



Algebra

Gruppen

Ringe

Körper

Modultheorie

Elemente der Darstellungstheorie

Abriss der Galoistheorie

*Wissen entsteht nicht durch Anhäufung
von Einzelinformationen, sondern durch
theoretisch angeleitete Integration in
grössere Zusammenhänge.*

T.A. Becker

Vorwort

Der vorliegende Text entspricht dem Skript der Vorlesung *Algebra*, die ich an der ETH für Mathematiker und Physiker mehrmals gehalten habe. Der Text wurde zwischen 1993 (Kapitel I, II, III, VI) und 1995 (Kapitel IV, V) fertiggestellt und in vervielfältigter Form abgegeben; im Jahre 1999 wurde er im Internet verfügbar gemacht. Er erscheint hier erstmals, nur an einigen wenigen Stellen korrigiert und ergänzt, als kleines Buch.

Begriffe und Resultate der abstrakten Algebra spielen in fast allen Gebieten der Mathematik eine grundlegende Rolle. Die Vorlesung, aus der dieser Text entstanden ist, hat zum Ziel, die Studierenden der Mathematik und Physik an der ETH Zürich mit dem zentralen Inhalt der Algebra bekannt zu machen.

Im ersten Teil des Textes werden die grundlegenden Begriffe *Gruppe*, *Ring* und *Körper* eingeführt. Inhalt und Aufbau dieser Kapitel entsprechen im wesentlichen dem Kanon, dem Algebra-Lehrbücher üblicherweise verpflichtet sind. Allerdings sind hier zusätzlich einige Abschnitte aufgenommen, die in anderen Algebra-Texten nicht zu finden sind. Es sind dies das Resultat über die Darstellung von Primzahlen als Summe von zwei Quadraten (II.5), ein Abschnitt über den Satz von Fermat für komplexe Polynomringe (II.6), eine elementare Behandlung des Problems der Konstruktion mit Zirkel und Lineal (III.3) und ein Abschnitt über Codierungstheorie (III.5), in dem u.a. auch die klassischen Newtonschen Identitäten behandelt werden.

Jedes der drei Kapitel zu Gruppen, Ringen und Körpern beginnt mit einer Einleitung, welche ganz kurz die Bedeutung und die historische Entwicklung der Gebiete beschreiben.

Im zweiten Teil des Textes werden drei algebraische Gebiete näher behandelt, nämlich die *Modultheorie*, die *Darstellungstheorie* und die *Galoistheorie*. Es werden damit drei algebraische Themenkreise berührt, die bei jeder weiteren Beschäftigung mit Algebra fundamental sind und die ferner historisch zu Resultaten geführt haben, die für benachbarte Fachgebiete wichtig sind: Die Modultheorie bildet die Grundlage der homologischen Algebra und stellt damit für das Gebiet der algebraischen Topologie den abstrakten, al-

gebraischen Apparat bereit. Die Darstellungstheorie der Gruppen führt nicht nur zu tief-
liegenden mathematischen Resultaten innerhalb der Gruppentheorie, sondern sie spielt
beispielsweise auch in der mathematischen Behandlung der Quantentheorie eine grosse
Rolle. Die Galoistheorie, ursprünglich entstanden, um die Auflösung von polynomialen
Gleichungen durch Radikale zu behandeln, wurde in der historischen Entwicklung bald
auch grundlegend für viele Resultate der algebraischen Zahlentheorie. Der Text folgt dem
Grundsatz, die einzelnen Gebiete nicht völlig voneinander getrennt darzustellen, sondern
immer auch Querbezüge zuzulassen. So enthält der Abschnitt IV.5 als Anwendung der
Modultheorie nicht nur den Hauptsatz für endlich erzeugte abelsche Gruppen sondern
auch einige Resultate zu Normalformen von Matrizen, im Abschnitt V.8 wird in einem
Beispiel gezeigt, wie die Darstellungstheorie in der Quantenmechanik verwendet wird und
im Abschnitt VI.11 wird mit Hilfe der Galoistheorie ein wichtiger Satz der Darstellungs-
theorie endlicher Gruppen bewiesen.

Zürich, im September 2009

Urs Stambach

Inhaltsverzeichnis

Kapitel I. Gruppen	1
I.1 Axiome, Beispiele	2
I.2 Untergruppen	7
I.3 Endliche Permutationsgruppen	9
I.4 Homomorphismen	13
I.5 Nebenklassen	16
I.6 Normalteiler	18
I.7 Isomorphiesätze	22
I.8 Transformationsgruppen	25
I.9 Direkte Produkte	32
Kapitel II. Ringe	35
II.1 Definitionen, Beispiele	36
II.2 Ringhomomorphismen, Ideale	40
II.3 Faktorielle Ringe	45
II.4 Polynomringe	50
II.5 Der Satz von den zwei Quadraten	56
II.6 Der Satz von Mason und der grosse Satz von Fermat für komplexe Polynome	58
Kapitel III. Körper	63
III.1 Körpererweiterungen	64
III.2 Adjunktion von Nullstellen	66
III.3 Konstruktion mit Zirkel und Lineal	70

III.4 Endliche Körper	73
III.5 Codierungstheorie; Newtonsche Identitäten	78
Kapitel IV. Modultheorie	85
IV.1 Definitionen und Beispiele	86
IV.2 Quotientenmodul, direkte Summe	90
IV.3 Linearkombinationen	95
IV.4 Moduln über einem Hauptidealbereich	98
IV.5 Endlich erzeugbare Torsionsmoduln über einem Hauptidealbereich	100
IV.6 Einfache Moduln	105
IV.7 Kompositionsreihen	109
IV.8 Tensorprodukt	111
Kapitel V. Elemente der Darstellungstheorie	117
V.1 $\mathbb{C}[G]$ -Moduln und Darstellungen	118
V.2 Das Lemma von Schur	121
V.3 Die Vollreduzibilität der Darstellungen	122
V.4 Orthogonalitätsrelationen	124
V.5 Gruppencharaktere	128
V.6 Die reguläre Darstellung einer endlichen Gruppe	134
V.7 Beispiele zur Darstellungstheorie endlicher Gruppen	138
V.8 Zur Darstellungstheorie unendlicher Gruppen	145
V.9 Das Kroneckerprodukt von Darstellungen	152
Kapitel VI. Abriss der Galoistheorie	157
VI.1 Endliche Körpererweiterungen, Zerfällungskörper	158

VI.2 Normale Körpererweiterungen	159
VI.3 Die Charakteristik eines Körpers, separable Polynome, separable Körpererweiterungen	160
VI.4 Einheitswurzeln und endliche Körper	163
VI.5 Die Galoisgruppe	164
VI.6 Einige Beispiele von Galoisgruppen	168
VI.7 Der Hauptsatz der Galoistheorie	170
VI.8 Ein Beispiel	174
VI.9 Konstruktion mit Zirkel und Lineal	177
VI.10 Auflösen von Gleichungen durch Radikale	179
VI.11 Galoistheorie und Darstellungstheorie	184
Literatur	189