

---

# Lehrbuch der Algebra

---

Gerd Fischer

# Lehrbuch der Algebra

Mit lebendigen Beispielen, ausführlichen  
Erläuterungen und zahlreichen Bildern

4., wesentlich überarbeitete und erweiterte Auflage

Unter Mitarbeit von Matthias Lehner, Florian Quiring  
und Reinhard Sacher



**Springer** Spektrum

Gerd Fischer  
Zentrum Mathematik  
Technische Universität München  
Garching, Deutschland

ISBN 978-3-658-19365-2 (Hardcopy)  
ISBN 978-3-658-19217-4 (Softcopy)  
<https://doi.org/10.1007/978-3-658-19218-1>

ISBN 978-3-658-19218-1 (eBook)

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

Springer Spektrum

© Springer Fachmedien Wiesbaden GmbH 2008, 2011, 2013, 2017

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

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften. Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Planung: Ulrike Schmickler-Hirzebruch

Abbildungen: Avril Bader, Matthias Lehner und Brigitte Singhof

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Spektrum ist Teil von Springer Nature

Die eingetragene Gesellschaft ist Springer Fachmedien Wiesbaden GmbH

Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Dem Andenken  
an meinen Lehrer  
REINHOLD REMMERT  
gewidmet

## Vorwort zur vierten Auflage

Für die neue Auflage wurde der gesamte Text gründlich überarbeitet. Vor allem habe ich mannigfache Anregungen von Studierenden berücksichtigt, die sich weitergehende Motivationen, mehr Details in Begründungen, sowie zusätzliche Beispiele und Abbildungen gewünscht haben. Darüber hinaus ist die Klassifikation der endlichen abelschen Gruppen mit Hilfe der Elementarteiler im Rahmen der Theorie zyklischer Gruppen völlig neu gestaltet worden. Auch das verbesserte Layout soll dabei helfen, die Lektüre zu vereinfachen und Neulinge im Land der Algebra leichter mit den zahlreichen Begriffen, Methoden und grundlegenden Ergebnissen vertraut zu machen. Ich hoffe sehr, dass sie dabei auch die Präzision, Klarheit und Schönheit dieses Gebäudes der Mathematik schätzen lernen.

Mein Dank gilt all denen, die mich bei der Überarbeitung mit Rat und Tat unterstützt haben, vor allem ANDREAS ALPERS, AVRIL BADER, GEORG OBERMEIER, GREGOR KEMPER, REINHOLD REMMERT, WILHELM SINGHOF sowie MATTHIAS LEHNER, der die Arbeit während der ganzen Zeit konstruktiv kritisch und stets hilfreich begleitet hat. Weiter danke ich KRISTINA REISS und der TUM School of Education für die personelle Unterstützung mit Hilfe der Telekom-Stiftung und ULRIKE SCHMICKLER-HIRZEBRUCH vom Springer Verlag für die Erfüllung all meiner Wünsche zur neuen Gestaltung des Buches.

Wie immer bin ich allen Leserinnen und Lesern für Hinweise dankbar: [gfisher@ma.tum.de](mailto:gfisher@ma.tum.de)

München und Garching, im Juli 2017

Gerd Fischer

## Vorwort zur ersten Auflage

Der vorliegende Text ist ein einführendes „*Lese- und Lernbuch*“ für Studierende, die sich nach dem Studium der Linearen Algebra erstmals mit grundlegenden Problemen, Methoden und Ergebnissen der „höheren“ Algebra vertraut machen möchten. Der Titel steht beim Vieweg-Verlag in einer alten Tradition: ab 1896 erschien das dreibändige Werk *Lehrbuch der Algebra* von H. WEBER, 1924 folgten zwei Bände mit dem gleichen Titel von R. FRICKE, aber mit einer

ganz anderen Intention. In den beiden klassischen Werken wurde versucht, möglichst umfassend den damaligen Stand der Algebra zu vermitteln.

