Vorwort

Vorwort zur zweiten Auflage

In dieser zweiten Auflage habe ich auf Anraten einiger Leser und des Verlages den Titel des Buches von „Elementare Algebra und Zahlentheorie“ in „Einführung in Algebra und Zahlentheorie“ geändert, um Verwechslungen mit Texten für den Bereich „Elementarmathematik vom höheren Standpunkt“ von Lehramtsstudiengängen auszuschließen - im Sinne dieser Terminologie von Studiengängen gehört der Inhalt des Buches trotz seiner Beschränkung auf die elementareren Teile der Algebra und der Zahlentheorie in den Studienbereich „Höhere Mathematik“. Ferner habe ich eine Reihe Druckfehler und sonstige Fehler korrigiert sowie eine Reihe weiterer kleinerer Änderungen vorgenommen; ich danke S. Kühnlein, Karlsruhe, der mich auf die meisten der Fehler aufmerksam gemacht hat.

Schließlich habe ich, ebenfalls auf Anregung einiger Leser, zwei weitere ergänzende Abschnitte hinzugefügt. In Kapitel 12 wird der Hauptsatz der Galoistheorie formuliert und bewiesen sowie zum Beweis des hinreichenden Kriteriums für Konstruierbarkeit mit Zirkel und Lineal des regelmäßigen n-Ecks benutzt. In dem anderen neu hinzugekommenen ergänzenden Abschnitt 10.4 wird die algebraische Theorie der zyklischen fehlerkorrigierenden Codes vorgestellt, ohne aber auf die informationstheoretischen Grundlagen der Codierungstheorie einzugehen.

Wie auch die anderen ergänzenden Abschnitte des Buchs werden beide Abschnitte in der Regel nicht in den Rahmen einer einsemestrigen Vorlesung über Algebra und Zahlentheorie passen und sind zum Verständnis der anderen Teile des Buchs nicht notwendig; sie sollen interessierten LeserInnen zur Abrundung des Stoffes und als erster Einblick in fortgeschrittene Themen und in Anwendungen dienen.

Wie bisher bitte ich LeserInnen, die noch verbliebene Fehler finden, mir diese an `schulzep@math.uni-sb.de` zu melden, damit ich die Korrekturen auf mei-

ner homepage unter `www.math.uni-sb.de/ag/schulze/eazbuch.html` im Internet zugänglich machen kann. Dort sind auch die mir bekannten Fehler der ersten Auflage mit Korrekturen aufgelistet.

Saarbrücken, Mai 2008 *Rainer Schulze-Pillot*

Vorwort zur ersten Auflage

Dieses Buch ist aus dem Versuch entstanden, die Ausbildung der Studierenden in Algebra und Zahlentheorie an der Universität des Saarlandes in Saarbrücken an die durch die Einführung der Bachelor- und Masterabschlüsse und die anstehende Reform des Lehramtsstudiums veränderten Randbedingungen anzupassen.

Da algebraische und diskrete Strukturen ebenso wie einige grundlegende Ergebnisse und Methoden der Zahlentheorie in zunehmendem Umfang auch für Anwender relevant werden, erschien es sinnvoll, eine einsemestrige Vorlesung über Algebra und Zahlentheorie anzubieten, die auf einer Grundvorlesung über lineare Algebra aufbaut und sich unabhängig von der beabsichtigten Schwerpunktbildung für alle Studierenden eignet.
Eine erste Testversion dieser Vorlesung habe ich im Sommersemester 2005 gehalten. Auf dem Skript zu dieser Vorlesung basiert dieses Buch, das sich vor allem an Studierende der Mathematik ab dem dritten oder ggf. auch dem zweiten Semester in Bachelor- oder Lehramts-Studiengängen an Universitäten wendet.
Ebenso wie die Vorlesung kombiniert es Teile des Stoffes, der üblicherweise in einer Vorlesung über elementare Zahlentheorie behandelt wird, mit Teilen des Stoffes einer klassischen Algebra-Vorlesung.
Mit der Beschränkung auf die elementareren Teile des Gebiets und einer relativ ausführlichen Darstellung will das Buch eine breite Leserschaft ansprechen. Ich möchte aber nicht das Versprechen einer „sanften“ Einführung oder eines leicht verdaulichen anschaulichen und abstraktionsfreien „Mathe-light“-Kurses abgeben – wer eine Scheu vor abstrakten Konzepten hat, wird in der Regel ohnehin nicht Mathematik studieren und mit Sicherheit die Algebra meiden.

