählbare Menge darstellen kann.

Es gibt allerdings auch eine Reihe von Beispielen, bei denen wir es mit „Zahlen“ zu tun haben, die nichts mit reellen Zahlen zu tun haben: Für Bits und Bytes lassen sich Addition und Multiplikation so definieren, daß dafür dieselben Rechenregeln gelten wie für Addition und Multiplikation reeller Zahlen, und das nutzt die Informationstechnik aus, um beispielsweise Informationen sicher zu übertragen. Dies betrifft sowohl die Fehlerkorrektur auf einer CD (fehlerkorrigierende Codes) als auch die Sicherung von Information gegen unbefugtes Abhören (Kryptographie). Daher müssen wir nicht nur für Vektoren, sondern auch für Skalare eine gemeinsame Struktur finden, daß möglichst viele Anwendungen unter ihrem Dach vereinigt.

Im Falle der Skalare ist das der aus der Analysis I bekannte Begriff des Körpers; der Begriff des Vektorraums formalisiert das Zusammenspiel zwischen Vektoren und Skalaren. Bevor wir ihn einführen, wollen wir uns zunächst Vektoren und Skalare etwas genauer ansehen.

§ 1: Zahlen und Körper

a) Von den natürlichen zu den komplexen Zahlen

Im Anfang waren die natürlichen Zahlen $1, 2, 3, \ldots$. Man kann sie addieren und multiplizieren, aber man kann dort weder die Gleichung $5 + x = 2$ noch die Gleichung $5 \cdot x = 2$ lösen. Ersteres Problem führt

auf die Erweiterung der Menge $\mathbb{N}$ der natürlichen Zahlen zur Menge $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ der ganzen Zahlen, in der auch die Subtraktion uneingeschränkt ausführbar ist, nicht aber die Division. Letzteres führte – für positive Zahlen schon rund zwei Tausend Jahre vor der Einführung negativer Zahlen – zur Einführung von Brüchen und letztlich zur Menge $\mathbb{Q}$ der rationalen Zahlen, in dem *alle* Grundrechenarten uneingeschränkt ausführbar sind – mit Ausnahme natürlich der Division durch Null.

Um diese „rationalen Zahlen" herum bauten PYTHAGORAS (geboren je nach Quelle zwischen *ca.* 600* *v. Chr.* und *ca.* 570* *v. Chr.*, gestorben zwischen *ca.* 509 *v. Chr.* und *ca* 475* *v. Chr.*) und seine Schüler in Süditalien eine ganze Weltanschauung; umso größer war ihr Schock, als sie entdeckten, daß ausgerechnet eine geometrisch so perfekte Größe wie die Diagonale eines Quadrats in keinem rationalen Verhältnis zur Seitenlänge steht, mit anderen Worten, daß die Quadratwurzel aus zwei keine rationale Zahl ist. Der Legende nach entdeckte dies HIPPASOS (*ca.* 520* *v. Chr.* – *a.* 480 *v. Chr.*), der dafür je nach Überlieferung entweder von den anderen Pythagoräern ertränkt wurde oder aber als Strafe der Götter auf einer Schiffsreise ertrank.

Trotzdem ließ sich seine Erkenntnis nicht unbeschränkt geheimhalten; kombiniert mit dem Interesse an Grenzwerten bei EUDOXOS (408 *v. Chr.* – 355 *v. Chr.*), ARCHIMEDES (287 *v. Chr.* – 212 *v. Chr.*), und vor allem rund 2 000 Jahre später bei NEWTON (1643–1727), LEIBNIZ (1664–1716), EULER (1707–1783) und vielen anderen, führte sie schließlich zu den reellen Zahlen.

Auch hier ist noch nicht alles möglich; beispielsweise hat zwar die Gleichung $x^2 = 3$ eine reelle Lösung (genauer gesagt zwei), nicht aber die Gleichung $x^2 = -3$. Diese könnte gelöst werden, wenn man die Quadratwurzel aus -1 ziehen könnte, denn dann wäre $\sqrt{-3} = \sqrt{-1} \cdot \sqrt{3}$. Genauso überlegt man sich leicht, daß dann jede quadratische Gleichung eine Lösung hätte.

Es liegt also nahe, auch die reellen Zahlen zu erweitern, indem man ein neues Element hinzufügt, dessen Quadrat -1 ist. Dieses Element wird in der Mathematik und Physik traditionellerweise mit i wie *imaginär* bezeichnet, da es zur Zeit seiner Einführung als imaginäre, d.h. nur in der Vorstellung vorhandene, Zahl angesehen wurde. In der Elektrotechnik, wo I und i eine feste andere Bedeutung haben, verwendet man stattdessen den Buchstaben j.

Natürlich genügt es nicht, nur die Menge $\mathbb{R} \cup \{i\}$ zu betrachten, denn wir möchten mit den neuen Zahlen auch rechnen und dabei möglichst wenig von den bewährten Rechenregeln für reelle Zahlen aufgeben.

Insbesondere sollten also alle Zahlen der Form $x + iy$ mit $x, y \in \mathbb{R}$ in der neuen Menge liegen, und es sollte möglich sein, mit ihnen wie gewohnt zu rechnen. Für zwei Zahlen $x + iy$ und $u + iv$ müßte also gelten

$$(x + iy) + (u + iv) = (x + u) + (iy + iv) = (x + u) + i(y + v)$$

und

$$\begin{aligned}(x + iy)(u + iv) &= xu + iyu + xiv + (iy)(iv) = xu + iyu + ixv + i^2 yv \\ &= (xu - yv) + (yu + xv)i\,.\end{aligned}$$

Damit lassen sich Zahlen dieser Form insbesondere addieren und multiplizieren, ohne daß neue Zahlen entstehen; wir können hoffen, daß sie vielleicht sogar schon für die geplante Erweiterung ausreichen.

Um dies zu überprüfen, nehmen wir die oben heuristisch abgeleiteten Regeln als *Definitionen* von Addition und Multiplikation und untersuchen die entstehende Struktur:

Definition: *a)* Die Menge $\mathbb{C}$ der komplexen Zahlen ist die Menge aller formaler Ausdrücke der Form $x + iy$ mit $x, y \in \mathbb{R}$.
b) Auf $\mathbb{C}$ wird eine Verknüpfung „+" definiert durch die Vorschrift

$$(x + iy) + (u + iv) = (x + u) + i(y + v)\,.$$

c) Dazu kommt eine Verknüpfung „·", definiert durch

$$(x + iy) \cdot (u + iv) = (xu - yv) + i(xv + yu)\,.$$

d) Für $z = x + iy \in \mathbb{C}$ nennen wir x den *Realteil* und y den *Imaginärteil* von z; in Zeichen

$$x = \mathfrak{Re}\, z \quad \text{und} \quad y = \mathfrak{Im}\, z\,.$$

(Eine komplexe Zahl heißt *komplex,* weil sie aus einem Realteil und einem Imaginärteil *zusammengesetzt* ist.)

b) Der Begriff des Körpers

Wir wollen sehen, daß die komplexen Zahlen mit diesen Verknüpfungen den „üblichen“ Rechenregeln genügen. Das soll heißen, daß wir Addition, Subtraktion, Multiplikation und Division (außer durch Null) uneingeschränkt durchführen können und daß wir auch mit Klammern „wie gewohnt“ umgehen können. Diese vage Beschreibung formalisierte ERNST STEINITZ 1910 durch den Begriff des *Körpers:*

Definition: Ein Körper k ist eine Menge zusammen mit zwei Abbildungen

$$+: k \times k \to k \quad \text{und} \quad \cdot: k \times k \to k\,,$$

genannt *Addition* und *Multiplikation,* für die gilt:

I.1) Das Assoziativgesetz der Addition

$$(a+b)+c = a+(b+c) \qquad \text{für alle } a,b,c \in k$$

I.2) Es gibt ein Element $0 \in k$, so daß gilt

$$a+0 = 0+a = a \qquad \text{für alle } a \in k$$

I.3) Zu jedem Element $a \in k$ gibt es ein Element $a' \in k$, so daß gilt

$$a+a' = a'+a = 0\,.$$

I.4) Das Kommutativgesetz der Addition

$$a+b = b+a \qquad \text{für alle } a,b \in k$$

II.1) Das Assoziativgesetz der Multiplikation

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \qquad \text{für alle } a,b,c \in k$$

II.2) Es gibt ein von 0 *verschiedenes* Element $1 \in k$, so daß gilt

$$a \cdot 1 = 1 \cdot a = a \qquad \text{für alle } a \in k$$

II.3) Zu jedem von 0 verschiedenen Element $a \in k$ gibt es ein Element $a'' \in k$, so daß gilt

$$a \cdot a'' = a'' \cdot a = 1\,.$$

II.4) Das Kommutativgesetz der Multiplikation

$$a \cdot b = b \cdot a \qquad \text{für alle } a,b \in k$$

III.) Das Distributivgesetz

$$a \cdot (b+c) = a \cdot b + a \cdot c \qquad \text{für alle } a,b,c \in k$$

Das Element a' aus I.3.) wird üblicherweise als $-a$ bezeichnet und a'' aus II.3) als a^{-1}. Statt $a+(-b)$ schreibt man kurz $a-b$, statt $a \cdot b^{-1}$ entsprechend a/b.

ERNST STEINITZ (1871–1928) wurde in Schlesien geboren und studierte ab 1890 an den Universitäten Breslau und Berlin. 1894 promovierte er in Breslau, ein Jahr später wurde er Privatdozent an der Technischen Hochschule Berlin-Charlottenburg. 1910 wurde er Professor in Breslau, 1920 in der Universität Kiel. In seinem Buch *Algebraische Theorie der Körper* gab er 1910 die erste Definition eines Körpers und bewies viele Sätze, die noch heute zum Standardstoff jeder Algebra-Vorlesung gehören. Auch die Konstruktion der rationalen Zahlen als Äquivalenzklassen von Paaren ganzer Zahlen geht auf ihn zurück.

Demnach bilden also die natürlichen Zahlen keinen Körper, weil dort weder die Addition noch die Multiplikation invertierbar ist, weil also mit anderen Worten weder die Subtraktion noch die Division (durch Zahlen ungleich Null) unbeschränkt möglich ist.

Genauso bilden auch die ganzen Zahlen keinen Körper, denn hier kann man zwar uneingeschränkt subtrahieren, aber außer ± 1 hat keine ganze Zahl ein multiplikatives Inverses.

Die beiden aus der Schule bekannten Standardbeispiele von Körpern sind die rationalen Zahlen $\mathbb{Q}$, d.h. also die Menge aller Brüche mit einem ganzzahligen Zähler und einer natürlichen Zahl als Nenner, und die Menge $\mathbb{R}$ der reellen Zahlen.

Nach dieser Präzisierung ist klar, was wir von den komplexen Zahlen erwarten, und der nächste Satz zeigt, daß unsere Erwartungen auch erfüllt werden:

Satz: Die Menge $\mathbb{C}$ mit den oben definierten Verknüpfungen ist ein Körper.

Beweis: Eigentlich müßten wir alle Körperaxiome einzeln überprüfen; um aber nicht garzu viel Papier zu produzieren, möchte ich mich hier im Sinne des Umweltschutzes auf die interessantesten beschränken.

Völlig uninteressant sind die Axiome, die sich mit der Addition in $\mathbb{C}$ befassen: Da die Addition komponentenweise für Realteil und Imaginärteil definiert ist, folgen alle Axiome sofort aus den entsprechenden Axiomen für $\mathbb{R}$. Das Neutralelement bezüglich der Addition ist natürlich $0 + i0$, und $-(x + iy) = (-x) + i(-y)$.

Die Forderungen an die Multiplikation sind weniger offensichtlich. Unmittelbar einsichtig ist das Kommutativgesetz; das Assoziativgesetz dagegen ist eine eher unangenehme sture Nachrechnerei, die jeder einmal, aber nur einmal in seinem Leben wirklich ausführen sollte. (Ich habe sie glücklicherweise schon hinter mir.) Wir werden im übrigen in Kürze, sobald wir mit Abbildungsmatrizen umgehen können, einen alternativen Beweis finden, der ganz ohne Rechnung auskommt.

Neutralelement bezüglich der Multiplikation kann, wenn alles Sinn haben soll, nur $1 + i0$ sein, und in der Tat sieht man sofort, daß jedes Element $x + iy$ sowohl bei Links- wie auch bei Rechtsmultiplikation hiermit sich selbst liefert.

Bleibt die Existenz eines multiplikativen Inversen, und hier hilft nur ein Trick: Für $x + iy \neq 0 + i0$ ist

$$(x + iy) \cdot (x - iy) = x^2 + y^2 \in \mathbb{R}_{>0}$$

eine positive reelle Zahl; falls also ein Inverses existiert und die üblichen Regeln der Bruchrechnung gelten, ist

$$\frac{1}{x + iy} = \frac{x - iy}{(x + iy)(x - iy)} = \frac{x - iy}{x^2 + y^2} = \frac{x}{x^2 + y^2} - i \cdot \frac{y}{x^2 + y^2}\,.$$

Eine leichte Rechnung zeigt, daß dieses ganz rechts stehende Element von $\mathbb{C}$ in der Tat sowohl bei Links- als auch bei Rechtsmultiplikation mit $x + iy$ das Neutralelement $1 + i0$ liefert.

Die noch verbleibenden Distributivgesetze sind wieder Rechnerei zum Abhaken, die man genau einmal in seinem Leben durchführen sollte, und auch sie werden zur trivialen Selbstverständlichkeit, wenn wir den komplexen Zahlen später Abbildungsmatrizen zuordnen. ∎

Es ist nun klar, daß die Abbildung

$$\begin{cases} \mathbb{R} & \hookrightarrow \mathbb{C} \\ x & \mapsto x + i0 \end{cases}$$

eine Einbettung des Körpers der reellen in den der komplexen Zahlen definiert; da wir ersteren erweitern wollen, betrachten wir diese Einbettung als Identifikation, d.h. wir identifizieren den „formalen Ausdruck" $x + i0$ mit der reellen Zahl x. Insbesondere sind jetzt also 0 und 1 das additive und das multiplikative Neutralelement. Außerdem schreiben wir kurz i anstelle von $0 + i1$; nach den Rechenregeln, die wir inzwischen kennen, ist der „formale Ausdruck $x + iy$" dann nichts anderes als die mit den Rechenoperationen von $\mathbb{C}$ berechnete komplexe Zahl $x + i \cdot y$.