Die Darstellung der Algebra hat sich seit WEBER und FRICKE stark verändert. Durch das Programm von HILBERT ist das axiomatische Gerüst ausgeprägt worden; die grundlegenden Vorlesungen in diesem Stil von EMIL ARTIN und EMMY NOETHER waren die Quellen für die 1930 erstmals veröffentlichte *Moderne Algebra* von VAN DER WAERDEN, sie haben alle seither erschienenen Bücher über Algebra geprägt. Durch die Axiomatik wird die Darstellung klarer, Beweise werden einfacher und durchsichtiger. Aber für Studierende besteht die Gefahr, die zahllosen hinter dem klaren Gerüst verborgenen konkreten Situationen nicht genügend kennen zu lernen. Dazu sei erinnert an die Arbeiten von C.F. GAUSS: Hier gab es keinen der abstrakten Begriffe wie Gruppe, Ring oder Körper; es wurden viele raffinierte Überlegungen und Berechnungen durchgeführt, deren Ergebnisse später elegante Formulierungen im abstrakten Rahmen gefunden haben.

In diesem Buch kann und soll die Zeit nicht zurückgedreht werden. Aber es wird versucht, durch sehr viele konkrete *Beispiele* die Bodenhaftung der Studierenden zu erhalten. In dieser Absicht beschreiben wir ausführlich die Symmetrien der *Platonischen Körper* als Illustration der Beziehungen zwischen Gruppen und Geometrie, *quadratische Zahlringe* zur Erläuterung der subtilen Teilbarkeitseigenschaften in Ringen und von GAUSS gefundene Formeln zur *Darstellung von Einheitswurzeln* aus der Sicht der Körpererweiterungen. In einer einführenden Vorlesung verbleibt kaum Zeit zur Behandlung all dieser Themen; die Studierenden erhalten die Möglichkeit, solche zur Vertiefung des Verständnisses wichtige Ergänzungen hier nachzulesen. Außerdem enthält dieser Text für ein Buch über Algebra ungewöhnlich viele Bilder. Dazu sei erinnert, dass die Algebra ein hervorragendes Werkzeug für die Geometrie ist, und dass vor der Entwicklung einer guten Symbolik für die „Buchstabenrechnung“ viele algebraische Beweise geometrisch geführt wurden.

Die zahlreichen Veränderungen der letzten Jahre in den Studiengängen haben sich mittlerweile etwas stabilisiert; dieses Buch versucht, darauf Rücksicht zu nehmen. Der gesamte Inhalt ist für eine zweisemestrige einführende Vorlesung ausgelegt, die nur Kenntnisse aus der Linearen Algebra voraussetzt und ab dem dritten Studiensemester besucht werden kann. In vielen Studiengängen ist nur eine einsemestrige Einführung in die Algebra vorgesehen. Daher sind einige Paragraphen und Abschnitte mit einem *Stern\** versehen: man kann sie beim ersten Durchgang weglassen, und eventuell im zweiten Semester nachholen. Insbesondere ist dadurch ein Minimalkanon für den *Bachelor* vorgeschlagen. Ganz besonders Studierende für das *Lehramt* können durch geeignete Auswahl aus dem Inhalt eine solide und nicht zu abstrakte Grundlage für die spätere Tätigkeit erhalten und das Buch dann als Nachschlagewerk nutzen.

In dieser Einführung soll nur die relativ „klassische“ Algebra behandelt werden, Höhepunkte sind die Ergebnisse über die Lösbarkeit von Polynomgleichungen; dieser Teil der Algebra kam im 19. Jahrhundert - abgesehen von der Darstellung - zu einem Abschluss. Einen sehr guten Eindruck von dem langen Weg dorthin seit den Wurzeln in der Antike vermittelt der *historische Text* von VAN DER WAERDEN [W<sub>2</sub>]. Die anschließende Entwicklung der Algebra im 20. Jahrhundert war rasant, vor allem in Richtung der algebraischen Geometrie und der Zahlentheorie; zwischen beiden wurden innige Zusammenhänge entdeckt, ein Höhepunkt war die Lösung des Problems von FERMAT im Jahr 1993. All das muss fortgeschrittenen Vorlesungen und weiter-

führenden Büchern vorbehalten bleiben; einen knappen historischen Abriss über das vergangene Jahrhundert findet man bei [Mi]. Wie überall in der Mathematik setzt das Studium der neueren Entwicklungen eine solide Kenntnis der klassischen Methoden voraus.

