

# **Allgemeine Algebra und Anwendungen**

Von Dr. phil. Dietmar W. Dorninger  
a.o. Professor an der Technischen Universität Wien

und Dr. phil. Winfried B. Müller  
a.o. Professor an der Universität für Bildungswissenschaften Klagenfurt

Mit zahlreichen Abbildungen, Beispielen und Übungen



**Springer Fachmedien Wiesbaden GmbH**

Prof. Dr. phil. Dietmar W. Dorninger

Geboren 1945 in Gaspoltshofen, Oberösterreich. Gymnasialzeit in Linz/Donau. Studium der Mathematik und Physik an der Universität Wien, Promotion 1969. Habilitation im Fach Mathematik an der Technischen Universität Wien 1973. Seit 1976 Ao. Universitätsprofessor am Institut für Algebra und Diskrete Mathematik der Technischen Universität Wien, seit 1981 Vorstand dieses Instituts.

Prof. Dr. phil. Winfried B. Müller

Geboren 1944 in der Stadt Salzburg. Studium der Mathematik, Physik und Darstellenden Geometrie an der Universität und der Technischen Universität Wien von 1962 bis 1967. Promotion an der Universität Wien 1967. Professor für Mathematik an der Universität Simón Bolívar in Caracas/Venezuela von 1971 bis 1973. Habilitation für das Fachgebiet Mathematik an der Technischen Universität Wien 1975. Christian Doppler Preis der Salzburger Landesregierung für außergewöhnliche Leistungen auf dem Gebiet der Naturwissenschaften 1976. Seit 1977 Ao. Universitätsprofessor am Institut für Mathematik der Universität für Bildungswissenschaften in Klagenfurt/Österreich. Vorstand dieses Instituts von 1980 bis 1983. Visiting Professor der University of Tasmania/Australien im Frühjahr 1983.

CIP-Kurztitelaufnahme der Deutschen Bibliothek

**Dorninger, Dietmar:**

Allgemeine Algebra und Anwendungen / von  
Dietmar W. Dorninger u. Winfried B. Müller. –  
Stuttgart : Teubner, 1984.

ISBN 978-3-519-02030-1      ISBN 978-3-663-09813-3 (eBook)

DOI 10.1007/978-3-663-09813-3

NE: Müller, Winfried B.:

Das Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, besonders die der Übersetzung, des Nachdrucks, der Bildentnahme, der Funksendung, der Wiedergabe auf photomechanischem oder ähnlichem Wege, der Speicherung und Auswertung in Datenverarbeitungsanlagen, bleiben, auch bei Verwertung von Teilen des Werkes, dem Verlag vorbehalten.

Bei gewerblichen Zwecken dienender Vervielfältigung ist an den Verlag gemäß § 54 UrhG eine Vergütung zu zahlen, deren Höhe mit dem Verlag zu vereinbaren ist.

© Springer Fachmedien Wiesbaden 1984

Originally published by B.G. Teubner, Stuttgart in 1984

Softcover reprint of the hardcover 1st edition 1984

Umschlaggestaltung: W. Koch, Sindelfingen

## VORWORT

Ausgehend von dem Werk des Arabers Mohammed ibn Musa al-Khowarizmi "Hisab aljabr w'almuqabalah" (Hinüberschaffen eines Gliedes einer Gleichung von einer Seite auf die andere) im 8.Jhdt. nach Chr., welches für die Algebra namensgebend war, verstand man bis zum Beginn des 19.Jhds. unter Algebra im wesentlichen die Lehre von der Lösung algebraischer Gleichungen. Eines der Hauptprobleme der Gleichungslehre war, die Frage zu beantworten, wann eine allgemeine Polynomgleichung n-ten Grades mit Hilfe der Grundrechnungsarten, des Potenzierens und Wurzelziehens auflösbar ist. Diese Frage wurde von E. Galois in einer im Jahre 1831 bei der Französischen Akademie der Wissenschaften eingereichten Arbeit endgültig entschieden. Galois verwendete bei seinem Beweis erstmals Hilfsmittel, die als charakteristisch für die moderne Algebra angesehen werden können, nämlich Eigenschaften von Gruppen und Körpern. - Angeregt durch Fragen der Logik folgten bald Untersuchungen anderer algebraischer Strukturen, nämlich von Booleschen Algebren, und mit der Zeit wandelte sich die Bedeutung des Wortes Algebra hin zur Lehre von algebraischen Strukturen, so wie wir sie heute vornehmlich verstehen.