Damit sind also alle von der reellen Zahlen gewohnte Rechenregeln für die Grundrechenarten auch für komplexe Zahlen gültig. Nicht zu retten sind allerdings die Regeln über die *Ordnungsbeziehung:* Falls es in $\mathbb{C}$ eine mit der algebraischen Struktur kompatible Ordnungsrelation gäbe, müßte $i^2 \geq 0$ sein, was nicht im Sinne des Erfinders ist. Nicht zuletzt aus diesem Grund machen die Körperaxiome keinerlei Aussage über Größer- und Kleinerbeziehungen.

c) Mehr über komplexe Zahlen

Der Erfolg, den wir bei der Herleitung des multiplikativen Inversen durch Erweiterung mit $x - iy$ hatten, verdient genauer untersucht zu werden:

Definition: Für $z = x + iy \in \mathbb{C}$ heißt $\overline{z} = x - iy$ die zu z konjugiert komplexe Zahl.

(Gelegentlich wird $x - iy$ auch als z^* bezeichnet.)

Offensichtlich ist $\overline{z + w} = \overline{z} + \overline{w}$, und auch das entsprechende Resultat für die Multiplikation $\overline{zw} = \overline{z} \cdot \overline{w}$ läßt sich leicht nachrechnen.

Für die Herleitung des Inversen wesentlich war die Tatsache, daß

$$(x+iy)(x-iy) = x^2 + y^2$$

eine reelle Zahl ist, die genau dann verschwindet, wenn sowohl x als auch y und damit auch $x+iy$ verschwinden; wir bezeichnen die Quadratwurzel aus dieser nichtnegativen reellen Zahl als *Betrag* der komplexen Zahl:

Definition: Der Betrag einer komplexen Zahl $z = x + iy$ ist

$$|z| = \sqrt{z \cdot \overline{z}} = \sqrt{x^2 + y^2}\,.$$

Für reelles z stimmt das natürlich genau mit dem gewohnten Betrag einer reellen Zahl überein.

Offensichtlich ist $|z| = 0 \Leftrightarrow z = 0$ und

$$\frac{1}{z} = \frac{\overline{z}}{z \cdot \overline{z}} = \frac{\overline{z}}{|z|^2}\,.$$

Der Betrag hat noch eine weitere nützliche Interpretation: Für zwei komplexe Zahlen $z = x + iy$ und $w = u + iv$ ist

$$|z - w| = \sqrt{(x-u)^2 + (y-v)^2}$$

gerade der EUKLIDische Abstand zwischen den Punkten (x, y) und (u, v) der EUKLIDischen Ebenen $\mathbb{R}^2$. Da die komplexen Zahlen natürlich über die Abbildung

$$\begin{cases} \mathbb{C} & \to \mathbb{R}^2 \\ x + iy & \mapsto (x, y) \end{cases}$$

in Bijektion mit den Punkten der EUKLIDischen Ebenen stehen, können wir die komplexen Zahlen also auch identifizieren mit den Punkten der EUKLIDischen Ebenen, wobei der Betrag der Differenz zwischen zwei Zahlen gerade dem Abstand entspricht. Man bezeichnet den Körper der komplexen Zahlen in diesem Zusammenhang auch als GAUSS*sche Zahlenebene.* Sie war zwar nicht zusammen mit GAUSS auf dem Zehnmarkschein abgebildet, war aber 1977 das Thema der Sondermarke zu seinem zweihundertsten Geburtstag.

CARL FRIEDRICH GAUSS (1777–1855) leistete wesentliche Beiträge zur Zahlentheorie, zur nichteuklidischen Geometrie, zur Differentialgeometrie und Kartographie, zur Fehlerrechnung und Statistik, zur Astronomie und Geophysik *usw.* Als Direktor der Göttinger Sternwarte baute er zusammen mit dem Physiker Weber den ersten Telegraphen. Er leitete die erste Vermessung und Kartierung des Königreichs Hannover und zeitweise auch den Witwenfond der Universität Göttingen; seine hierbei gewonnene Erfahrung benutzte er für erfolgreiche Spekulationen mit Aktien.

Sätze und Verfahren von Gauß werden uns im weiteren Laufe der Vorlesung noch sehr häufig begegnen.

d) Weitere Körper

Wir kennen inzwischen die drei ineinander liegenden Körper

$$\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}\,;$$

tatsächlich liegen zwischen $\mathbb{Q}$ und $\mathbb{C}$ noch zahlreiche andere Körper, mit denen wir uns hier zwar nicht ausführlich beschäftigen wollen, die aber trotzdem in der Informationsverarbeitung teilweise sehr wichtig sind.

Der Grund dafür liegt darin, daß die reellen Zahlen trotz ihres Namens alles andere als „real“ sind: Sie sind zwar ein sehr erfolgreiches Hilfsmittel zur Behandlung von Problemen aus den Naturwissenschaften, der Technik, den Wirtschaftswissenschaften *usw.*, aber es ist beispielsweise nicht möglich, eine beliebige reelle Zahl mit endlichem Aufwand zu beschreiben – erst recht hat man keine Chance, beliebige reelle Zahlen in einem Computer darzustellen.

Es kommt noch schlimmer: Nach einem 1968 von RICHARDSON bewiesenen Satz läßt sich selbst für zwei endlich beschreibbare reelle Zahlen im allgemeinen nicht entscheiden, ob sie gleich sind oder nicht.

Die Mathematik kennt zwei mehr oder weniger erfolgreiche Auswege aus diesem Dilemma: Standard in den meisten Anwendung ist die Approximation der reellen Zahlen durch sogenannte Gleitkommazahlen, die in einigen Programmiersprachen als *real* bezeichnet werden, in den meisten heute gebräuchlichen aber die korrektere Bezeichnung *float* haben. Mit den Möglichkeiten und Grenzen dieser Strategie beschäftigt

sich die *Numerische Mathematik;* da es darüber eine eigene Vorlesung gibt, werde ich solche Fragen in der *Höheren Mathematik* nur gelegentlich kurz am Rande erwähnen.

Die andere Strategie besteht darin, sich auf einen *Teilkörper* der reellen (oder komplexen) Zahlen zu beschränken, in dem man exakt rechnen kann. Dies ist der (gegenüber der Numerik erheblich aufwendigere) Ansatz der *Computeralgebra,* der beispielsweise bei manchen Problemen der Computergraphik verwendet werden muß, da man hier zum Erhalt der logischen und topologischen Konsistenz der Daten *exakt* wissen muß, ob zwei auf verschiedene Weise berechneten Punkte gleich sind oder nicht. Eine falsche Antwort auf diese Frage führt erstaunlich oft zum Systemabsturz, beispielsweise wegen einer Division durch Null.

Zum Glück gibt es einen Teilkörper von $\mathbb{R}$, den sogenannten Körper der berechenbaren Zahlen, in dem alle Berechnungen exakt und algorithmisch ausgeführt werden können – wenn auch meist sehr teuer. In der Praxis wendet man daher solche Verfahren meist nur dann an, wenn numerische Berechnungen keine hinreichend exakte Antwort garantieren können.

e) Der Körper mit zwei Elementen

Nicht jeder Körper läßt sich in die reellen oder komplexen Zahlen einbetten; das einfachste Gegenbeispiel ist folgendes:

In der digitalen Informationsverarbeitung gibt es fast überall genau zwei Zustände, die – unabhängig von ihrer tatsächlichen technischen Realisierung – üblicherweise mit 0 und 1 bezeichnet werden. Wir wollen aus der Menge $\mathbb{F}_2 = \{0, 1\}$ dieser beiden Zustände einen Körper machen.

Schon bei der Addition gibt es nicht viele Möglichkeiten: Wir müssen eines der beiden Elemente zum Neutralelement machen, wofür wir natürlich sinnvollerweise die Null wählen. Alsdann ist nach Definition der Eigenschaften eines Neutralelements

$$0 + 0 = 0 \quad \text{und} \quad 0 + 1 = 1 + 0 = 1\,;$$

die einzige noch unbekannte Summe ist also $1 + 1$. Wäre $1 + 1 = 1$, müßte nach Subtraktion von 1 auf beiden Seiten, $1 = 0$ sein, was wir nicht wollen, also müssen wir festlegen, daß $1 + 1 = 0$ ist.

Bei der Multiplikation ist alles noch deutlicher festgelegt: In jedem Körper ist für jedes Element x

$$0 \cdot x = (1 - 1) \cdot x = x - x = 0 \quad \text{und} \quad 1 \cdot x = 1\,,$$

also ist

$$0 \cdot 0 = 0, \quad 0 \cdot 1 = 1 \cdot 0 = 0 \quad \text{und} \quad 1 \cdot 1 = 1\,.$$

Die Verknüpfungstabellen sehen damit folgendermaßen aus:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Ein Leser, der bereits über Kenntnisse der Logik und/oder der Schaltungstechnik verfügt, wird hier sicherlich bekanntes entdecken:

- Falls man 1 als *wahr* und 0 als *falsch* interpretiert, ist „·“ das logische Und, während „+“ das *exklusive* logische Oder ist. (Für Altphilologen ist dies das lateinische *aut* im Gegensatz zum *vel;* wer sich eher mit Logik oder Schaltalgebra auskennt, sollte zumindest eine der (äquivalenten) Bezeichnungen XOR oder *Antivalenz* schon einmal gehört haben.)
- Falls man ganze Zahlen in Binärdarstellung addieren möchte, ist für jede einzelne Binärstelle $x \cdot y$ der Übertrag, während $x + y$ bis auf den Übertrag der vorherigen Stelle gleich der Binärstelle des Ergebnisses ist. Man bezeichnet daher eine Schaltung, die $x + y$ und $x \cdot y$ berechnet auch als einen *Halbaddierer;* der Volladdierer, der ein Bit plus dem Übertrag des vorherigen Bits verarbeitet, besteht aus zwei Halbaddierern und einem Oder-Gatter.

So seltsam dieser Körper auf den ersten Blick auch aussehen mag, hat er also anscheinend doch das Potential für nützliche Anwendungen; einige davon werden wir schon bald kennenlernen. Wie wir dann sehen werden, gibt es noch eine ganze Reihe weiterer endlicher Körper mit wichtigen Anwendungen in der Kryptographie, der Kodierungstheorie und einer ganzen Reihe weiterer Gebiete der Informationsverarbeitung.

§2: Vektoren und Vektorräume

a) Vektoren in der Ebene und im Raum

Vektoren werden anschaulich dargestellt durch *Pfeile,* d.h. durch gerichtete Verbindungsstrecken zweier Punkte. Sie sind festgelegt durch die Angabe von Anfangs- und Endpunkt, aber auch beispielsweise durch die Angabe von Anfangspunkt, Länge und Richtung, wobei diese Richtung jedoch für Pfeile der Länge Null nicht definiert ist.

Pfeile dieser Art sind nützlich beispielsweise für die Darstellung von elektrischen oder magnetischen Feldern wie etwa den in Abbildung eins dargestellten: dem elektrischen Feld einer abstoßenden Punktladung und dem Magnetfeld eines stromdurchflossenen Leiters.

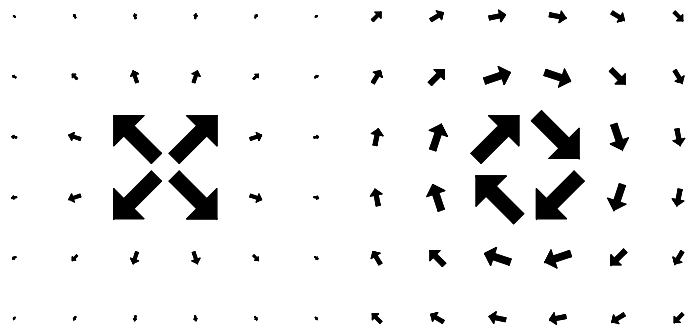

Abb. 1: Zwei elektromagnetische Felder

Zwei Pfeile lassen sich addieren, falls der Endpunkt des ersten gleich dem Anfangspunkt des zweiten ist; die Summe ist dann derjenige Pfeil, der den Anfangspunkt des ersten mit dem Endpunkt des zweiten Pfeils verbindet. Auch läßt sich ein Pfeil mit einer reellen Zahl multiplizieren, wenn wir vereinbaren, daß das Ergebnis jeder Pfeil sein soll, der denselben Anfangspunkt und dieselbe Richtung hat wie der ursprüngliche Pfeil, dessen Länge aber mit der reellen Zahl multipliziert wurde. (Eine

Multiplikation mit einer negativen Zahl soll dabei bedeuten, daß der Pfeil an seinem Anfangspunkt gespiegelt und dann mit dem Betrag der Zahl multipliziert wird.)

Sobald wir uns allerdings dafür interessieren, wie sich ein Teilchen im kombinierten Kraftfeld der Punktladung und des stromdurchflossenen Leiters bewegt, reichen Pfeile nicht mehr aus: Wir haben zwar für jeden Punkt der Ebene (außer dem Nullpunkt) einen Kraftpfeil für jedes Feld, aber natürlich müssen wir in jedem Punkt die beiden *dort* beginnenden Kraftpfeile addieren, was mit Pfeilen nicht geht.

Die Lösung dieses Problems ist wohl bekannt: Die beiden Pfeile werden gemäß dem „Parallelogramm der Kräfte“ kombiniert, d.h. der eine Pfeil wird so verschoben, daß sein Anfangspunkt gleich dem Endpunkt des anderen Pfeils ist. Wie Abbildung zwei zeigt, ist das Ergebnis unabhängig von der Reihenfolge der Summanden, d.h.

$$\vec{v} + \vec{w} = \vec{w} + \vec{v}\,.$$

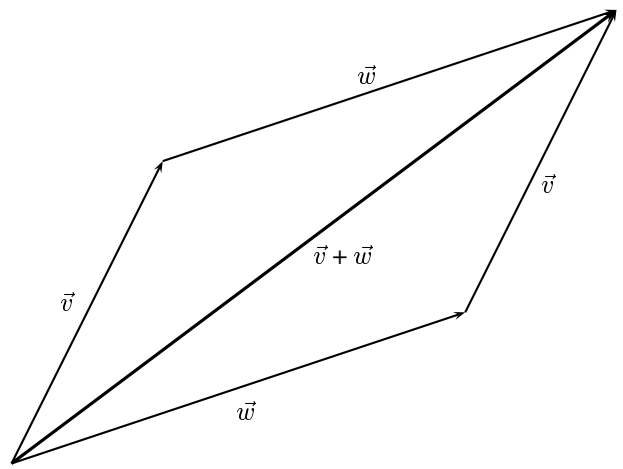

Abb. 2: Das „Parallelogramm der Kräfte“

Wir definieren daher als neuen Begriff einen *Vektor* als etwas, das zwar wie ein Pfeil eine Länge und eine Richtung haben soll, aber keinen

Anfangspunkt. Mathematisch exakt ausgedrückt ist also ein Vektor eine *Äquivalenzklasse* von Pfeilen, wobei zwei Pfeile genau dann äquivalent sind, wenn sie dieselbe Länge und (so die Länge von Null verschieden ist) dieselbe Richtung haben.