Die *Gliederung des Inhalts* folgt der üblichen Systematik „Gruppen, Ringe, Körper“, dadurch wird das logische Gerüst deutlich und die Darstellung vereinfacht. Zur Erhöhung der Motivation beim Lernen kann man getrost davon abweichen: Man kann ganz hinten anfangen mit den *geometrischen Konstruktionen* und die zunehmend komplexeren algebraischen Hilfsmittel nach Bedarf nachlesen. Wenn man mit dem Paragraphen über die *Lösungen von Polynomgleichungen* anfängt, wird man feststellen, dass die wesentlichen zuvor entwickelten Techniken über Gruppen, Ringe und Körper benötigt werden. In den zahlreichen Beispielen sind nicht immer alle Einzelheiten ausgeführt; da verbleiben viele kleinere und größere *Übungsaufgaben*.

An der Darstellung der grundlegenden Ergebnisse der Algebra ist von vielen Autoren gefeilt worden. Es gibt zahllose Tricks, deren Urheber kaum noch festzustellen sind; man kann sie schon als „Folklore“ bezeichnen. Im *Literaturverzeichnis* sind Bücher aufgeführt, aus denen ich gelernt habe, außerdem zahlreiche Texte für weiterführende Lektüre. Aus den Werken von C.F. GAUSS sind einige Stellen im Faksimile abgedruckt, in der Hoffnung, die Neugier des Lesers auf diese einmaligen Texte zu wecken.

Mein Dank gilt den Studierenden der TU-München für viele kritische Bemerkungen, und vor allem REINHARD SACHER, dem Coautor unseres gemeinsamen Buches „Einführung in die Algebra“ [F-S]; aus diesem alten Text ist vieles übernommen worden. Sowie FLORIAN QUIRING, der vier Semester lang Übungen zur Vorlesung betreut und viele wertvolle Details beigesteuert hat. BRIGITTE SINGHOF hat mit großer Präzision und persönlichem Einsatz die druckfertige  $\text{\TeX}$ -Vorlage erstellt, Ulrike Schmickler-Hirzebruch hat das Projekt vom Verlag begleitet und vorangetrieben.

Trotz sorgfältiger Suche nach Druckfehlern und mathematischen Irrtümern werden wohl einige verblieben sein. Daher möchte ich alle Leser bitten, mir Fundstellen mitzuteilen, am einfachsten an

`gfischer@ma.tum.de`

Wir haben unter

<http://www-m10.ma.tum.de/~GerdFischer>

eine Seite mit Kommentaren und Verbesserungen eingerichtet.

München, im November 2007

Gerd Fischer

*Es ist der Fluch aller abstrakten Theorien,  
dass sie sehr weit entwickelt werden müssen,  
bis sie nützliche Ergebnisse bei konkreten Problemen liefern.*

**HERMANN WEYL**

# Inhaltsverzeichnis

<b>Leitfaden</b>	<b>1</b>
<b>1 Gruppen</b>	<b>5</b>
1.1 Halbgruppen, Gruppen und Untergruppen	5
1.1.1 Innere Verknüpfungen und Halbgruppen	5
1.1.2 Beispiele	6
1.1.3 Definition einer Gruppe	8
1.1.4 Abschwächung der Gruppenaxiome	9
1.1.5 Translationen und Kürzungsregeln	10
1.1.6 Definition einer Untergruppe	11
1.1.7 Erzeugung von Untergruppen	12
1.1.8 Untergruppen von $\mathbb{Z}$ , Kongruenzen und Restklassen	13
1.1.9 Beispiele	18
1.2 Homomorphismen und Normalteiler	28
1.2.1 Definition eines Homomorphismus	28
1.2.2 Beispiele	30
1.2.3 Nebenklassen	36
1.2.4 Ordnung und Index	38
1.2.5 Beispiele	40
1.2.6 Definition eines Normalteilers	44
1.2.7 Homomorphismen und Normalteiler	45
1.2.8 Faktorgruppen	46
1.2.9 Beispiele	47
1.3 Isomorphiesätze, Produkte von Gruppen und zyklische Gruppen	50
1.3.1 Isomorphiesätze	50
1.3.2 Äußeres direktes Produkt	53
1.3.3 Inneres direktes Produkt	54
1.3.4 Äußeres semidirektes Produkt*	58
1.3.5 Inneres semidirektes Produkt*	60
1.3.6 Beispiele*	62
1.3.7 Zyklische Gruppen	69
1.3.8 Teilbarkeit ganzer Zahlen	71
1.3.9 Der Chinesische Restsatz	75