Mit den vielen neu gewonnenen Ergebnissen über algebraische Strukturen gewann die Frage an Bedeutung, was diesen Ergebnissen gemeinsam ist, und so entstand vor etwa 30 Jahren eine neue Teildisziplin der Algebra, die sogenannte Universelle (oder Universale) Algebra. Zugleich mit dem Trend zur abstrakten Algebra hin geriet allerdings teilweise etwas in Vergessenheit, daß viele Probleme der Algebra aus konkreten Fragen der Anwendungen entstanden und für die Anwendungen bedeutsam sind. - In den letzten Jahren hat jedoch das Interesse an Anwendungen der Algebra sowohl innerhalb als auch außerhalb der Mathematik wieder sehr zugenommen.

Mit dem vorliegenden Buch verfolgen wir zweierlei: Erstens, einen Überblick über die wichtigsten algebraischen Strukturen zu geben, wobei der Hervorhebung von Gemeinsamkeiten dieser Strukturen neben deren ausführlicher Besprechung durch die Bezeichnung "Allgemeine Algebra" im Buchtitel Rechnung getragen wird. Zweitens, ein breites Spektrum von Anwendungsmöglichkeiten vorzustellen, wobei der Bogen der Anwendungen von Problemen, die aus dem Alltag vertraut sind, wie z.B. die Schaltung von Verkehrsampeln oder die Ermittlung von Wahlergebnissen, bis hin zur Lösung von Problemen bei der elektronischen Nachrichtenübertragung und zur axiomatischen Quantenmechanik gespannt ist. (Einen Überblick über die besprochenen Anwendungen gibt die Tabelle auf den Seiten 7 und 8).

Die Aufgaben aus den Anwendungen sind so formuliert, daß zu ihrem Verständnis keine speziellen Vorkenntnisse aus den einzelnen Fachdisziplinen erforderlich sind.

Im theoretischen Teil, der unabhängig von den Abschnitten über Anwendungen gelesen werden kann und welcher die Inhalte einer traditionellen Einführungsvorlesung in die Algebra abdeckt, kommen ebenfalls Anwendungsbeispiele vor; dort dienen sie allerdings nur als didaktisches Hilfsmittel und können von Lesern, die in erster Linie an der Theorie interessiert sind, übergangen werden.

Allen, die uns bei der Veröffentlichung dieses Buches, mit dem wir aufzeigen wollen, daß die Algebra nicht nur eine schöne mathematische Theorie ist, sondern in vielen Gebieten Anwendungen findet, unterstützt haben, gilt unser Dank. Die Damen Chr.Mitterfellner, E.Wiesenbauer und H.Reinauer haben mit viel Mühe und Sorgfalt die Reinschrift des Manuskriptes besorgt. Herr Mag.W.Nowak hat die zahlreichen Abbildungen angefertigt. Herrn Doz.Dr.G.Eigenthaler sind wir für einige wertvolle Hinweise verpflichtet. Insbesondere danken wir jedoch Herrn Dr.P.Spuhler vom Teubner-Verlag in Stuttgart für die Übernahme der Herausgabe des Buches und seine verständnisvolle Kooperation.

Wien und Klagenfurt, im Februar 1984

Die Verfasser

## INHALT

<u>I. Operationen und Relationen</u> .....	9
1. n-stellige Operationen .....	10
2. Algebraische Strukturen .....	19
3. Relationen und Graphen .....	28
4. Ein Beispiel aus der Verkehrsplanung .....	35
5. Kongruenzrelationen und Homomorphismen .....	39
6. Halbordnungsrelationen .....	48
7. Ein Beispiel aus der Soziologie .....	57
<u>II. Verbände und Boolesche Algebren</u> .....	64
8. Grundlagen und modulare Verbände .....	64
9. Verbände und Universelle Algebra .....	78
10. Boolesche Algebren und Orthoverbände .....	88
11. Anwendungen in der Quantenmechanik .....	107
12. Aussagenlogik .....	116
13. Schaltalgebra .....	124
<u>III. Halbgruppen</u> .....	132
14. Monoide .....	132
15. Das DNS-Protein Codierungsproblem .....	137
16. Elemente der Automatentheorie .....	140
17. Formale Sprachen und ein Beispiel aus der Biologie .....	150
<u>IV. Gruppen</u> .....	158
18. Elementare Eigenschaften .....	158
19. Faktorgruppen und Direkte Produkte .....	172
20. Erzeugende und Relationen .....	187
21. Permutationsgruppen .....	192
22. Gruppen und Glockenspiele .....	198
23. Ein Beispiel aus der Anthropologie .....	203
24. Kristallographische Gruppen .....	211
25. Zähltheorie und Anwendungen .....	223
26. Elemente der Darstellungstheorie .....	229