Vektoren werden in der Literatur meist durch Fraktur- oder Fettbuchstaben bezeichnet; da sich Fettdruck schlecht an der Tafel realisieren läßt und Frakturbuchstaben meist zu Hörerprotesten führen, verwenden wir hier stattdessen lateinische Buchstaben, die mit einem Pfeil überstrichen sind, also $\vec{u}, \vec{v}, \vec{w}, \ldots$. Die Addition zweier Vektoren wird durch das gewöhnliche Pluszeichen ausgedrückt, wir schreiben also $\vec{v}+\vec{w}$. Aus dem „Parallelogramm der Kräfte“ in Abbildung zwei liest man sofort ab, daß $\vec{v}+\vec{w} = \vec{w}+\vec{v}$ ist. Abbildung drei zeigt die Summe der beiden Kraftfelder aus Abbildung eins.

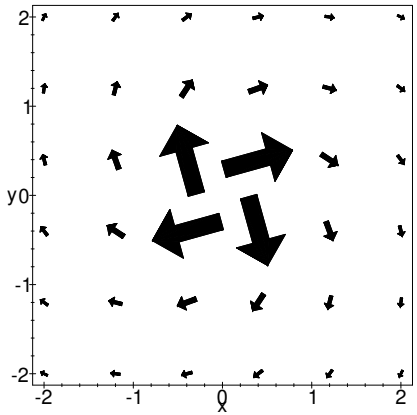

Abb. 3: Die Summe der beiden Felder aus Abbildung eins

Als weitere Eigenschaft der Vektoraddition wollen wir festhalten, daß es zu jedem Vektor $\vec{v}$ einen Vektor $\vec{w}$ gibt, so daß

$$\vec{v}+\vec{w} = \vec{0}$$

der Nullvektor ist; $\vec{w}$ ist einfach der entgegengesetzt orientierte Vektor $\vec{v}$. Wir bezeichnen diesen Vektor kurz als $-\vec{v}$.

Die Addition des Nullvektors ändert natürlich nichts am anderen Summanden, d.h.

$$\vec{v}+\vec{0} = \vec{0}+\vec{v} = \vec{v} \quad \text{für alle Vektoren } \vec{v}\,.$$

Schließlich gilt für die Vektoraddition auch noch das Assoziativgesetz

$$\left(\vec{u}+\vec{v}\right)+\vec{w} = \vec{u}+\left(\vec{v}+\vec{w}\right)\,,$$

wie man sich leicht überzeugt, indem man das Diagramm für die Konstruktion von $\vec{v}+\vec{w}$ an den Endpunkt des Vektors $\vec{u}$ verschiebt; siehe Abbildung vier.

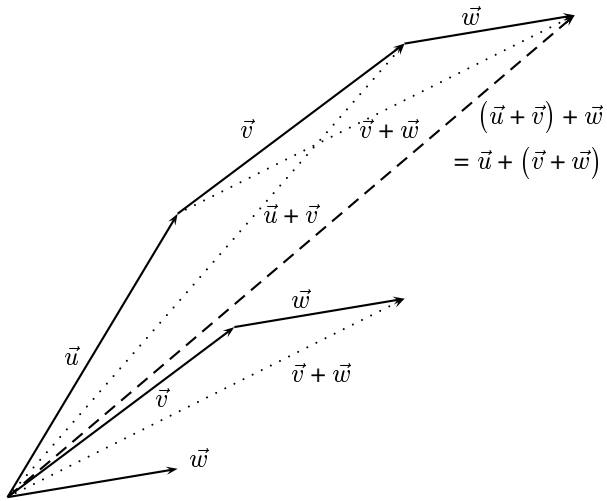

Abb. 4: Das Assoziativgesetz der Vektoraddition

Außer der Addition von Vektoren können wir auch ihre Streckung, d.h. ihre Multiplikation mit einer reellen Zahl, definieren: Ist $\vec{v}$ ein Vektor und $\lambda > 0$ eine positive reelle Zahl, so soll $\lambda\vec{v}$ dieselbe Richtung haben wie $\vec{v}$ und die λ-fache Länge; für $\lambda < 0$ soll $\lambda\vec{v}$ die entgegengesetzte Richtung haben und die $|\lambda|$-fache Länge. Für $\lambda = 0$ schließlich ist $\lambda\vec{v}$ der Nullvektor.

Anwendung des Strahlensatzes auf das Dreieck in Abbildung fünf zeigt, daß für diese Multiplikation das Distributivgesetz

$$\lambda(\vec{v}+\vec{w}) = \lambda\vec{v} + \lambda\vec{w}$$

gilt: Als Strahlen betrachten wir von $\vec{v}$ und $\vec{v}+\vec{w}$ aufgespannten Halbgeraden, und wir schneiden mit den beiden parallelen Geraden durch die eingezeichneten Vektoren $\lambda\vec{w}$ und $\vec{w}$. Dabei sollen die fett eingezeichneten Vektoren die mit λ multiplizierten sein; im Bild ist $\lambda = 0{,}4$.

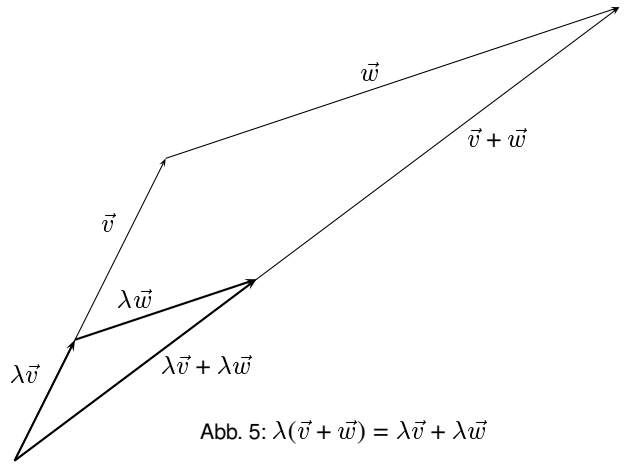

Abb. 5: $\lambda(\vec{v}+\vec{w}) = \lambda\vec{v} + \lambda\vec{w}$

Das andere Distributivgesetz $(\lambda+\mu)\vec{v} = \lambda\vec{v} + \mu\vec{v}$ ist ziemlich trivial: Da sich alles auf der von $\vec{v}$ aufgespannten Geraden abspielt und wir diese mit der reellen Zahlengeraden identifizieren können, läßt sich diese Regel auf das gewöhnliche Distributivgesetz in $\mathbb{R}$ zurückführen, genauso wie sich die Regel $(\lambda\mu)\vec{v} = \lambda(\mu\vec{v})$ auf das gewöhnliche Assoziativgesetz der Multiplikation in $\mathbb{R}$ zurückführen läßt.

b) Definition des Vektorraums

Damit haben wir alle Rechenregeln zusammen, die wir für die Definition eines Vektorraums brauchen. Da wir Vektoren auch mit Zahlen multiplizieren wollen, müssen wir zwei Arten von Objekten betrachten:

Vektoren, die wir weiterhin mit $\vec{v}$, $\vec{w}$ *usw.* bezeichnen, sowie Skalare, für die wir griechische Buchstaben verwenden.

Für die Skalare lassen wir, wie bereits in §1*c)* diskutiert, Elemente eines beliebigen Körpers zu; für den Anfänger ist es wahrscheinlich am einfachsten, sich die Skalare zunächst als reelle Zahlen vorzustellen.

Definition: k sei ein Körper. Eine Menge V heißt *Vektorraum* über k oder k-Vektorraum, wenn es zwei Verknüpfungen

$$+: V \times V \to V \quad \text{und} \quad \cdot: k \times V \to V$$

gibt, so daß gilt:

I.1) Das Assoziativgesetz der Vektoraddition

$$(\vec{u}+\vec{v})+\vec{w} = \vec{u}+(\vec{v}+\vec{w}) \qquad \text{für alle } \vec{u},\vec{v},\vec{w} \in V$$

I.2) Es gibt einen Vektor $\vec{0} \in V$, so daß für jeden Vektor $\vec{v} \in V$ gilt

$$\vec{v}+\vec{0} = \vec{0}+\vec{v} = \vec{v}\,.$$

I.3) Zu jedem Vektor $\vec{v} \in V$ gibt es einen Vektor $-\vec{v} \in V$, so daß

$$\vec{v}+(-\vec{v}) = (-\vec{v})+\vec{v} = \vec{0}\,.$$

I.4) Das Kommutativgesetz der Vektoraddition

$$\vec{u}+\vec{v} = \vec{v}+\vec{u} \qquad \text{für alle } \vec{u},\vec{v} \in V$$

II.1) Das Distributivgesetz bei der Addition von Skalaren

$$(\lambda+\mu)\vec{v} = \lambda\vec{v}+\mu\vec{v} \quad \text{für alle } \lambda,\mu \in k \text{ und alle } \vec{v} \in V\,.$$

II.2) Das Distributivgesetz bei der Addition von Vektoren

$$\lambda(\vec{v}+\vec{w}) = \lambda\vec{v}+\lambda\vec{w} \quad \text{für alle } \lambda \in k \text{ und alle } \vec{v},\vec{w} \in V\,.$$

II.3) Kompatibilität von Körper- und Skalarmultiplikation

$$(\lambda\mu)\vec{v} = \lambda(\mu\vec{v}) \quad \text{für alle } \lambda,\mu \in k \text{ und alle } \vec{v} \in V\,.$$

II.4) Multiplikation mit der Eins

$$1\vec{v} = \vec{v} \quad \text{für alle } \vec{v} \in V\,.$$

II.5) Multiplikation mit der Null *bzw.* mit dem Nullvektor

$$0\vec{v} = \vec{0} \quad \text{für alle } \vec{v} \in V \qquad \text{und} \qquad \lambda\vec{0} = \vec{0} \quad \text{für alle } \lambda \in k\,.$$

Bemerkung: Die Forderungen I.1–I.4 in der Definition des Körpers und des Vektorraums sowie die Forderungen II.1–II.4 in der Körperdefinition sind fast identisch, und in der Tat beschreiben sie eine gemeinsame mathematische Struktur, die sogenannte *abelsche Gruppe*. Da wir diese nicht weiter benötigen werden, sei auf Einzelheiten verzichtet.

Vektoren und Vektorräume sind als mathematische Begriffe recht jung: Rechnerische Methoden zur Lösung geometrischer Probleme wurden zwar schon ab etwa 1636 von RENÉ DESCARTES (1596–1650) eingesetzt (kartesische Koordinaten), aber erst gegen Mitte des 19. Jahrhunderts wurden Ansätze entwickelt, um geometrische Objekte *koordinatenfrei* algebraisch zu behandeln. Ein erster Durchbruch war das 1844 erschienene Buch *Die Ausdehnungslehre* von HERMANN GÜNTER GRASSMANN (1809–1877, oberes Bild): Er betrachtete abstrakte Objekte, die unter anderem alle Vektorraumaxiome erfüllten, die darüber hinaus allerdings auch miteinander multipliziert werden konnten, so daß er etwas komplizierteres als einen Vektorraum definiert hatte: eine sogenannte Algebra. Sie spielt noch heute eine große Rolle bei der Charakterisierung der Lage zweier Vektorräume ineinander. 1888 definierte GIUSEPPE PEANO (1858–1932, unteres Bild) in seinem Buch *Calcolo geometrico secondo l'Ausdehnungslehre di H. Grassmann preceduto dalle operazioni della logica deduttiva* Vektorräume (über $\mathbb{R}$) im obigen Sinne; in diesem Buch treten auch erstmalig mengentheoretische Symbole wie $\cap$, $\cup$ und $\in$ auf. Ab etwa 1920 wandte STEFAN BANACH (1892–1945) PEANOs Theorie an auf Funktionenräume und lineare Operatoren.

c) Erste Beispiele

Standardbeispiel sind natürlich die $\mathbb{R}$-Vektorräume $\mathbb{R}^n$. Wir schreiben ihre Elemente als Spaltenvektoren der Form

$$\vec{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}, \quad \vec{w} = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}, \quad \ldots$$

und haben die beiden Rechenoperationen

$$\vec{v} + \vec{w} = \begin{pmatrix} v_1 + w_1 \\ \vdots \\ v_n + w_n \end{pmatrix} \quad \text{und} \quad \lambda\vec{v} = \begin{pmatrix} \lambda v_1 \\ \vdots \\ \lambda v_n \end{pmatrix}.$$

Alle Rechenregeln folgen sofort aus den entsprechenden Regeln für reelle Zahlen, und genauso können wir auch für einen beliebigen Körper k die k-Vektorräume k^n definieren.

Auf den ersten Blick seltsam erscheint, daß $\mathbb{R}$ ein $\mathbb{Q}$-Vektorraum ist: Vektoraddition ist die gewöhnliche Addition reeller Zahlen und Multiplikation mit Skalaren die Multiplikation einer reellen Zahl mit einer rationalen. Auch hier folgen alle Vektorraumaxiome sofort aus den üblichen Rechenregeln für reelle Zahlen, für die es natürlich gleichgültig ist, daß hier einige der betrachteten Zahlen sogar rational sind.

Interessanter ist das folgende Beispiel: Für eine natürliche Zahl $n \in \mathbb{N}$ und eine offene Teilmenge U von $\mathbb{R}$, als z.B. ein offenes Intervall $(a,\, b)$ oder $\mathbb{R}$ selbst, definieren wir die Menge

$$\mathcal{C}^n(U, \mathbb{R}) = \left\{ f\colon U \to \mathbb{R} \;\middle|\; f \text{ ist (mindestens) } n\text{-mal stetig differenzierbar} \right\}.$$

Für deren Elemente seien Addition und Skalarmultiplikation punktweise definiert, d.h. für $f, g \in \mathcal{C}^n(U, \mathbb{R})$ und $\lambda \in \mathbb{R}$ setzen wir

$$f + g\colon \begin{cases} U \to \mathbb{R} \\ t \mapsto f(t) + g(t) \end{cases} \quad \text{und} \quad \lambda f\colon \begin{cases} U \to \mathbb{R} \\ t \mapsto \lambda f(t) \end{cases}.$$

Abbildung sechs zeigt für $(a,\, b) = (0,\, 3\pi)$ zu den beiden dünn eingezeichneten Funktionen $f(t) = \sin t$ und $g(t) = \sin 3t$ die dick eingezeichnete Funktion $f + g$, und Abbildung sieben zeigt f zusammen mit der Funktion $2f$.