1.3.10	Der euklidische Algorithmus . . . . .	77
1.3.11	Produkte zyklischer Gruppen . . . . .	81
1.3.12	Untergruppen zyklischer Gruppen . . . . .	83
1.3.13	Zerlegung einer zyklischen Gruppe . . . . .	84
1.3.14	Primrestklassengruppen . . . . .	85
1.3.15	Automorphismen zyklischer Gruppen* . . . . .	90
1.3.16	Beispiele . . . . .	91
1.3.17	Unendlich zyklische und frei-abelsche Gruppen* . . . . .	97
1.4	Operationen von Gruppen auf Mengen . . . . .	102
1.4.1	Definition einer Operation . . . . .	102
1.4.2	Beispiele . . . . .	103
1.4.3	Bahnraum und Standgruppe . . . . .	104
1.4.4	Die Klassengleichung* . . . . .	106
1.4.5	Zyklenzerlegung einer Permutation . . . . .	108
1.4.6	Beispiele . . . . .	110
1.5	Symmetriegruppen* . . . . .	115
1.5.1	Regelmäßige $n$ -Ecke und die Diedergruppe . . . . .	115
1.5.2	Endliche Untergruppen von $O(2)$ . . . . .	117
1.5.3	Symmetrien des Tetraeders . . . . .	119
1.5.4	Symmetrien von Würfel und Oktaeder . . . . .	120
1.5.5	Symmetrien von Ikosaeder und Dodekaeder . . . . .	123
1.5.6	Die Klassengleichung der Ikosaedergruppe . . . . .	126
1.5.7	Endliche Untergruppen von $SO(3)$ . . . . .	128
1.5.8	Symmetrien von Fußbällen . . . . .	128
1.6	Struktursätze . . . . .	130
1.6.1	Elemente zu vorgegebener Ordnung . . . . .	130
1.6.2	Struktursatz für endliche abelsche Gruppen . . . . .	132
1.6.3	Endliche abelsche $p$ -Gruppen* . . . . .	137
1.6.4	Klassifikation der endlichen abelschen Gruppen* . . . . .	138
1.6.5	Endlich erzeugte abelsche Gruppen* . . . . .	142
1.6.6	Spaltung in Torsion und freien Anteil * . . . . .	144
1.6.7	Endliche $p$ -Gruppen* . . . . .	147
1.6.8	Die Sätze von SYLOW* . . . . .	149
1.6.9	Beispiele* . . . . .	154
1.7	Einfache und auflösbare Gruppen* . . . . .	162
1.7.1	Einfache Gruppen . . . . .	162
1.7.2	Kommutatorgruppen . . . . .	164
1.7.3	Beispiele . . . . .	165
1.7.4	Auflösbare Gruppen . . . . .	166
1.7.5	Auflösbarkeit von $p$ -Gruppen . . . . .	169
<b>2</b>	<b>Ringe</b> . . . . .	<b>171</b>
2.1	Grundbegriffe . . . . .	171
2.1.1	Definition eines Rings . . . . .	171
2.1.2	Einheiten, Körper, Unterringe . . . . .	173

