

Wolfgang K. Seiler

Höhere Mathematik I

Vorlesung an der Universität Mannheim
im Sommersemester 2004

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 Entstehungsweise 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.

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: Bei Modellierung durch kontinuierliche Größen wird man typischerweise mit analytischen Methoden arbeiten, oft mit Differentialgleichungen; bei Modellierung 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

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 Werkzeugen betrachtet und Abhandlungen über das Drehmoment liest, und niemand, der einfach mathematische Sätze und deren Beweise auswendig lernt, wird damit erfolgreich Probleme der Informatik lösen.

Zum einen beginnen Probleme der Informatik nie mit „ $f: \mathbb{R}^3 \rightarrow \mathbb{R}$ 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 reellen Zahlen modellieren, da die Mathematik der reellen Zahlen erheblich

zweiten Semesters möglich ist – die notwendige Erfahrung dazu vermitteln sollen. Hauptziel der Vorlesung ist also, daß Sie praktische Fähigkeiten 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 auszuwählen, 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 gesehen habe; im Buchhandel sind möglicherweise 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, ⁶2001

[MV2] K. MEYBERG, P. VACHENAUER: *Höhere Mathematik II, Differentialgleichungen, Funktionentheorie, Fourier-Analyse, Variationsrechnung*, Springer, ⁴2001

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.

[DJ] 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 Internettechnologien, 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 ¹⁰2001, Band 2 ¹⁰2001, Band 3 ⁴2001, Anwendungsorientierte Übungsaufgaben aus Naturwissenschaft und Technik ⁴2000, Mathematische Formelsammlung für Ingenieure und Naturwissenschaftler, ⁷2001

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, ⁶2003, 2. Lineare Algebra, ⁴2002, 3. Gewöhnliche Differentialgleichungen, Distributionen, Integraltransformationen, ⁴2002, 4. Vektoranalysis und Funktionentheorie, ²1994, 5. Funktionalanalysis und Partielle Differentialgleichungen, ²1993

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 ⁹1995

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 ²2000

[W2] T. WESTERMANN: *Mathematik für Ingenieure mit MAPLE II*, Springer ²2001

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 Computeralgebrasytem 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 Computeralgebrasytem 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.

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

[BGZ] I.N. BRONSTEIN, G. GROSCHKE, 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*, Binomi⁴2001,

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.

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 Beispielen 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 $1, 2, 3, \dots$. 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

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

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 HIPPOSOS (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 2000 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 „ \cdot “, 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

$$z = \Re z + i \Im z.$$

(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

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

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

I.1) Das Assoziativgesetz der Addition

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

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

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

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

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

II.1) Das Assoziativgesetz der Multiplikation

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

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

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

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

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

III.) Das Distributivgesetz

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

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} fassen: 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 $\bar{z} = x - iy$ die zu z konjugiert komplexe Zahl.

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

Offensichtlich ist $\overline{\bar{z} + \bar{w}} = z + w$, und auch das entsprechende Resultat für die Multiplikation $\overline{z\bar{w}} = \bar{z} \cdot \bar{w}$ 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

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

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

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

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

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

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

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 *GAUSSSCHE Zahlenebene*. Sie war zwar nicht zusammen mit GAUSS auf dem Zehnmarschein 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 Anwendungen 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 „ \cdot “ das logische Und, während „ $+$ “ das *exklusive* logische Oder ist. (Für Algorithologen ist dies das lateinische *aut* im Gegensatz zum *vel*; wer sich eher für Logik oder Schaltalgebra interessiert, 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.