Damit dies alles wohldefiniert ist, müssen wir uns noch überlegen, daß mit f und g die Funktionen $f + g$ und λf wieder in $\mathcal{C}^n(U, \mathbb{R})$ liegen. Das ist aber klar, denn die Summe zweier stetiger *bzw.* differenzierbarer Funktionen ist wieder stetig *bzw.* differenzierbar, und wegen der Rechenregel $(f + g)' = f' + g'$ gilt dies auch für die höheren Ableitungen. Genauso kann man für λf argumentieren. Da alle Rechenoperationen auf

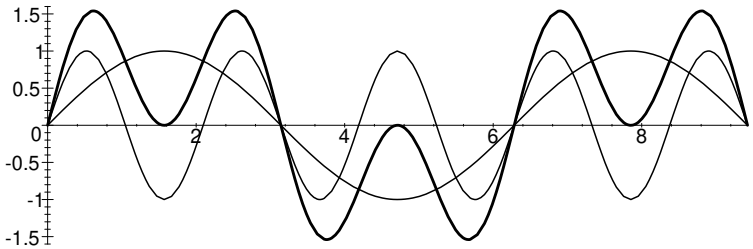

Abb. 6: Die Summe von $f(t) = \sin t$ und $g(t) = \sin 3t$

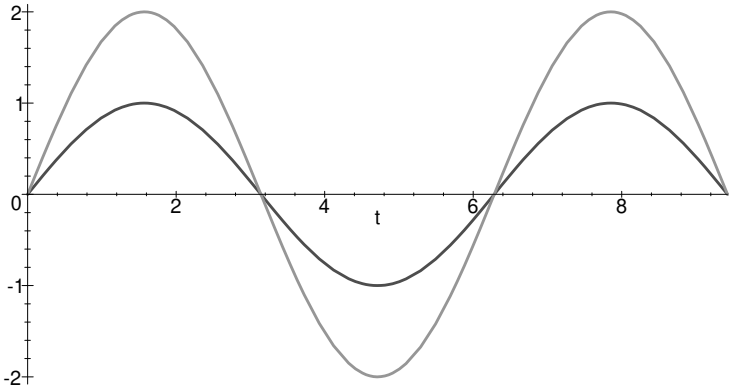

Abb. 7: $f(t) = \sin t$ zusammen mit $2f$

die gewöhnliche reelle Addition und Multiplikation für die Funktionswerte zurückgeführt ist, folgen die Vektorraumaxiome aus den üblichen Rechenregeln für reelle Zahlen: Um etwa das Assoziativgesetz

$$(f + g) + h = f + (g + h)$$

nachzuweisen, müssen wir zeigen, daß für jede reelle Zahl t die Funktionen auf beiden Seiten denselben Wert haben, d.h.

$$\big((f + g) + h\big)(t) = \big(f + (g + h)\big)(t) \quad \text{für alle } t \in \mathbb{R}\,.$$

Dazu rechnen wir beide Seiten aus:

$$\big((f + g) + h\big)(t) = (f + g)(t) + h(t) = \big(f(t) + g(t)\big) + h(t)$$

und

$$\big(f + (g + h)\big)(t) = f(t) + (g + h)(t) = f(t) + \big(g(t) + h(t)\big)\,,$$

und die beiden rechten Seiten stimmen in der Tat überein nach dem Assoziativgesetz für die Addition reeller Zahlen.

Die restlichen Axiome folgen genauso, nur etwas einfacher.

Ganz entsprechend lassen sich auch die Mengen

$$\mathcal{C}^0(U, \mathbb{R}) = \big\{ f\colon U \to \mathbb{R} \;\big|\; f \text{ ist stetig} \big\}$$

und

$$\mathcal{C}^\infty(U, \mathbb{R}) = \big\{ f\colon U \to \mathbb{R} \;\big|\; f \text{ ist beliebig oft differenzierbar} \big\}$$

sowie

$$\mathcal{C}^\omega(U, \mathbb{R}) = \left\{ f\colon U \to \mathbb{R} \;\middle|\; \begin{array}{l} f \text{ ist um jeden Punkt } x \in U \text{ durch} \\ \text{eine TAYLOR-Reihe darstellbar} \end{array} \right\}$$

zu $\mathbb{R}$-Vektorräumen machen. (Wer noch nicht weiß, was eine TAYLOR-Reihe ist, wird es im nächsten Kapitel lernen.)

Als trivialstes Beispiel überhaupt haben wir schließlich noch über jedem Körper k den Nullvektorraum, der nur aus dem Nullvektor $\vec{0}$ besteht.

d) Lineare Abbildungen

Vektorräume werden erst richtig interessant, wenn man mit ihren Elementen etwas mehr tun kann als sie nur zu addieren und mit Skalaren zu multiplizieren. In der Geometrie etwa möchte man Vektoren gelegentlich auch drehen, bei Vektorräumen von differenzierbaren Funktionen möchte man deren Elemente differenzieren und so weiter. Viele derartige Operationen lassen sich unter dem Begriff der linearen Abbildung einordnen:

Definition: *a)* Eine Abbildung $\varphi\colon V \to W$ heißt *linear,* wenn für alle Vektoren $\vec{u}, \vec{v} \in V$ und alle $\lambda, \mu \in k$ gilt:

$$\varphi(\lambda\vec{u} + \mu\vec{v}) = \lambda\varphi(\vec{u}) + \mu\varphi(\vec{v})\,.$$

b) Unter dem *Kern* von φ verstehen wir die Menge

$$\operatorname{Kern}\varphi \underset{\text{def}}{=} \left\{ \vec{v} \in V \;\middle|\; \varphi(\vec{v}) = \vec{0} \right\} .$$

c) Das *Bild* von φ ist die Menge

$$\operatorname{Bild}\varphi \underset{\text{def}}{=} \left\{ \vec{w} \in W \;\middle|\; \text{Es gibt } \vec{v} \in V \text{ mit } \varphi(\vec{v}) = \vec{w} \right\} .$$

Die beiden allereinfachsten Beispiele für lineare Abbildungen sind für jeden Vektorraum V die identische Abbildung $V \to V$ sowie die Nullabbildung, die jedem Vektor $\vec{v} \in V$ den Nullvektor zuordnet. Letztere kann man wahlweise als Abbildung $V \to V$ oder als Abbildung von V in den Nullvektorraum auffassen.

Ebenfalls völlig trivial ist die Linearität von *Projektionen* wie etwa der Projektion $\mathbb{R}^3 \to \mathbb{R}^2$, die jedem Vektor seine ersten beiden Komponenten zuordnet.

Ein etwas interessanteres Beispiel einer linearen Abbildung ist

$$\varphi\colon \begin{cases} \mathbb{R}^3 \to \mathbb{R}^2 \\ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto \begin{pmatrix} x - y \\ y - z \end{pmatrix} \end{cases} ;$$

sie ist linear, denn

$$\begin{aligned} \varphi\left(\lambda \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} + \mu \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} \right) &= \varphi\left(\begin{pmatrix} \lambda x_1 + \mu x_2 \\ \lambda y_1 + \mu y_2 \\ \lambda z_1 + \mu z_2 \end{pmatrix} \right) \\ &= \begin{pmatrix} \lambda x_1 + \mu x_2 - \lambda y_1 - \mu y_2 \\ \lambda y_1 + \mu y_2 - \lambda z_1 - \mu z_2 \end{pmatrix} \end{aligned}$$

und

$$\begin{aligned} \lambda \cdot \varphi\left(\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \right) + \mu \cdot \varphi\left(\begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} \right) &= \lambda \begin{pmatrix} x_1 - y_1 \\ y_1 - z_1 \end{pmatrix} + \mu \begin{pmatrix} x_2 - y_2 \\ y_2 - z_2 \end{pmatrix} \\ &= \begin{pmatrix} \lambda x_1 - \lambda y_1 + \mu x_2 - \mu y_2 \\ \lambda y_1 - \lambda z_1 + \mu y_2 - \mu z_2 \end{pmatrix} , \end{aligned}$$

was offensichtlich dasselbe ist.

Bei Vektorräumen von Funktionen ist beispielsweise für jeden Punkt $t_0 \in (a,\, b)$ die Auswertungsabbildung

$$\mathcal{C}^n\big((a,\, b), \mathbb{R}\big) \to \mathbb{R}; \quad f \mapsto f(t_0)$$

nach Definition der Vektorraumoperationen von $\mathcal{C}^n\big((a,\, b), \mathbb{R}\big)$ linear, denn $\lambda f + \mu g$ wurde ja gerade so definiert, daß für t_0 wie auch für jeden anderen Punkt aus $(a,\, b)$ gilt

$$\big(\lambda f + \mu g\big)(t_0) = \lambda f(t_0) + \mu g(t_0) .$$

Allgemeiner können wir auch die *Abtastung* einer Funktion betrachten: Für vorgegebene Punkte $t_1, \ldots, t_N \in (a,\, b)$ definieren wir die Abbildung

$$\varphi\colon \begin{cases} \mathcal{C}^n\big((a,\, b), \mathbb{R}\big) \to \mathbb{R}^N \\ \qquad f \mapsto \begin{pmatrix} f(t_1) \\ \vdots \\ f(t_N) \end{pmatrix} \end{cases} ,$$

die f an N Argumenten auswertet. Anwendung ist beispielsweise die Digitalisierung eines Signals, etwa eines Musikstücks für eine CD. Hier würde die Funktion f die zeitliche Variation des Schalldrucks beschreiben (die man zumindest als stetig annehmen kann, d.h. $n = 0$), und die Punkte t_i wären gleichmäßig über die Länge des Musikstücks verteilt, jeweils 44 100 Stück pro Sekunde.

Diese Abbildung ist linear, weil jede ihrer Komponentenabbildungen $f \mapsto f(t_i)$ linear ist. Wir können die Linearität dieser Digitalisierung eines Signals aber auch inhaltlich interpretieren: Die Eigenschaft

$$\varphi(\lambda f + \mu g) = \lambda \varphi(f) + \mu \varphi(g)$$

bedeutet für positive λ und μ, daß es gleichgültig ist, ob man zwei verschiedene Signale (z.B. Mikrophonkanäle) zunächst in einem analogen Mischpult vereinigt und dann digitalisiert oder zunächst digitalisiert und dann digital mischt. (Dieses setzt natürlich voraus, daß man sowohl analog als auch digital mit perfekter Genauigkeit arbeitet – keine sehr realistische Annahme.)

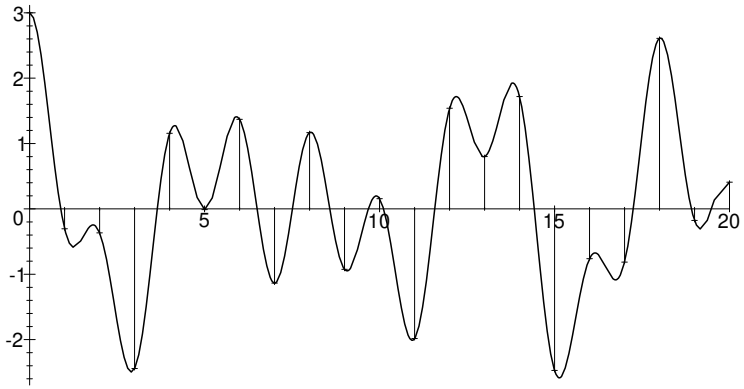

Abb. 8: Abtastung eines Signals

Ein anderes Beispiel einer linearen Abbildung zwischen Vektorräumen von Funktionen ist die Differentiation

$$\mathcal{C}^{n+1}\big((a,b),\mathbb{R}\big) \to \mathcal{C}^{n}\big((a,b),\mathbb{R}\big); \quad f \mapsto \dot{f}\,,$$

denn $(\lambda f + \mu g)' = \lambda f' + \mu g'$. Auch die Abbildung

$$\mathcal{C}^{2}\big((a,b),\mathbb{R}\big) \to \mathcal{C}^{0}\big((a,b),\mathbb{R}\big); \quad f \mapsto f'' + \omega^2 f$$

ist für jedes $\omega \in \mathbb{R}$ linear; ihr Kern besteht genau aus jenen Funktionen $f(t)$, die der Schwingungsdifferentialgleichung

$$f''(t) + \omega^2 f(t) = 0$$

genügen, enthält also beispielsweise die Funktionen $\cos\omega t$ und $\sin\omega t$.

e) Untervektorräume

Kern und Bild einer linearen Abbildung werden im allgemeinen unendliche Mengen sein, so daß selbst bei Vektorräumen wie dem $\mathbb{R}^3$ zunächst nicht ganz klar ist, wie man sie mit endlichem Aufwand beschreiben kann. Bei nichtlinearen Abbildungen kann so etwas in der Tat ein großes Problem sein, aber hier im Linearen reichen unsere vorhandenen Werkzeuge zumindest für Vektorräume wie einen $\mathbb{R}^n$ völlig aus. Zur Klärung der Begriffe beginnen wir mit einer

Definition: Eine Teilmenge $U \subseteq V$ eines k-Vektorraums V heißt *Untervektorraum,* in Zeichen $U \leq V$, wenn U nicht leer ist und mit je zwei Vektoren $\vec{u}$, $\vec{v} \in U$ und Skalaren $\lambda, \mu \in k$ auch den Vektor $\lambda\vec{u} + \mu\vec{v}$ enthält.

Lemma: $\varphi\colon V \to W$ sei eine lineare Abbildung zwischen zwei k-Vektorräumen. Dann ist Kern φ ein Untervektorraum von V und Bild φ ein Untervektorraum von W.

Beweis: Sind $\vec{u}$ und $\vec{v}$ Elemente des Kerns von $\varphi\colon V \to W$ und $\lambda, \mu \in k$ Skalare, so ist

$$\varphi(\lambda\vec{u} + \mu\vec{v}) = \lambda\varphi(\vec{u}) + \mu\varphi(\vec{u}) = \lambda\vec{0} + \mu\vec{0} = \vec{0}\,,$$

also liegt auch $\lambda\vec{u} + \mu\vec{v}$ im Kern von φ. Außerdem ist dieser nicht leer, denn wegen

$$\varphi(\vec{0}) = \varphi(0 \cdot \vec{0}) = 0 \cdot \varphi(\vec{0}) = \vec{0}$$

liegt der Nullvektor in Kern φ. Also ist der Kern ein Untervektorraum.