2.1.3	Ringhomomorphismen . . . . .	175
2.1.4	Beispiele . . . . .	176
2.1.5	Polynomringe . . . . .	183
2.1.6	Grad eines Polynoms . . . . .	186
2.1.7	Division mit Rest . . . . .	188
2.1.8	Nullstellen und Werte von Polynomen . . . . .	190
2.1.9	Einheitswurzeln in $\mathbb{C}$ . . . . .	192
2.1.10	Polynome in mehreren Veränderlichen* . . . . .	194
2.1.11	Endliche Untergruppen der multiplikativen Gruppe eines Körpers . . . . .	198
2.1.12	Einbettung einer Halbgruppe in eine Gruppe . . . . .	200
2.1.13	Quotientenkörper . . . . .	202
2.1.14	Beispiele . . . . .	204
2.2	Ideale und Restklassenringe . . . . .	206
2.2.1	Definition von Idealen . . . . .	206
2.2.2	Ideale und Einheiten . . . . .	207
2.2.3	Restklassenringe . . . . .	208
2.2.4	Isomorphiesätze . . . . .	209
2.2.5	Beispiele . . . . .	210
2.2.6	Hauptidealringe und noethersche Ringe . . . . .	213
2.2.7	Euklidische Ringe . . . . .	215
2.2.8	Beispiele . . . . .	216
2.2.9	Der Hilbertsche Basissatz* . . . . .	220
2.2.10	Operationen mit Idealen* . . . . .	222
2.2.11	Der Chinesische Restsatz* . . . . .	223
2.2.12	Beispiele* . . . . .	225
2.2.13	Primideale und maximale Ideale . . . . .	227
2.2.14	Beispiele . . . . .	229
2.2.15	Existenz maximaler Ideale und das Lemma von ZORN* . . . . .	231
2.3	Teilbarkeit in Integritätsringen . . . . .	235
2.3.1	Teiler und assoziierte Elemente . . . . .	235
2.3.2	Irreduzible Elemente und Primelemente . . . . .	236
2.3.3	Teilerketten . . . . .	240
2.3.4	Primzahlen . . . . .	242
2.3.5	Faktorielle Ringe . . . . .	245
2.3.6	Gemeinsame Teiler und Vielfache . . . . .	247
2.3.7	Polynomringe über faktoriellen Ringen . . . . .	249
2.3.8	Irreduzibilitätskriterien für Polynome . . . . .	255
2.3.9	Beispiele . . . . .	259
2.3.10	Ringe holomorpher Funktionen* . . . . .	264
2.4	Quadratische Zahlkörper und Zahlringe* . . . . .	266
2.4.1	Quadratische Zahlkörper . . . . .	266
2.4.2	Quadratische Zahlringe . . . . .	269
2.4.3	Einheiten in quadratischen Zahlringen . . . . .	271
2.4.4	Euklidische quadratische Zahlringe . . . . .	276

2.4.5	Faktorzerlegung in quadratischen Zahlringen . . . . .	280
2.4.6	Ideale als ideale Zahlen . . . . .	287
<b>3</b>	<b>Körpererweiterungen</b>	<b>291</b>
3.1	Grundbegriffe . . . . .	291
3.1.1	Charakteristik und Primkörper . . . . .	292
3.1.2	Grad einer Körpererweiterung . . . . .	293
3.1.3	Adjunktion von Elementen . . . . .	295
3.1.4	Algebraische und transzendente Elemente . . . . .	297
3.1.5	Das Minimalpolynom . . . . .	299
3.1.6	Beispiele . . . . .	301
3.1.7	Algebraische Körpererweiterungen . . . . .	306
3.1.8	Algebraisch abgeschlossene Körper . . . . .	309
3.2	Konstruktion von Körpererweiterungen . . . . .	313
3.2.1	Symbolische Adjunktion von Nullstellen . . . . .	313
3.2.2	Existenz und Fortsetzung von Körperisomorphismen . . . . .	315
3.2.3	Zerfällungskörper eines Polynoms . . . . .	320
3.2.4	Beispiele . . . . .	324
3.2.5	Der algebraische Abschluss* . . . . .	328
3.3	Einfache und mehrfache Nullstellen . . . . .	332
3.3.1	Vielfachheit von Nullstellen und formale Ableitung . . . . .	332
3.3.2	Separabilität . . . . .	335
3.3.3	Der Frobenius-Homomorphismus . . . . .	337
3.3.4	Endliche Körper . . . . .	339
3.3.5	Beispiele . . . . .	342
3.3.6	Algebraischer Abschluss eines endlichen Körpers . . . . .	345
3.3.7	Der Satz vom primitiven Element . . . . .	346
3.3.8	Beispiele . . . . .	347
3.3.9	Resultanten* . . . . .	349
3.3.10	Diskriminanten* . . . . .	353
3.3.11	Beispiele* . . . . .	355
3.4	Galois-Theorie . . . . .	359
3.4.1	Symmetrische Polynome . . . . .	359
3.4.2	Die Galoisgruppe . . . . .	364
3.4.3	Fixkörper . . . . .	370
3.4.4	Galois-Erweiterungen . . . . .	373
3.4.5	Der Hauptsatz der Galois-Theorie . . . . .	376
3.4.6	Beispiele . . . . .	379
3.4.7	Der Fundamentalsatz der Algebra* . . . . .	383
3.4.8	Diskriminante und Galois-Gruppe* . . . . .	387
3.4.9	Galois-Theorie endlicher Körper* . . . . .	389
3.5	Lösung von Polynomgleichungen* . . . . .	391
3.5.1	Quadratische Gleichungen . . . . .	391
3.5.2	Kubische Gleichungen . . . . .	391
3.5.3	Beispiele . . . . .	395