<u>V. Ringe und Körper</u> .....	233
27. Grundlagen .....	233
28. Faktorrings und Quotientenringe (Ringe von Quotienten) ...	242
29. Polynome und formale Potenzreihen .....	249
30. Faktorielle Ringe, Hauptidealringe und Euklidische Ringe .....	261
31. Körpererweiterungen und Konstruktionen mit Zirkel und Lineal .....	270
32. Endliche Körper .....	280
33. Lateinische Quadrate und statistische Versuchsplanung ....	286
<u>VI. Algebraische Codierungstheorie und Kryptographie</u> .....	292
34. Algebraische Codierung .....	293
35. Aktuelle Fragen der Chiffrierung .....	308
<u>Literaturhinweise</u> .....	316
<u>Index</u> .....	318

## ANWENDUNGEN UND DAFÜR BENÖTIGTE ALGEBRAISCHE KENNTNISSE

(Die römischen Zahlen beziehen sich auf das Kapitel, die arabischen Zahlen geben den Abschnitt an.)

ANWENDUNG	ALGEBRAISCHE ERFORDERNISSE
<u>1) Naturwissenschaften</u>	
Kreuzung zweier Genotypen (I/2)	Assoziativitätstest (III/14)
Symmetrieeigenschaften von Molekülen (I/2 und IV/24)	Gruppen (I/2 und IV), Permutationsgruppen (IV/21)
Darstellung von physikalischen Meßgrößen (Observablen) (II/11)	} Orthomodulare Verbände (II/10 und II/11) Homomorphismen (I/5 und II/11)
Gleichzeitige Meßbarkeit von Observablen (II/11)	
Quantenlogik (II/11)	
DNS-Protein Codierungsproblem (III/15)	Freie Halbgruppen (III/14), Homomorphismen (I/5)
Stoffwechselfvorgänge im Tricarbonsäurezyklus (III/16)	Halbautomaten (III/16)
Wachstum von Zellsystemen (III/17)	Lindenmeyersysteme (III/17)
Kristallographie (IV/24)	Permutationsgruppen (IV/21)
Anzahlbestimmungen chemischer Verbindungen (IV/25)	Permutationsgruppen (IV/21), Zähltheorie (IV/25)
<u>2) Technik und Informatik</u>	
Phasenfolgen an durch Ampeln geregelten Kreuzungen (I/4)	Graphen (I/3)
Aussagenlogik (II/12)	} Boolesche Algebra (II/10)
Analyse und Entwurf von elektrischen Schaltungen (II/13)	
Automaten (III/16)	Monoide (III/14), Automaten- theorie (III/16)
Formale Sprachen (III/17)	Relationen (I/3), Graphen (I/3), Automatentheorie (III/16)
Widerstandstransformationen (IV/19)	Faktorgruppen (IV/19)
Anzahlbestimmungen bei elektrischen Schaltungen (IV/25)	Zähltheorie (IV/25), Gruppen (IV)
Schieberegister zur Polynommultiplikation (V/29)	Ringe und Körper (V/27), Polynome (V/29)

Störungen im Fernsprechverkehr (V/32)	Endliche Körper (V/32)
Fehlerkorrigierende Codes (VI/34)	} Gruppen (IV/19), Endliche Körper (V/32), Polynome und formale Potenzreihen (V/29)
Elektronische Nachrichtenübermittlung (VI/34)	
Übertragung von Bildern aus dem Weltraum, Entfernungsmessungen mittels Radar (VI/34)	Endliche Körper (V/32), Polynome und formale Potenzreihen (V/29)
Das "Rote Telefon" (VI/35)	Endliche Körper (V/32)
Chiffriersysteme (VI/35)	} Endliche Körper (V/32), Faktorgruppen (IV/19)
Probleme des Datenschutzes (VI/35)	
Kontrolle des Atomsperrvertrages (VI/35)	

### 3) Sozial- und Wirtschaftswissenschaften

Organisationsstruktur eines Betriebes (I/6)	Halbordnungen (I/6)
Präferenzen und Auswahl (I/7)	} Halbordnungsrelationen (I/6)
Abstimmungsverfahren bei Wahlen (I/7)	
Heiratssysteme (IV/23)	Gruppentheorie (IV/20 und IV/21)
Statistische Versuchsplanung (V/33)	Endliche Körper (V/32), Lateinische Quadrate (V/33)

### 4) Angewandte Kunst

Melodien für Glockenspiele (IV/22)	Permutationsgruppen (IV/21)
Klassifikation von Mustern (IV/25)	} Gruppen (IV), Zahltheorie (IV/25)
Anzahlbestimmungen bei geometrischen Gebilden (IV/25)	
Konstruktionen mit Zirkel und Lineal (V/31)	Körpererweiterungen (V/31)