Ähnlich ist die Situation für das Bild: Für zwei Vektoren $\vec{v}, \vec{w} \in$ Bild φ gibt es Vektoren $\vec{r}, \vec{s} \in V$, so daß $\varphi(\vec{r}) = \vec{v}$ und $\varphi(\vec{s}) = \vec{w}$ ist. Wegen der Linearität von φ liegt dann für zwei Skalare $\lambda, \mu \in k$ auch

$$\lambda\vec{v} + \mu\vec{w} = \lambda\varphi(\vec{r}) + \mu\varphi(\vec{s}) = \varphi(\lambda\vec{r} + \mu\vec{s})$$

im Bild von φ, das somit ein Untervektorraum von W ist. ■

Kern und Bild einer linearen Abbildung haben natürlich etwas mit deren Injektivität und Surjektivität zu tun; erinnern wir uns zunächst an die Definition dieser Begriffe:

Definition: *a)* Eine Abbildung $\varphi\colon M \to N$ zwischen zwei Mengen heißt *injektiv,* wenn keine zwei verschiedenen Elemente von M dasselbe Bild haben, d.h. aus der Gleichheit von $\varphi(m_1)$ und $\varphi(m_2)$ folgt für zwei Elemente $m_1, m_2 \in M$, daß $m_1 = m_2$ ist.
b) φ heißt *surjektiv,* wenn es zu jedem $n \in N$ (mindestens) ein $m \in M$ gibt, so daß $\varphi(m) = n$ ist.
c) φ heißt *bijektiv* oder auch „eins-zu-eins (1-1)“, wenn φ injektiv und surjektiv ist.

Lemma: $\varphi\colon V \to W$ ist genau dann injektiv, wenn Kern φ der Nullvektorraum ist; φ ist genau dann surjektiv, wenn Bild $\varphi = W$ ist.

Beweis: Die zweite Aussage ist zu trivial, als daß man etwas dazu sagen müßte, betrachten wir also die erste. Falls φ injektiv ist, hat insbesondere der Nullvektor nur ein einziges Urbild, d.h. der Kern besteht nur aus dem Nullvektor, der natürlich immer im Kern liegt. Ist umgekehrt Kern φ der Nullraum und haben zwei Vektoren $\vec{u}, \vec{v} \in V$ dasselbe Bild, so ist

$$\varphi(\vec{u} - \vec{v}) = \varphi(\vec{u}) - \varphi(\vec{v}) = \vec{0}\,,$$

d.h. $\vec{u} - \vec{v}$ liegt im Kern und muß daher gleich dem Nullvektor sein, so daß $\vec{u} = \vec{v}$ ist. Dies zeigt die Injektivität von φ. ∎

Als Beispiel einer Anwendung dieses Lemmas betrachten wir noch einmal die Digitalisierung eines Signals: Aufgrund der hoch gelobten CD-Qualität erwarten wir, daß in diesem Fall die Abtastung eine „einigermaßen injektive“ lineare Abbildung ist. Das Wort „einigermaßen injektiv“ ist zwar kein wohldefinierter mathematischer Begriff, aber schon die Tatsache, daß bei einer CD die Abtastwerte nicht als reelle Zahlen gespeichert werden, sondern als 16bit-Zahlen, macht eine „echte“ Injektivität unmöglich. Überlegen wir uns, was sonst noch alles schiefgehen kann.

Nach dem gerade bewiesenen Lemma reicht es, wenn wir den Kern der Abbildung kennen. Dort liegt, bei einer Abtastung mit 44 100 Hz und in Sekunden gemessener Zeit, beispielsweise die Funktion

$$f(t) = \sin\bigl(44\,100\,\pi t\bigr) = \sin\bigl(22\,050 \cdot 2\pi t\bigr)\,;$$

denn für jedes ganzzahlige Vielfache von $1/44\,100$ ist das Argument des Sinus ein ganzzahliges Vielfaches von π, der Sinus also Null.

Die Funktion $f(t)$ entspricht einer reinen Schwingung mit einer Frequenz von 22,05 kHz. Solche Frequenzen sind zwar sehr wichtig für die Navigation von Fledermäusen, sie sind aber unhörbar für Käufer von CDs, so daß uns dieses Element des Kerns nicht weiter stört.

Betrachten wir aber beispielsweise die Funktionen

$$g(t) = \sin\bigl(66\,150\,\pi t\bigr) \quad \text{und} \quad h(t) = \sin\bigl(22\,050\,\pi t\bigr)\,.$$

Für $k \in \mathbb{Z}$ und $t = k/44\,100$ ist

$$g(t) = g\left(\frac{k}{44\,100}\right) = \sin\left(66\,150\pi \cdot \frac{k}{44\,100}\right) = \sin\left(\frac{3k\pi}{2}\right)$$
$$= \begin{cases} 0 & \text{für gerades } k \\ -1 & \text{für } k \equiv 1 \bmod 4 \\ 1 & \text{für } k \equiv 3 \bmod 4 \end{cases}$$

und

$$h(t) = h\left(\frac{k}{44\,100}\right) = \sin\left(22\,050\pi \cdot \frac{k}{44\,100}\right) = \sin\left(\frac{k\pi}{2}\right)$$
$$= \begin{cases} 0 & \text{für gerades } k \\ 1 & \text{für } k \equiv 1 \bmod 4 \\ -1 & \text{für } k \equiv 3 \bmod 4 \end{cases},$$

wobei $k \equiv a \bmod b$ bedeuten soll, daß $k - a$ durch b teilbar ist. Damit sind die beiden Funktionen g und h an allen Abtaststellen entgegengesetzt gleich, d.h. die Funktion $g + h$ liegt im Kern von φ.

Dieses Element des Kern stört uns erheblich mehr, denn es hat zur Folge, daß die beiden Funktion $g(t) = \sin\bigl(66\,150\,\pi t\bigr)$ und $-h(t) = -\sin\bigl(22\,050\,\pi t\bigr)$ auf dieselbe Weise digitalisiert werden. g beschreibt aber einen für Menschen unhörbaren Ton mit einer Frequenz von 33,075 kHz, während h mit nur 11,025 kHz durchaus hörbar ist. Abbildung neun zeigt die beiden Schwingungen; die Zeitachse ist der besseren Übersicht wegen in Millisekunden beschriftet, und die Abtastwerte sind durch Quadrate markiert.

Die Digitalisierungsabbildung kann also höchstens dann injektiv sein, wenn wir uns auf Funktionen beschränken, an deren Aufbau keine Schwingungen mit einer Frequenz von 22,05 kHz oder höher beteiligt sind. Was das bedeutet, und ob dann wirklich Injektivität gilt, werden wir in der *Höheren Mathematik II* im Kapitel über harmonische Analyse genauer untersuchen.

f) Lineare Abhängigkeit

Im $\mathbb{R}^3$ definieren zwei Vektoren eine Ebene – es sei denn, sie liegen, wenn man sie am gleichen Anfangspunkt beginnen läßt, auf einer Geraden, d.h einer der beiden Vektoren ist ein Vielfaches des anderen.

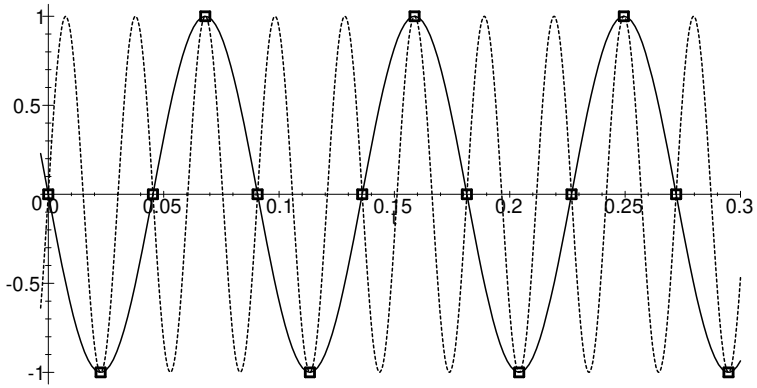

Abb. 9: Zwei verschiedene Signale, die gleich abgetastet werden

Entsprechend spannen drei Vektoren im allgemeinen den gesamten $\mathbb{R}^3$ auf – es sei denn, sie liegen, wenn man sie am gleichen Anfangspunkt beginnen läßt, in einer Ebenen, d.h. einer der drei ist als Summe von Vielfachen der anderen beiden darstellbar.

Der Begriff der *linearen Abhängigkeit* verallgemeinert diese Ausnahmebedingungen so, daß sie auf beliebige Vektorräume angewandt werden können:

Definition: $\vec{v}_1, \ldots, \vec{v}_n$ seien Elemente des k-Vektorraums V.

a) Eine *Linearkombination* von $\vec{v}_1, \ldots, \vec{v}_n$ ist eine Summe der Form

$$\lambda_1 \vec{v}_1 + \cdots + \lambda_n \vec{v}_n$$

mit Skalaren $\lambda_i \in k$; ist diese Summe gleich dem Vektor $\vec{v} \in V$, so sagen wir, $\vec{v}$ sei als Linearkombination von Vektoren aus M darstellbar.

b) Die Menge aller Vektoren, die sich als Linearkombination der Vektoren $\vec{v}_1, \ldots, \vec{v}_n$ darstellen lassen, bezeichnen wir mit $[\vec{v}_1, \ldots, \vec{v}_n]$; wir nennen sie das *Erzeugnis* von $\vec{v}_1, \ldots, \vec{v}_n$.

c) Eine Linearkombination wie in *a)* heißt *nichttrivial,* falls mindestens ein λ_i von Null verschieden ist; ansonsten heißt sie *trivial.*

d) Die Vektoren $\vec{v}_1, \ldots, \vec{v}_n$ heißen *linear unabhängig,* wenn der Nullvektor nicht als nichttriviale Linearkombination von $\vec{v}_1, \ldots, \vec{v}_n$ darstellbar ist, d.h. eine Gleichung der Form

$$\lambda_1 \vec{v}_1 + \cdots + \lambda_n \vec{v}_n = \vec{0}$$

kann nur gelten, wenn alle λ_i verschwinden.

e) Sind $\vec{v}_1, \ldots, \vec{v}_n$ *nicht* linear unabhängig, so bezeichnen wir sie als *linear abhängig.*

f) Eine *Teilmenge* $M \subseteq V$ eines Vektorraums V heißt *linear unabhängig,* wenn jede Auswahl endlich vieler verschiedener Vektoren $\vec{v}_1, \ldots \vec{v}_m$ (für beliebiges $m \in \mathbb{N}$) linear unabhängig ist.

g) Das *Erzeugnis* $[M]$ einer Teilmenge $M \subseteq V$ eines Vektorraums V ist die Menge aller Vektoren aus V, die als Linearkombination aus endlich vielen Vektoren aus V dargestellt werden können.

Beispielsweise sind also die Vektoren

$$\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \quad \begin{pmatrix} 2 \\ 4 \\ 6 \end{pmatrix} \in \mathbb{R}^3$$

linear abhängig, da der zweite das Zweifache des ersten ist, und auch die Vektoren

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 2 \\ 3 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \in \mathbb{R}^3$$

sind linear abhängig, denn

$$\lambda \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \mu \begin{pmatrix} 2 \\ 3 \\ 0 \end{pmatrix} + \nu \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \lambda + 2\mu + \nu \\ 3\mu + \nu \\ 0 \end{pmatrix}$$

ist gleich dem Nullvektor wann immer $\nu = -3\mu$ und $\lambda = -2\mu - \nu = \mu$ ist. Eine nichttriviale Darstellung des Nullvektors ist beispielsweise

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \\ 0 \end{pmatrix} - 3 \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Die drei Vektoren

$$\begin{pmatrix}1\\0\\0\end{pmatrix}, \quad \begin{pmatrix}0\\1\\0\end{pmatrix}, \quad \begin{pmatrix}0\\0\\1\end{pmatrix} \in \mathbb{R}^3$$

dagegen sind linear unabhängig, denn

$$\lambda_1 \begin{pmatrix}1\\0\\0\end{pmatrix} + \lambda_2 \begin{pmatrix}0\\1\\0\end{pmatrix} + \lambda_3 \begin{pmatrix}0\\0\\1\end{pmatrix} = \begin{pmatrix}\lambda_1\\\lambda_2\\\lambda_3\end{pmatrix}$$

ist genau dann gleich dem Nullvektor, wenn alle λ_i verschwinden.

Allgemein sind die Vektoren $\vec{v}_1, \dots, \vec{v}_n$ aus einem beliebigen Vektorraum V dann trivialerweise linear abhängig, wenn zwei Vektoren $\vec{v}_i$ und $\vec{v}_j$ (mit $j \neq i$) gleich sind, denn dann ist beispielsweise

$$1 \cdot \vec{v}_i + (-1) \cdot \vec{v}_j = \vec{0}$$

eine nichttriviale Darstellung des Nullvektors. Ebenfalls trivial ist die lineare Abhängigkeit, falls einer der Vektoren $\vec{v}_i$ gleich dem Nullvektor ist: Dann ist bereits

$$1 \cdot \vec{v}_i = \vec{0}$$

eine solche Darstellung. Eine Menge, die den Nullvektor enthält, ist also stets linear abhängig.

Auch in Vektorräumen von Funktionen können wir leicht Beispiele für lineare Abhängigkeit und Unabhängigkeit finden. In $\mathcal{C}^0(\mathbb{R}, \mathbb{R})$ sind etwa Sinus und Kosinus linear unabhängig, denn gäbe es $\lambda_{1/2} \in \mathbb{R}$ mit

$$\lambda_1 \sin x + \lambda_2 \cos x = 0 \quad \text{für alle } x \in \mathbb{R}$$

mit $\lambda_1 \neq 0$, so wäre

$$\tan x = \frac{\sin x}{\cos x} = -\frac{\lambda_2}{\lambda_1}$$

eine konstante Funktion; wäre $\lambda_2 \neq 0$, könnten wir entsprechend auf die Konstanz des Kotangens schließen.

Genauso sieht man, daß die Funktionen $\sin^2 x$ und $\cos^2 x$ linear unabhängig sind, denn auch die Quadrate von Tangens und Kotangens

sind nicht konstant. Dagegen sind die drei Funktionen $\sin^2 x$, $\cos^2 x$ und 1 (konstante Funktion) linear abhängig, denn

$$\sin^2 x + \cos^2 x - 1 = 0 \quad \text{für alle } x \in \mathbb{R}\,.$$

Elementare Beispiele von Linearkombinationen sind etwa die Zerlegung eines Vektors in seine Komponenten entlang der Achsen eines gegebenen Koordinatensystems, also etwa

$$\lambda \begin{pmatrix}1\\0\\0\end{pmatrix} + \mu \begin{pmatrix}0\\1\\0\end{pmatrix} + \nu \begin{pmatrix}0\\0\\1\end{pmatrix} = \begin{pmatrix}\lambda\\\mu\\\nu\end{pmatrix},$$

oder die „übliche“ Darstellung eines Polynoms durch Potenzen der Variable:

$$f(x) = \lambda_0 + \lambda_1 x + \lambda_2 x^2 + \lambda_3 x^3\,.$$

Im Vektorraum $V = \mathbb{R}[x]$ aller reeller Polynome in x ist demgemäß das Erzeugnis $[1, x, x^2, x^3]$ der Untervektorraum aller Polynome vom Grad höchstens drei.