3.5.4	Gleichungen vierten Grades . . . . .	397
3.5.5	Beispiele . . . . .	401
3.5.6	Kreisteilung in Charakteristik Null . . . . .	404
3.5.7	Kreisteilung in Charakteristik $p > 0$ . . . . .	411
3.5.8	Reine Polynome . . . . .	414
3.5.9	Zyklische Erweiterungen . . . . .	417
3.5.10	Lösbarkeit von Polynomgleichungen . . . . .	419
3.5.11	Die allgemeine Polynomgleichung . . . . .	423
3.5.12	Gleichungen fünften Grades und das Ikosaeder . . . . .	424
3.5.13	Darstellung von Einheitswurzeln . . . . .	427
3.5.14	Beispiele . . . . .	429
3.5.15	Das Umkehrproblem der Galois-Theorie . . . . .	434
3.6	Geometrische Konstruktionen . . . . .	437
3.6.1	Konstruktionen mit Zirkel und Lineal . . . . .	438
3.6.2	Der Körper der konstruierbaren Punkte . . . . .	439
3.6.3	Struktur des Körpers der konstruierbaren Punkte . . . . .	441
3.6.4	Unlösbarkeit klassischer Konstruktionsaufgaben . . . . .	444
3.6.5	Konstruktion von regelmäßigen $n$ -Ecken* . . . . .	446
3.6.6	Andere Regeln für Konstruktionsverfahren* . . . . .	451
<b>Anhang 1</b>	<b>Platonische Körper</b>	<b>453</b>
<b>Anhang 2</b>	<b>Begriffe und Axiome</b>	<b>459</b>
	<b>Literaturverzeichnis</b>	<b>481</b>
	<b>Index</b>	<b>487</b>
	<b>Symbolverzeichnis</b>	<b>493</b>

# Leitfaden

Die Algebra hat eine sehr lange Geschichte. Der Name ist von AL-HWARIZMI abgeleitet, der um 800 n. Chr. beim Kalifen von Bagdad tätig war, aber die Wurzeln der Algebra – das Rechnen mit Zahlen – reichen bis tief in die Frühzeit zurück. Bevor wir hier mit dem heute üblichen Standardprogramm **Gruppen-Ringe-Körper** beginnen, soll anhand von einigen Jahrhundert-Problemen ein Vorgeschmack auf die Entwicklung algebraischer Methoden gegeben werden.

## 1. Geometrische Konstruktionen mit Zirkel und Lineal

### Die Quadratur des Kreises

Dieses uralte Problem der Geometrie konnte erst 1882 gelöst werden, nachdem LINDEMANN bewiesen hatte, dass die Kreiszahl  $\pi$  *transzendent ist*. Das bedeutet, dass es keine Relation der Form

$$\pi^n + a_{n-1}\pi^{n-1} + \dots + a_1\pi + a_0 = 0$$

mit  $n \geq 1$  und rationalen  $a_0, \dots, a_{n-1}$  gibt (vgl. dazu 3.1.4 und 3.6.4).