Das Buch enthält aus der Zahlentheorie einige Grundlagen der Primzahltheorie, den euklidischen Algorithmus, die Theorie der linearen diophantischen Gleichungen sowie des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen, die Theorie der Kongruenzen mit dem chinesischen Restsatz, die Theorie der primen Restklassengruppe und der Potenzreste und das quadratische Reziprozitätsgesetz.
Aus der Algebra behandeln wir die Grundtatsachen über Gruppen und Ringe einschließlich der Operationen von Gruppen auf Mengen und der Behandlung

von Idealen und Restklassenringen, die Theorie der (endlich erzeugten) abelschen Gruppen und ihrer Charaktere sowie die Grundlagen der Körpertheorie unter besonderer Betonung der endlichen Körper.

Während in den Teilen des Stoffes, die aus der elementaren Zahlentheorie stammen, die zu Grunde liegenden abstrakten algebraischen Konzepte betont werden, werden die Teile, die aus der Algebra stammen, eng an die Behandlung (meist zahlentheoretischer) Beispiele angebunden.
Die Behandlung von Anwendungen ergibt sich dabei in natürlicher Weise; wir behandeln etwa das RSA-Verschlüsselungsverfahren, Primzahltests, Zahldarstellungen und modulares Rechnen im Computer sowie die diskrete Fourier-Transformation.

Wichtige Teile der klassischen Algebra-Vorlesung fallen bei dieser Vorgehensweise notwendigerweise unter den Tisch: Die Galoistheorie erscheint nur in ihrer einfachsten Form als Galoistheorie der endlichen Körper, die Theorie als solche und ihre Anwendungen für die Auflösung von Gleichungen durch Radikale bleiben ebenso einer weiterführenden Algebra-Vorlesung vorbehalten wie die Ausarbeitung der Gruppentheorie (Auflösbarkeit, Satz von Jordan-Hölder, freie Gruppen).
Die algebraische Behandlung der Konstruktionen mit Zirkel und Lineal führt nur bis zum notwendigen Kriterium, das immerhin erlaubt, die bekannten Sätze über Nicht-Konstruierbarkeit zu beweisen. Den Begriff des Zerfällungskörpers eines Polynoms und den Beweis seiner Eindeutigkeit behandeln wir in Abschnitt 9.4, haben aber die Theorie der endlichen Körper ohne deren Benutzung aufgebaut, so dass man diesen Abschnitt überspringen kann, wenn man möglichst rasch zu den endlichen Körpern kommen will.

Auf einige für das weitere Verständnis nicht notwendige Themen wird in ergänzenden Bemerkungen oder in Abschnitten eingegangen, die in der Überschrift als Ergänzung gekennzeichnet sind. Bei einer einsemestrigen an dem Buch orientierten Vorlesung wird man auf die Behandlung der meisten dieser Ergänzungen in der Vorlesung verzichten müssen, ihre Lektüre will ich aber interessierten Studierenden, die ein wenig über das Grundwissen hinausgehen wollen, ausdrücklich ans Herz legen.

Die Übungsaufgaben habe ich meiner im Laufe der Jahre entstandenen Sammlung entnommen. Viele von ihnen stammen aus anderen Lehrbüchern, ohne dass ich die ursprünglichen Quellen noch zurück verfolgen kann; die Kollegen, die ihre Aufgaben hier wiederfinden, bitte ich um Verständnis für die fehlende Quellenangabe.

Abschließend möchte ich Christine Wilk-Pitz sowie Michael Bergau, Matthias Horbach und Alexander Rurainski danken, die Teile des Manuskripts als Skript zu der eingangs erwähnten Vorlesung bzw. zu früheren Vorlesungen in LaTeX geschrieben haben. Ferner danke ich Ute Staemmler, Markus

Zacharski und den HörerInnen meiner Vorlesung für etliche Fehlerkorrekturen. LeserInnen, die noch verbliebene Fehler finden, bitte ich, mir diese an `schulzep@math.uni-sb.de` zu melden, damit ich die Korrekturen auf meiner homepage unter `www.math.uni-sb.de/ag/schulze/eazbuch.html` im Internet zugänglich machen kann.

Saarbrücken, November 2006 *Rainer Schulze-Pillot*