Auch für Erzeugnisse unendlicher Mengen gibt es einfache Beispiele in $\mathbb{R}[x]$; beispielsweise ist das Erzeugnis

$$[1, x^2, x^4, x^6, x^8, \dots]$$

der Menge aller gerader Potenzen gleich die Menge aller Polynome, in denen nur gerade x-Potenzen vorkommen, also (wie man sich leicht überlegt) gleich der Menge aller gerader Polynome, d.h. der Polynome $f \in \mathbb{R}[x]$ mit $f(-x) = f(x)$ für alle $x \in \mathbb{R}$.

Da Konstanten und x-Potenzen stetige Funktionen sind, können wir auch im Vektorraum $\mathcal{C}^0(\mathbb{R}, \mathbb{R})$ aller stetiger Funktionen das Erzeugnis derselben Menge betrachten, und wieder erhalten wir die Menge aller gerader Polynome. Das mag auf den ersten Blick verwundern, da einige vielleicht erwartet hätten, daß auch die Funktion

$$\cos x = 1 - \frac{x^2}{2} + \frac{x^4}{24} - \frac{x^6}{720} + - \cdots = \sum_{i=0}^{\infty} (-1)^i \frac{x^{2i}}{(2i)!}$$

in $[1, x^2, x^4, x^6, x^8, \dots]$ liegt, aber dies ist eine *unendliche* Summe, und $[M]$ war ausdrücklich definiert als die Menge aller Linearkombinationen, in denen jeweils nur *endlich* viele Elemente aus M auftreten.

In der Musik (und in der Signalverarbeitung) spielen Linearkombinationen von Sinus- und Kosinusschwingungen eine große Rolle: Der Aufbau eines Tons aus Grundschwingung und Oberschwingungen ist mathematisch betrachtet einfach eine Linearkombination

$$f(t) = \sum_{i=1}^{n} \sin 2\pi i \nu t\,,$$

wobei ν die (Grund-)Frequenz des Tons ist. Bei einem Orchester, das den Kammerton a auf 440 Hz festlegt, sind also alle möglichen Klänge, die dieser Ton auf den verschiedenen Instrumenten annehmen kann, Funktionen aus dem Erzeugnis

$$[\sin 440 \cdot 2\pi t,\ \sin 880 \cdot 2\pi t,\ \sin 1320 \cdot 2\pi t,\ \dots] \leq \mathcal{C}^0(\mathbb{R},\ \mathbb{R})\,.$$

Abbildung zehn zeigt den Ton, den die g-Saite einer Geige produziert zusammen mit der (kaum sichtbaren) Grundschwingung von 196 Hz sowie den ersten acht Oberschwingungen; außerdem ist zum Vergleich gestrichelt eine reine Schwingung der Frequenz 196 Hz eingezeichnet. Wie man sieht, spielen in diesem Beispiel die Oberschwingungen mit der doppelten und der dreifachen Grundfrequenz die größte Rolle.

(Wer selbst Töne aus Grund- und Oberschwingungen synthetisieren möchte, findet unter `http://www.gac.edu/~huber/fourier/` ein Java-Applet, das die entsprechenden Summenkurven zeichnen und die dazugehörigen Töne hörbar machen kann.)

Linearkombinationen sind somit ein einfaches Mittel, um aus relativ wenigen einfachen Funktionen oder Vektoren kompliziertere aufzubauen. Insbesondere bieten sie auch die Möglichkeit, Untervektorräume mit endlichem Aufwand zu beschreiben: Im $\mathbb{R}^n$ etwa ist jeder Untervektorraum mit Ausnahme des Nullraums $\{\vec{0}\}$ eine unendliche Menge, aber wie wir bald sehen werden, läßt sich jeder dieser Untervektorräume als Erzeugnis von endlich vielen Vektoren darstellen.

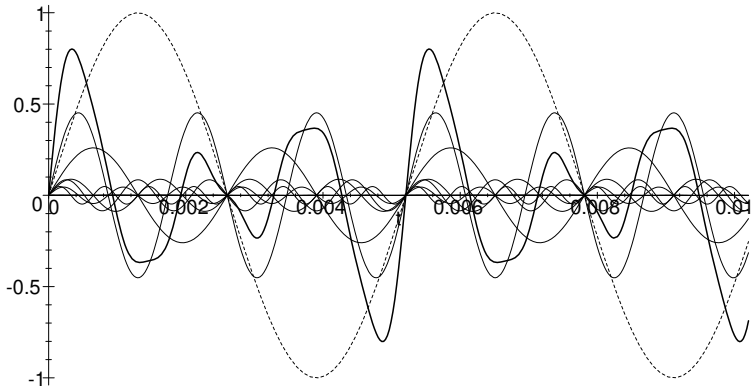

Abb. 10: Ton der g-Saite einer Geige und seine Komponenten

Als ersten Schritt dazu wollen wir uns überlegen, daß die Teilmenge $[M]$ stets ein Untervektorraum ist:

Lemma: Für jede Teilmenge M eines k-Vektorraums V ist $[M] \leq V$ ein Untervektorraum von V; es ist der kleinste Untervektorraum von V, der M enthält.

Beweis: Nach dem Untervektorraumkriterium müssen wir zeigen, daß $[M]$ nicht leer ist und mit je zwei Vektoren $\vec{u}, \vec{v} \in [M]$ und zwei Skalaren $\lambda, \mu \in k$ auch den Vektor $\lambda\vec{u} + \mu\vec{v}$ enthält.

Die erste Eigenschaft ist (fast) trivial: Ist $\vec{v}$ irgendein Vektor aus M, so ist $1\vec{v} = \vec{v}$ eine Linearkombination von $\vec{v}$, liegt also in $[M]$, und insbesondere ist damit $M \subseteq [M]$. Die einzige kleine Schwierigkeit ergibt sich, wenn $M = \emptyset$ die leere Menge ist. Hier müssen wir uns auf die übliche Konvention berufen, daß leere Summen gleich Null sein sollen, eine „Linearkombination“ aus null Vektoren als entsprechend gleich dem Nullvektor, der somit auch im Falle $M = \emptyset$ in $[M]$ liegt.

Nun seien

$$\vec{u} = \lambda_1\vec{u}_1 + \dots + \lambda_n\vec{u}_n \quad \text{und} \quad \vec{v} = \lambda_1\vec{v}_1 + \dots + \lambda_m\vec{v}_m$$

zwei Linearkombinationen von Vektoren aus M. Da wir zu jeder Linearkombination Summanden der Form $0\vec{w}$ hinzufügen können, ohne etwas

an der Summe zu ändern, können wir die beiden Linearkombinationen auch in der Form

$$\vec{u} = \alpha_1\vec{w}_1 + \cdots + \alpha_\ell\vec{w}_\ell \quad \text{und} \quad \vec{v} = \beta_1\vec{w}_1 + \cdots + \beta_\ell\vec{w}_\ell$$

schreiben, wobei

$$\{\vec{w}_1, \ldots, \vec{w}_\ell\} = \{\vec{u}_1, \ldots, \vec{u}_n\} \cup \{\vec{v}_1, \ldots, \vec{v}_m\}$$

ist mit irgendeiner beliebigen Nummerierung der Elemente. Dann ist aber klar, daß auch

$$\lambda\vec{u} + \mu\vec{w} = (\lambda\alpha_1 + \mu\beta_1)\vec{w}_1 + \cdots + (\lambda\alpha_\ell + \mu\beta_\ell)\vec{w}_\ell$$

eine Linearkombination von Vektoren aus M ist und somit in $[M]$ liegt.

Schließlich müssen wir noch zeigen, daß $[M]$ der *kleinste* Untervektorraum von V ist, der M enthält. Wir wissen bereits, daß $[M]$ ein Untervektorraum von V ist, der M enthält; um zu sehen, daß es der kleinste ist, betrachten wir irgendeinen Untervektorraum U von V ist, der M enthält. Dann ist U insbesondere ein Vektorraum, enthält also mit je zwei Vektoren auch deren sämtliche Linearkombinationen. Induktiv folgt, daß er mit jeder endlichen Anzahl von Vektoren auch deren sämtliche Linearkombinationen enthält, also enthält er mit M auch alle Vektoren aus $[M]$. Damit ist $[M] \subseteq U$ für jeden Untervektorraum U, der M enthält, und $[M]$ ist somit in der Tat der kleinste solche Untervektorraum von V. ∎

Vektorräume wurden früher und werden auch gelegentlich noch heute als *lineare Räume* bezeichnet; da $[M]$ somit der kleinste lineare Raum ist, der M enthält, nennt man $[M]$ auch die *lineare Hülle* von M.

Am ökonomischsten ist die Darstellung eines Untervektorraums $U \leq V$ in der Form $U = [M]$ dann, wenn M möglichst wenig Elemente enthält. Wir wollen uns als nächstes überlegen, daß dies höchstens dann der Fall sein kann, wenn M linear unabhängig ist:

Lemma: Falls die Menge $M \subseteq V$ linear abhängig ist, gibt es ein Element $\vec{v} \in M$, das sich als Linearkombination der übrigen, d.h. von Vektoren aus $M \setminus \{\vec{v}\}$, schreiben läßt. Insbesondere ist dann auch

$$[M] = \big[M \setminus \{\vec{v}\}\big] .$$

Beweis: Wenn M linear abhängig ist, gibt es eine nichttriviale Linearkombination von Vektoren $\vec{v}_i \in M$, so daß

$$\lambda_1\vec{v}_1 + \cdots + \lambda_n\vec{v}_n = \vec{0}$$

ist mit Körperelementen λ_i, die nicht alle gleich Null sind. Sei zum Beispiel $\vec{\lambda}_j \neq 0$. Dann kann obige Gleichung nach $\vec{v}_j$ aufgelöst werden; für $1 < j < n$ etwa ist

$$\vec{v}_j = -\frac{\lambda_1}{\lambda_j}\vec{v}_1 - \cdots - \frac{\lambda_{j-1}}{\lambda_j}\vec{v}_{j-1} - \frac{\lambda_{j+1}}{\lambda_j}\vec{v}_{j+1} - \cdots - \frac{\lambda_n}{\lambda_j}\vec{v}_n ,$$

und entsprechend läßt sich $\vec{v}_j$ auch im Falle $j = 1$ oder $j = n$ als Linearkombination der übrigen $\vec{v}_i$ schreiben. ∎

g) Die Dimension eines Vektorraums

Die Dimension eines Vektorraums soll natürlich so definiert werden, daß $\mathbb{R}^n$ die Dimension n hat; wir müssen die Zahl n also irgendwie als Eigenschaft von (Mengen von) Vektoren aus $\mathbb{R}^n$ rekonstruieren.

Offensichtlich kann jeder Vektor aus $\mathbb{R}^n$ als Linearkombination der n Einheitsvektoren geschrieben werden:

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = a_1 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + a_2 \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} + \cdots + a_n \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} .$$

Es fällt aber schwer sich eine Menge aus weniger als n Vektoren vorzustellen, aus der sich ebenfalls *jeder* Vektor aus $\mathbb{R}^n$ als Linearkombination darstellen läßt.

Diese Eigenschaft machen wir uns zunutze, um allgemein Dimensionen zu definieren:

Definition: *a)* Eine Teilmenge $M \subseteq V$ eines k-Vektorraums V heißt *Erzeugendensystem,* wenn $[M] = V$ ist.
b) Wir sagen, der k-Vektorraum V sei *endlichdimensional,* wenn er ein endliches Erzeugendensystem hat; ansonsten bezeichnen wir V als *unendlichdimensional.*

c) Wir sagen, der endlichdimensionale k-Vektorraum V habe die Dimension n, in Zeichen $n = \dim_k V$ oder kurz $n = \dim V$, wenn er ein n-elementiges Erzeugendensystem enthält, aber kein Erzeugendensystem mit weniger als n Elementen.
d) Dem Nullvektorraum $\{\vec{0}\}$ ordnen wir (formal) die Dimension Null zu.

Als Beispiel eines unendlichdimensionalen Vektorraums haben wir den Vektorraum aller reeller Polynome. Hätte dieser nämlich ein endliches Erzeugendensystem, bestehend etwa aus den Polynomen f_1 bis f_n, so ließe sich sich jedes Polynom als Linearkombination

$$f = \lambda_1 f_1 + \cdots + \lambda_n f_n$$

schreiben. Auf diese Weise aber erhält man nur Polynome, deren Grad nicht größer ist als der größte Grad eines f_i. Damit sind auch alle Vektorräume $\mathcal{C}^k\big((a, b), \mathbb{R}\big)$ unendlichdimensional, denn sie enthalten insbesondere alle Polynome.

Endlichdimensional sind natürlich die reellen Vektorräume $\mathbb{R}^n$, denn $\mathbb{R}^n$ wird von seinen n Einheitsvektoren erzeugt. Da wir aber noch nicht sicher wissen, daß es kein Erzeugendensystem mit *weniger* als n Vektoren gibt, können wir im Augenblick nur sagen, daß die Dimension von $\mathbb{R}^n$ *höchstens* n ist.

Für $\mathbb{R}^2$ sieht man leicht, daß sie genau zwei ist: Ansonsten gäbe es nämlich ein Erzeugendensystem aus nur einem Vektor, d.h. alle Vektoren aus $\mathbb{R}^2$ wären proportional zueinander, was natürlich nicht der Fall ist. Für beliebiges n müssen wir ähnlich argumentieren mit linearer Abhängigkeit anstelle von Proportionalität; die Methoden dazu entwickelt der nächste Abschnitt.

h) Basen

Im $\mathbb{R}^3$ läßt sich jeder Vektor

$$\vec{v} = \begin{pmatrix} a \\ b \\ c \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + c \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

auf genau eine Weise als Linearkombination der drei Einheitsvektoren

$$\vec{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad \vec{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \quad \text{und} \quad \vec{e}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

schreiben; dies entspricht der Tatsache, daß wir im $\mathbb{R}^3$ drei Koordinaten haben.

Mit dem Begriff der *Basis* soll dieser Sachverhalt (soweit möglich) auf beliebige Vektorräume verallgemeinert werden. Da bei der Beschreibung eines Punkts durch seine Koordinaten deren Reihenfolge wesentlich ist, werden wir Basen meist nicht einfach als Mengen auffassen, sondern als geordnete Systeme, im endlichen Fall also als Tupel:

Definition: Ein System $\mathcal{B}$ von Vektoren $\vec{b}_1, \vec{b}_2, \ldots$ eines k-Vektorraums V heißt *Basis* von V, wenn gilt:
1.) Die Menge der $\vec{b}_i$ erzeugt den Vektorraum V, *und*
2.) $\mathcal{B}$ ist linear unabhängig.