### Die Konstruktion regelmäßiger $n$ -Ecke

Für  $n = 3, 4, 5, 6$  sind die Konstruktionen seit ewigen Zeiten bekannt; für  $n = 7$  war die Frage bis 1796 offen gewesen. Da zeigte GAUSS (im Alter von 19 Jahren), dass eine solche Konstruktion unmöglich ist. In seinem 1801 veröffentlichten *Disquisitiones arithmeticae* gab er ein Kriterium mit Hilfe der EULERSchen  $\phi$ -Funktion (vgl. 1.3.14) an: *Das  $n$ -Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn  $\phi(n)$  eine Potenz von 2 ist* (vgl. dazu 3.6.5).

## 2. Lösungen von Polynomgleichungen

Für ein Polynom  $f = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0 = 0$  mit Koeffizienten  $a_0, \dots, a_{n-1} \in \mathbb{C}$  gilt der

**Fundamentalsatz der Algebra**     *Es gibt  $x_1, \dots, x_n \in \mathbb{C}$  derart, dass*

$$f = (X - x_1) \cdot \dots \cdot (X - x_n).$$

Ein strenger Beweis wurde von GAUSS in seiner Dissertation 1799 gegeben (vgl. 3.1.8 und 3.4.7). Der Fundamentalsatz liefert aber keine Methode zur Berechnung der Nullstellen  $x_i$  aus den Koeffizienten  $a_j$ . In der Praxis benutzt man dafür seit langer Zeit numerische Methoden zur

approximativen Berechnung, aber klassisch war man auf der Suche nach Formeln mit geschaltelten Wurzeln, denn Wurzeln waren numerisch relativ einfach zu berechnen. Für  $n = 2$  ist

$$f = X^2 + pX + q \quad \text{und} \quad x_{1,2} = \frac{1}{2} \left( -p \pm \sqrt{p^2 - 4q} \right).$$

Formeln dieser Art waren schon seit langer Zeit bekannt, erst 1525 und 1545 gelang es CARDANO und FERRARI [C] für  $n = 3$  und 4 ähnliche, aber kompliziertere Formeln zu finden (vgl. 3.5.2 und 3.5.4). Alle Versuche das Problem für  $n \geq 5$  zu lösen blieben erfolglos, bis ABEL [A] und GALOIS [G] in den Jahren 1826 und 1830 die ersten Beweise dafür fanden, dass es für  $n \geq 5$  keine allgemein gültige Lösung geben kann.

### 3. Das FERMAT-Problem

Gesucht sind ganzzahlige Lösungen  $x, y, z$  einer Gleichung

$$x^n + y^n = z^n.$$

Für  $n = 2$  gibt es unendlich viele *pythagoreische Tripel*  $(x, y, z)$ : Für jede Primzahl  $p \geq 3$  und  $p^2 = 2k + 1$  ist  $(p, k, k + 1)$  ein solches Tripel. Um 1670 glaubte FERMAT einen Beweis dafür zu haben, dass es für  $n \geq 3$  keine Lösung gibt. Nach unzähligen Versuchen gelang es schließlich A. WILES im Jahr 1994 ein sehr komplizierter Beweis.

### 4. Das GOLDBACH-Problem

Im Jahr 1742 äußerte GOLDBACH in einem Brief an EULER die folgenden Vermutungen:

**Starke Form:** *Jede gerade Zahl  $n \geq 6$  ist Summe von zwei ungeraden Primzahlen.*

**Schwache Form:** *Jede ungerade Zahl  $n \geq 9$  ist Summe von drei ungeraden Primzahlen.*

Man kann sich leicht überlegen, dass die schwache Form aus der starken Form folgt. Weiter findet man durch einfache Rechnung für kleine  $n$ , dass es im allgemeinen mehrere solche Summandendarstellungen gibt. Erst im Jahr 2013 gelang es HELFGOTT die letzten Lücken im Beweis der schwachen Form zu schließen; die starke Form ist weiter offen.

### 5. Beweismethoden

Wie die Beispiele zeigen, hat es Jahrhunderte gedauert, bis relativ einfach zu formulierende Probleme gelöst werden konnten. Im folgenden soll versucht werden, das zu erklären.