Wenn es nicht auf die Reihenfolge ankommt, bezeichnen wir gelegentlich auch die Menge der Basisvektoren als Basis; in diesem Sinne ist also eine Basis einfach ein linear unabhängiges Erzeugendensystem.

Es ist klar, daß die Einheitsvektoren $\vec{e}_1, \vec{e}_2, \vec{e}_3$ eine Basis des $\mathbb{R}^3$ bilden. Ihre wesentliche Eigenschaft der eindeutigen Darstellbarkeit eines jeden Vektors als Linearkombination teilt sie mit jeder anderen Basis:

Lemma: Ist $\mathcal{B}$ eine Basis eines Vektorraums V, so läßt sich jeder Vektor $\vec{v} \in V$ auf genau eine Weise als Linearkombination

$$\vec{v} = \lambda_1 \vec{b}_1 + \cdots + \lambda_r \vec{b}_r$$

von Basisvektoren $\vec{b}_i$ aus $\mathcal{B}$ darstellen.

Beweis: Nach der ersten Eigenschaft aus der Definition einer Basis müssen die Basisvektoren V erzeugen, also läßt sich jeder Vektor $\vec{v} \in V$ als Linearkombination von endlich vielen Elementen aus $\mathcal{B}$ darstellen. Auch wenn wir von zwei solchen Darstellungen ausgehen, ist die Menge

der daran beteiligten Vektoren aus $\mathcal{B}$ noch endlich; wir können also annehmen, daß es r Vektoren $\vec{b}_1, \ldots, \vec{b}_r$ gibt, so daß

$$\begin{aligned}\vec{v} &= \lambda_1\vec{b}_1 + \cdots + \lambda_r\vec{b}_r \\ &= \mu_1\vec{b}_1 + \cdots + \mu_r\vec{b}_r\end{aligned}$$

ist, wobei wir einfach λ_i oder μ_i gleich Null setzen, wenn $\vec{b}_i$ in der entsprechenden Darstellung nicht vorkommt. Subtrahieren wir die beiden Darstellungen voneinander, erhalten wir eine Darstellung des Nullvektors als Linearkombination

$$\vec{0} = (\lambda_1 - \mu_1)\vec{b}_1 + \cdots + (\lambda_r - \mu_r)\vec{b}_r$$

von Basisvektoren. Da diese nach der zweiten definierenden Eigenschaft einer Basis linear unabhängig sind, müssen alle Koeffizienten $\lambda_i - \mu_i$ verschwinden. Damit sind die beiden betrachteten Darstellungen von $\vec{v}$ als Linearkombination der Vektoren aus $\mathcal{B}$ gleich, mit anderen Worten: Es gibt genau eine solche Darstellung. ■

Lemma: Ein Erzeugendensystem eines k-Vektorraum V ist genau dann eine Basis, wenn es minimal ist.

Beweis: Das Erzeugendensystem $\mathcal{B}$ sei eine Basis. Um zu zeigen, daß es minimal ist, müssen wir uns überlegen, daß jeder Basisvektor $\vec{v}$ aus $\mathcal{B}$ wirklich notwendig ist, daß also $\mathcal{B}$ ohne diesen Vektor $\vec{v}$ kein Erzeugendensystem mehr ist.

Falls es eines wäre, könnte insbesondere der Vektor $\vec{v}$ als Linearkombination der restlichen Vektoren aus $\mathcal{B}$ geschrieben werden. Gleichzeitig hat er aber die Darstellung $\vec{v} = \vec{v}$, deren rechte Seite man auch als Linearkombination von Elementen aus $\mathcal{B}$ auffassen kann. Somit ist seine Basisdarstellung nicht eindeutig, im Widerspruch zum gerade bewiesenen Lemma. Daher muß $\mathcal{B}$ minimal sein.

Umgekehrt sei $\mathcal{B}$ ein minimales Erzeugendensystem. Um zu zeigen, daß es eine Basis ist, reicht der Nachweis der linearen Unabhängigkeit von $\mathcal{B}$.

Sei also $\lambda_1\vec{b}_1 + \cdots + \lambda_n\vec{b}_n = \vec{0}$ eine Darstellung des Nullvektors als Linearkombination von Elementen aus $\mathcal{B}$. Falls darin einer der Koeffizienten λ_i nicht verschwindet, läßt sich der zugehörige Vektor $\vec{v}_i$ als Linearkombination der restlichen $\vec{v}_j$ schreiben. Dann reicht aber bereits $\mathcal{B}$ ohne $\vec{v}_i$ zur Erzeugung aus, $\mathcal{B}$ ist also nicht minimal. Somit müssen alle λ_i verschwinden, $\mathcal{B}$ ist also linear unabhängig und damit eine Basis. ■

Lemma: Eine System von linear unabhängigen Elementen eines Vektorraums ist genau dann eine Basis, wenn es maximal ist.

Beweis: $\mathcal{B}$ sei eine Basis. Dann läßt sich jeder Vektor $\vec{v} \in V$ als Linearkombination der Elemente von $\mathcal{B}$ schreiben, nimmt man also $\vec{v}$ zu $\mathcal{B}$ hinzu, ist das System nicht mehr linear unabhängig.

Umgekehrt sei $\mathcal{B}$ maximal linear unabhängig, und $\vec{v}$ sei ein beliebiger Vektor; wir müssen zeigen, daß er als Linearkombination der Vektoren aus $\mathcal{B}$ darstellbar ist. Das ist trivial, falls $\vec{v}$ bereits zu $\mathcal{B}$ gehört.

Andernfalls ist $\mathcal{B}$ zusammen mit $\vec{v}$ linear abhängig, da $\mathcal{B}$ ja als *maximal* linear unabhängig vorausgesetzt war. Somit gibt es ein nichttriviale Linearkombination

$$\lambda\vec{v} + \lambda_1\vec{b}_1 + \cdot + \lambda_n\vec{b}_n = \vec{0}$$

mit Vektoren $\vec{b}_i \in \mathcal{B}$. Darin muß $\lambda \neq 0$ sein, denn sonst wäre $\mathcal{B}$ linear abhängig. Also liegt

$$\vec{v} = -\frac{\lambda_1}{\lambda}\vec{b}_1 + \cdots + -\frac{\lambda_n}{\lambda}\vec{b}_n$$

in $[\mathcal{B}]$, und $\mathcal{B}$ ist ein Erzeugendensystem. ■

Basen lassen sich somit auch charakterisieren als minimale Erzeugendensysteme oder als maximale Systeme linear unabhängiger Vektoren.

Als nächstes stellt sich die Frage, wann es Basen gibt. Glücklicherweise hat *jeder* Vektorraum eine Basis; der Beweis ist allerdings für unendlichdimensionale Vektorräume logisch nicht ganz einfach. Für diese Vorlesung wollen wir uns daher mit einem Beweis für endlichdimensionale

Vektorräume begnügen. Wir beweisen dazu den etwas allgemeineren, tatsächlich ebenfalls für beliebige Vektorräume gültigen

Basisergänzungssatz: $M \subset V$ sei eine linear unabhängige Teilmenge des endlichdimensionalen Vektorraums V. Dann gibt es eine Basis $\mathcal{B}$ von V, die M enthält.

Beweis: Da V nach Voraussetzung endlichdimensional ist, gibt es zunächst einmal überhaupt eine endliche Menge $E \subset V$, die V erzeugt. Falls E einen oder mehrere der Vektoren aus M enthält, entfernen wir diese; was übrigbleibt, sei die Menge N, d.h. $N = E \setminus M$.

Damit sind M und N zwei disjunkte Teilmengen von V, deren Vereinigung die Menge E enthält und somit insbesondere ein Erzeugendensystem von V ist.

Konkret sei $M = \{\vec{b}_1, \ldots, \vec{b}_r\}$ und $N = \{\vec{v}_1, \ldots, \vec{v}_s\}$; dann wird V also erzeugt von

$$M \cup N = \{\vec{b}_1, \ldots, \vec{b}_r, \vec{v}_1, \ldots, \vec{v}_s\}\,.$$

Wir beweisen die Behauptung durch Induktion nach der Elementanzahl s von N.

Für $s = 0$ bilden die Elemente von M, in irgendeiner Weise angeordnet, bereits eine Basis, und wir sind fertig.

Für $s > 0$ sind wir fertig, falls $M \cup N$ linear unabhängig ist; denn dann ist $M \cup N$ eine Basis von V, die M enthält.

Andernfalls gibt es Elemente $\lambda_1, \ldots, \lambda_r$ und $\mu_1, \ldots, \mu_s$, die nicht alle gleichzeitig verschwinden, so daß

$$\lambda_1\vec{b}_1 + \cdots + \lambda_r\vec{b}_r + \mu_1\vec{v}_1 + \cdots + \mu_s\vec{v}_s = \vec{0}$$

ist. In dieser Gleichung können nicht alle μ_i verschwinden, denn sonst wären die $\vec{b}_i$ linear abhängig, im Widerspruch zur Voraussetzung. Also gibt es (mindestens) ein $\mu_i \neq 0$, und der zugehörige Vektor $\vec{v}_i$ läßt sich als Linearkombination der restlichen $\vec{v}_j$ und der $\vec{b}_\ell$ ausdrücken.

Damit wird $V = [M \cup (N \setminus \{\vec{v}_i\})]$ auch von der um $\vec{v}_i$ verminderten Menge erzeugt, und wir haben nur noch $s - 1$ Vektoren $\vec{v}_j$. Daher gibt es nach Induktionsannahme eine Basis von V, die M enthält. ■

Korollar: Jeder endlichdimensionale Vektorraum $V \neq \{\vec{0}\}$ hat eine Basis.

Beweis: Man wende den obigen Satz an auf eine Menge M, die aus einem einzigen Vektor $\vec{v} \neq \vec{0}$ besteht. ■

Um die Sonderrolle des Nullvektorraums zu eliminieren, vereinbaren wir, daß er die leere Menge als Basis haben soll; dies ist kompatibel mit der üblichen Interpretation von leeren Summen und leeren Aussagen.

Wie bereits erwähnt, gelten sowohl der Basisergänzungssatz als auch das obige Korollar für beliebige Vektorräume, d.h. also auch im Falle unendlicher Dimension. Für interessierte Leser sei kurz erwähnt, wie man hier vorgeht. Das wesentliche neue Hilfsmittel ist das ZORNsche Lemma, benannt nach dem deutschen Mathematiker MAX ZORN (1906–1993), der es, nachdem er Deutschland wegen der nationalsozialistischen Politik verlassen mußte, um 1935 an der amerikanischen Yale Universität bewies. Es besagt folgendes:

Gegeben sei eine nichtleere partiell geordnete Menge $\mathcal{M}$, d.h. für manche Paare von Elementen $A, B \in \mathcal{M}$ ist eine Relation $A < B$ erklärt mit der Eigenschaft, daß mit $A < B$ und $B < C$ auch $A < C$ gilt, wohingegen nie $A < A$ ist. Diese partiell geordnete Menge habe die zusätzliche Eigenschaft, daß es zu jeder Kette

$$A_1 < A_2 < A_3 < \cdots$$

von Elementen aus $\mathcal{M}$ ein Element A_∞ gebe mit der Eigenschaft, daß $A_i < A_\infty$ für alle i. Dann gibt es in $\mathcal{M}$ ein *maximales* Element, d.h. ein Element B, zu dem es kein $C \in \mathcal{M}$ gibt mit $B < C$.

Dieses Lemma kann nicht aus den üblichen Axiomen der Mengenlehre hergeleitet werden, sondern ist äquivalent zum sogenannten *Auswahlaxiom.* Für dieses bewies um 1940 der österreichische Mathematiker KURT GÖDEL (1906–1978), seit 1940 im amerikanischen Exil in Princeton, daß sowohl dieses Axiom als auch seine Negation mit den restlichen Axiomen der Mengenlehre kompatibel ist; das gleiche gilt demnach auch für das ZORNsche Lemma. Man kann daher wählen, ob man eine Mathematik mit oder ohne ZORNsches Lemma bevorzugt. Die meisten Mathematiker haben sich für „mit“ entschieden, es gibt aber auch welche, die das ZORNsche Lemma ablehnen.

Aus dem ZORNschen Lemma folgt der Basisergänzungssatz recht einfach: Als Menge $\mathcal{M}$ nehmen wir die Menge aller linear unabhängiger Teilmengen $A \subset V$, die M enthalten; die partielle Ordnungsrelation sei die gewöhnliche (echte) Teilmengenbeziehung. Die Kettenbedingung des ZORNschen Lemmas ist offensichtlich erfüllt, denn für eine Kette

$$M \subset A_1 \subset A_2 \subset A_3 \subset \cdots$$

aus linear unabhängigen Mengen A_i, die M enthalten, ist auch

$$A_\infty = \bigcup_{i \geq 1} A_i$$

eine linear unabhängige Teilmenge von V, die M enthält, da jede endliche Menge von Vektoren aus A_∞ bereits in einer der Mengen A_m liegt. Also gibt es nach dem ZORNschen Lemma ein maximales Element $\mathcal{B} \in \mathcal{M}$. Diese Menge $\mathcal{B}$ ist linear unabhängig, da sie in $\mathcal{M}$ liegt, und sie ist eine Basis, denn gäbe es einen Vektor $\vec{v} \notin [\mathcal{B}]$, so wäre auch die Menge $\mathcal{C} = \mathcal{B} \cup \{\vec{v}\}$ linear unabhängig, im Widerspruch zur Maximalität von $\mathcal{B}$. Damit ist der Basisergänzungssatz bewiesen, und das Korollar folgt wie oben.

Um wenigstens anhand eines Beispiels zu sehen, daß auch unendlichdimensionale Vektorräume Basen haben, betrachten wir den Vektorraum V aller Polynome mit reellen Koeffizienten. Da sich ein Polynom P vom Grad d als

$$P = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$$

schreiben läßt, erzeugt das System $\mathcal{B}$ der x-Potenzen $1, x, x^2, x^3, \ldots$ diesen Vektorraum. Jede Linearkombination des Nullvektors, des Polynoms $P \equiv 0$ also, aus Elementen von $\mathcal{B}$ wäre ein Polynom

$$\lambda_0 + \lambda_1 x + \cdots + \lambda_n x^n \,,$$

dessen Koeffizienten zumindest teilweise von Null verschieden sind, während es selbst identisch Null wäre. Da es kein solches Polynom gibt, ist $\mathcal{B}$ linear unabhängig, also eine Basis von V.

Die Schwierigkeiten, die bei unendlichdimensionalen Vektorräumen auftreten können, sieht man, wenn man in diesem Beispiel die Polynome durch Potenzreihen (egal ob formal oder konvergent) ersetzt: Da Potenzreihen *unendliche* Summen sind, während bei Linearkombinationen nur *endliche* Summen erlaubt sind, bilden nun die x-Potenzen kein Erzeugendensystem mehr. Nach dem Basisergänzungssatz, der, auch wenn wir das nicht bewiesen haben, auch für unendlichdimensionale Vektorräume gilt, gibt es eine Menge von Potenzreihen, die zusammen mit der obigen Menge $\mathcal{B}$ eine Basis bilden; explizit angeben konnte diese Menge aber noch niemand, genauso wenig wie eine explizite Basis für einen der Räume $\mathcal{C}^n(\mathbb{R}, \mathbb{R})$.

Kehren wir also zurück zum überschaubareren endlichdimensionalen Fall, und beweisen wir dort zunächst die anschaulich fast selbstverständliche Aussage, daß jede Basis eines n-dimensionalen Vektorraums aus n Vektoren besteht. Dazu benötigen wir eine leichte Verschärfung

des Basisergänzungssatzes; er geht zurück auf ERNST STEINITZ, den wir bereits von der Körperdefinition aus §1*b)* kennen:

Austauschsatz von STEINITZ: M sei eine endliche linear unabhängige Teilmenge des endlichdimensionalen Vektorraums V, und $\mathcal{B}$ sei eine Basis von V. Dann gibt es eine Teilmenge $\mathcal{B}'$ von $\mathcal{B}$, so daß $M \cup \mathcal{B}'$ eine Basis von V ist. Diese hat genauso viele Elemente wie $\mathcal{B}$.

Mit anderen Worten: Man kann Vektoren aus $\mathcal{B}$ finden, die sich Stück für Stück gegen die Vektoren aus M *austauschen* lassen.

Der *Beweis* ist dem des Basisergänzungssatzes sehr ähnlich; mit Rücksicht auf die Anzahlaussage führen wir ihn aber durch Induktion nach der Elementanzahl m von M.

Für $m = 0$ ist $M = \emptyset$ und wir setzen einfach $\mathcal{B}' = \mathcal{B}$.

Für $m \geq 1$ entfernen wir einen Vektor $\vec{v}$ aus M und wenden den Satz auf die Menge $M' = M \smallsetminus \{\vec{v}\}$ an. Für diese gilt er nach Induktionsannahme, es gibt also eine Teilmenge $\mathcal{C}'$ von $\mathcal{B}$, so daß $\mathcal{C} = M' \cup \mathcal{C}'$ eine Basis von V ist mit gleicher Elementanzahl wie $\mathcal{B}$. Bezüglich dieser Basis habe $\vec{v}$ die Darstellung

$$\vec{v} = \lambda_1 \vec{v}_1 + \cdots + \lambda_{m-1} \vec{v}_{m-1} + \mu_1 \vec{c}_1 + \cdots + \mu_r \vec{c}_r \,,$$

wobei $M' = \{\vec{v}_1, \ldots, \vec{v}_{m-1}\}$ und $\mathcal{C}' = \{\vec{c}_1, \ldots, \vec{c}_r\}$ sein soll.

Da $M = M' \cup \{\vec{v}\}$ linear unabhängig ist, muß in dieser Darstellung mindestens ein $\vec{\mu}_i$ von Null verschieden sein. Daher läßt sich der zugehörige Vektor $\vec{c}_i$ als Linearkombination aus den restlichen $\vec{c}_j$, den $\vec{v}_\ell$ und dem Vektor $\vec{v}$ schreiben, d.h. auch die durch den *Austausch* von $\vec{c}_i$ durch $\vec{v}$ entstehende Menge

$$M' \cup \left(\mathcal{C}' \smallsetminus \{\vec{c}_i\}\right) \cup \{\vec{v}\} = M \cup \left(\mathcal{C}' \smallsetminus \{\vec{c}_i\}\right)$$

erzeugt ganz V. Diese Menge ist auch linear unabhängig und somit eine Basis, denn ist

$$\alpha \vec{v} + \sum_{\ell=1}^{m-1} \alpha_\ell \vec{v}_\ell + \sum_{\substack{j=1 \\ j \neq i}}^{n} \beta_j \vec{c}_j = \vec{0} \,,$$

so muß zunächst α verschwinden, da $\vec{v}$ sonst als Linearkombination der $\vec{v} \in M'$ und der $\vec{c}_j$ mit $j \neq i$ dargestellt werden könnte, was wir oben durch die Wahl eines i mit $\mu_i \neq 0$ ausgeschlossen haben. Also steht hier nur eine Linearkombination von Elementen einer Basis, so daß alle α_ℓ und β_j verschwinden müssen. Mit

$$\mathcal{B}' = \left(\mathcal{C}' \setminus \{\vec{c}_i\}\right)$$

ist somit die Behauptung des Satzes erfüllt. ∎

Aus dem STEINITZschen Austauschsatz folgt

Satz: *a)* Jede Basis $\mathcal{B}$ eines n-dimensionalen Vektorraums V besteht aus n Vektoren.
b) Jede Teilmenge von V mit mehr als n Elementen ist linear abhängig.
c) Keine Teilmenge von V mit weniger als n Elementen ist ein Erzeugendensystem.

Beweis: a) Da V die Dimension n hat, gibt es ein Erzeugendensystem $M = \{\vec{v}_1, \ldots, \vec{v}_n\}$ mit n-Elementen, aber keines mit weniger Elementen. Also ist M ein minimales Erzeugendensystem und somit eine Basis.

Nun sei $\mathcal{B} = \{\vec{b}_1, \ldots, \vec{b}_m\}$ irgendeine andere Basis von V. Nach dem Austauschsatz läßt sich M zu einer Basis von V ergänzen, die genauso viele Elemente hat wie $\mathcal{B}$. Da es keine Basis geben kann, die M echt enthält, muß M genauso viele Elemente enthalten wie $\mathcal{B}$, also n.

b) Jede linear unabhängige Teilmenge läßt sich zu einer Basis ergänzen, und jede Basis besteht aus n Vektoren. Also kann eine linear unabhängige Menge höchstens n Vektoren enthalten.

c) Das ist die Definition der Dimension. ∎

Nach diesem Satz läßt sich die Dimension eines Vektorraums einfach dadurch bestimmen, daß man eine Basis findet und deren Elemente zählt. Insbesondere hat $\mathbb{R}^n$ als $\mathbb{R}$-Vektorraum die Dimension n, da die n Einheitsvektoren eine Basis bilden.

Weniger offensichtlich ist, daß $\mathbb{R}$ als $\mathbb{Q}$-Vektorraum unendlichdimensional ist: Dazu betrachten wir die unendliche Menge M aller Logarithmen

$\ln p$ der Primzahlen. Wäre diese Menge linear abhängig, gäbe es eine nichttriviale Linearkombination

$$\lambda_1 \ln p_1 + \cdots + \lambda_r \ln p_r = 0$$

mit $\lambda_i \in \mathbb{Q}$. Multipliziert man diese Gleichung mit dem Hauptnenner der λ_i, so erhält man eine entsprechende Gleichung mit Koeffizienten $\mu_i \in \mathbb{Z}$. Dann ist

$$\mu_1 \ln p_1 + \cdots + \mu_r \ln p_r = \ln(p_1^{\mu_1} \cdot \cdots \cdot p_r^{\mu_r}) = 0$$

gleichbedeutend mit

$$p_1^{\mu_1} \cdot \cdots \cdot p_r^{\mu_r} = 1\,,$$

was wegen der Eindeutigkeit der Primzerlegung in $\mathbb{Z}$ nur gelten kann, wenn alle μ_i und damit auch alle λ_i verschwinden.

Also ist $\mathbb{R}$ als $\mathbb{Q}$-Vektorraum unendlichdimensional, und dies erklärt, warum Computer so große Schwierigkeiten mit reellen Zahlen haben: Exakt rechnen kann ein Computer nur in Teilmengen von $\mathbb{R}$, die endlichdimensionale $\mathbb{Q}$-Vektorräume sind – und selbst da gibt es zumindest theoretisch noch das Problem der potentiell beliebig großen Zähler und Nenner.

i) Dimensionen und lineare Abbildungen

Als nächstes wollen wir uns mit Dimensionen von Untervektorräumen, insbesondere auch Kernen und Bildern beschäftigen. Anschaulich klar und auch recht einfach zu beweisen ist der folgende

Satz: Für einen echten Untervektorraum $U < V$ eines endlichdimensionalen Vektorraums V ist $\dim U < \dim V$.

Beweis: Eine Basis von U ist auch in V linear unabhängig, läßt sich also ergänzen zu einer Basis von V. Da die Dimension eines Vektorraums gleich der Elementanzahl einer beliebigen Basis ist, folgt sofort, daß $\dim U \leq \dim V$ sein muß, und wenn beide gleich sind, ist $U = V$. ∎

Hier haben wir ganz wesentlich benutzt, daß V endlichdimensional ist; in einen unendlichdimensionalen Vektorraum gibt es stets Untervektorräume, die ebenfalls unendlichdimensinal sind, im Vektorraum V

aller reeller Polynome in x beispielsweise den Untervektorraum aller Polynome in x^2.

Satz: Für endlichdimensionale Vektorräume V, W und eine lineare Abbildung $\varphi\colon V \to W$ ist $\dim \operatorname{Bild} \varphi = \dim V - \dim \operatorname{Kern} \varphi$.

Beweis: $\vec{b}_1, \ldots, \vec{b}_r$ sei eine Basis von $\operatorname{Kern} \varphi$; falls φ injektiv ist, setzen wir $r = 0$. Nach dem Basisergänzungssatz oder (falls $r = 0$) wegen der Existenz von Basen lassen sich dann $n - r$ Vektoren $\vec{b}_{r+1}, \ldots, \vec{b}_n$ finden mit $n = \dim V$, so daß $\vec{b}_1, \ldots, \vec{b}_n$ eine Basis von V ist.

Das Bild eines beliebigen Vektors $\vec{v} = \lambda_1 \vec{b}_1 + \cdots + \lambda_n \vec{b}_n$ ist dann

$$\varphi(\vec{v}) = \lambda_1 \varphi(\vec{b}_1) + \cdots + \lambda_n \varphi(\vec{b}_n) = \lambda_{r+1} \varphi(\vec{b}_{r+1}) + \cdots + \lambda_n \varphi(\vec{b}_n) ,$$

da $\vec{b}_1 \ldots, \vec{b}_r$ ja auf den Nullvektor abgebildet werden. Also wird $\operatorname{Bild} \varphi$ von den Vektoren $\varphi(\vec{b}_{r+1}), \ldots, \varphi(\vec{b}_n)$ erzeugt.

Diese Vektoren sind auch linear unabhängig in W, denn ist

$$\lambda_{r+1} \varphi(\vec{b}_{r+1}) + \cdots + \lambda_n \varphi(\vec{b}_n) = \varphi(\lambda_{r+1} \vec{b}_{r+1} + \cdots + \lambda_n \vec{b}_n) = \vec{0} ,$$

so liegt $\lambda_{r+1} \vec{b}_{r+1} + \cdots + \lambda_n \vec{b}_n$ im Kern von φ.

Im Fall einer injektiven Abbildung ist $\lambda_{r+1} \vec{b}_{r+1} + \cdots + \lambda_n \vec{b}_n$ daher gleich dem Nullvektor, und damit müssen alle $\lambda_i = 0$ sein, denn die $\vec{b}_i$ sind als Basisvektoren insbesondere linear unabhängig.

Falls φ nicht injektiv ist, können wir nur sagen, daß der Vektor $\lambda_{r+1} \vec{b}_{r+1} + \cdots + \lambda_n \vec{b}_n$ im Kern von φ liegt; er ist also darstellbar als Linearkombination der Basisvektoren $\vec{b}_1, \ldots, \vec{b}_r$ des Kerns:

$$\lambda_{r+1} \vec{b}_{r+1} + \cdots + \lambda_n \vec{b}_n = \lambda_1 \vec{b}_1 + \cdots + \lambda_r \vec{b}_r .$$

Auch daraus folgt wegen der linearen Unabhängigkeit der $\vec{b}_i$, daß alle λ_i Null sein müssen.

Damit ist $\{\varphi(\vec{b}_{r+1}), \ldots, \varphi(\vec{b}_n)\}$ eine Basis von $\operatorname{Bild} \varphi$, d.h.

$$\dim \operatorname{Bild} \varphi = n - r = \dim V - \dim \operatorname{Kern} \varphi ,$$

wie behauptet. ∎

Wir werden diese Aussage im folgenden als *Dimensionsformel* bezeichnen. Da wir hier mit Dimensionen rechnen, ist klar, daß sie nicht auf unendlichdimensionale Vektorräume verallgemeinert werden kann: Sind etwa sowohl V als auch $\operatorname{Kern} \varphi$ unendlichdimensional, kann $\operatorname{Bild} \varphi$ jede beliebige Dimension haben – einschließlich null und unendlich. Der sogenannte *Homomorphiesatz* macht eine genauere Aussage über $\operatorname{Bild} \varphi$, die auch für unendlichdimensionale Vektorräume gilt. Da wir die zu seiner Formulierung benötigten Begriffe nur teilweise kennen und für diese Vorlesung auch nicht brauchen, sei auf Einzelheiten verzichtet.

Korollar: Eine lineare Selbstabbildung $\varphi\colon V \to V$ eines endlichdimensionalen Vektorraums V ist genau dann injektiv, wenn sie surjektiv ist.

Beweis: φ ist genau dann injektiv, wenn $\dim \operatorname{Kern} \varphi = 0$ ist und genau dann surjektiv, wenn $\dim \operatorname{Bild} \varphi = \dim V$ ist. Diese beiden Dimensionsaussagen sind nach dem gerade bewiesenen Satz äquivalent. ∎

Man beachte, daß es in diesem Korollar sehr wesentlich ist, daß wir von einem *endlichdimensionalen* Vektorraum ausgehen: Für den Vektorraum V aller reeller Polynome ist die Abbildung

$$\varphi\colon V \to V; \quad \sum_{i=0}^{d} a_i x^i \mapsto \sum_{i=0}^{d} a_i x^{2i}$$

linear *(warum?)* und injektiv, aber nicht surjektiv. Umgekehrt ist die Ableitung

$$\psi\colon V \to V; \quad f \mapsto f'$$

linear und surjektiv, aber nicht injektiv.

§3: Vektorräume und endliche Körper

Bislang hatten wir in fast allen Beispielen nur Vektorräume über dem Körper der reellen Zahlen betrachtet; in der Informationsverarbeitung treten aber oftmals auch Probleme auf, für die Vektorräume über endlichen Körpern nützlich sind. Als einfachstes Beispiel kennen wir bereits aus §1*e)* den Körper $\mathbb{F}_2 = \{0, 1\}$ der Bits; erstes Thema dieses Paragraphen sind Vektorräume über $\mathbb{F}_2$.