Die GOLDBACH-Vermutung ist in unserer Liste insofern eine Ausnahme, als hier bewiesen werden soll, dass etwas geht. Die Tücke dabei ist, dass es bislang keine Methode gibt, für beliebig große  $n$  Summandendarstellungen berechnen zu können. Als Ersatz werden für die schwache Form höchst komplizierte Hilfsmittel aus der Analysis, insbesondere der Verteilung von Primzahlen benutzt.

Bei den anderen Problemen muss gezeigt werden, dass etwas unmöglich ist. Dazu ist es nötig, irgendein nicht zu umgehendes Hindernis zu finden. Das liegt in den drei anderen Beispielen in

einem passenden mehr oder weniger abstrakten theoretischen Rahmen. Besonders ausgeprägt ist das beim FERMAT-Problem. Hier benötigt man höchst diffizile im 20. Jahrhundert entwickelte Hilfsmittel der Algebraischen Geometrie, um aus der Annahme der Existenz einer Lösung einen Widerspruch zu produzieren. Das ist nur einem sehr kleinen Kreis von Experten zugänglich.

Einfacher ist die Situation bei den Problemen 1 und 2, hier kann der nötige theoretische Rahmen in einer Einführung zur Algebra aufgebaut werden. Wir erläutern das im Sinn einer Vorschau am Problem 2, der Lösung von Polynomgleichungen. Im einfachsten Fall sind die Koeffizienten  $a_j$  von  $f$  rationale Zahlen, die Nullstellen  $x_i$  komplexe Zahlen. Zwischen den Körpern  $\mathbb{Q}$  und  $\mathbb{C}$  wird nun ein weiterer Körper  $K$  eingeschoben:

$$\mathbb{Q} \subset K \subset \mathbb{C}.$$

$K$  wird „Zerfällungskörper“ von  $f$  genannt, er ist der kleinste Zwischenkörper, der alle Nullstellen  $x_i$  von  $f$  enthält. Nun wird das Hindernis gegen die Existenz der gesuchten Lösungsformeln in der „Struktur“ von  $K$  gesucht. Genauer gesagt gehört zu  $K$  eine Gruppe  $G$  von Permutationen der Nullstellen  $x_1, \dots, x_n$ , also eine Untergruppe der vollen Permutationsgruppe  $\mathcal{S}_n$ . Das Hindernis kann schließlich in der „Struktur“ von  $G$  lokalisiert werden:

*Es gibt genau dann eine Lösungsformel der gesuchten Art, wenn  $G$  „auflösbar“ ist.*

Die negative Antwort folgt dann aus dem folgenden Ergebnis:

*Für ein „allgemeines“ Polynom ist  $G = \mathcal{S}_n$  und  $\mathcal{S}_n$  ist für  $n \geq 5$  nicht auflösbar.*

Diese Methode wurde von ABEL und GALOIS skizziert, die Details in den Originalarbeiten sind schwer verständlich. Um die Schritte leichter nachvollziehbar zu machen, wurden im Lauf des 19. Jahrhunderts die Begriffe Gruppe und Körper zur Klärung des theoretischen Hintergrunds axiomatisch eingeführt und schließlich konnte E. ARTIN im Jahr 1948 die GALOIS-Theorie in dem legendären Büchlein [ArE] auf 86 Seiten recht elementar darstellen; mehr als hundert Jahre nach GALOIS.

Der Weg zu den Resultaten der GALOIS-Theorie hat drei Etappen:

1. Die Grundlagen der Gruppentheorie, insbesondere die Eigenschaften der symmetrischen Gruppe  $\mathcal{S}_n$ .
2. Die Teilbarkeitseigenschaften im Ring der Polynome, analog zu denen der ganzen Zahlen.
3. Die Struktur von Körpererweiterungen.

Dem entsprechen die drei Kapitel des vorliegenden Buches. Sie sind aber nicht ausschließlich auf die GALOIS-Theorie ausgerichtet, denn diese ist wie das FERMAT-Problem nur eine von mehreren Triebfeldern zur Entwicklung der axiomatisch aufgebauten „modernen“ Algebra gewesen. Ihre Anwendungen gehen weit über die Lösungen der klassischen Probleme hinaus.