

Undergraduate Texts in Mathematics

Editors

S. Axler
F.W. Gehring
K.A. Ribet

Undergraduate Texts in Mathematics

- Abbott:** Understanding Analysis.
- Anglin:** Mathematics: A Concise History and Philosophy.
Readings in Mathematics.
- Anglin/Lambek:** The Heritage of Thales.
Readings in Mathematics.
- Apostol:** Introduction to Analytic Number Theory. Second edition.
- Armstrong:** Basic Topology.
- Armstrong:** Groups and Symmetry.
- Axler:** Linear Algebra Done Right. Second edition.
- Beardon:** Limits: A New Approach to Real Analysis.
- Bak/Newman:** Complex Analysis. Second edition.
- Banchoff/Wermer:** Linear Algebra Through Geometry. Second edition.
- Berberian:** A First Course in Real Analysis.
- Bix:** Conics and Cubics: A Concrete Introduction to Algebraic Curves.
- Brémaud:** An Introduction to Probabilistic Modeling.
- Bressoud:** Factorization and Primality Testing.
- Bressoud:** Second Year Calculus.
Readings in Mathematics.
- Brickman:** Mathematical Introduction to Linear Programming and Game Theory.
- Browder:** Mathematical Analysis: An Introduction.
- Buchmann:** Introduction to Cryptography.
- Buskes/van Rooij:** Topological Spaces: From Distance to Neighborhood.
- Callahan:** The Geometry of Spacetime: An Introduction to Special and General Relativity.
- Carter/van Brunt:** The Lebesgue–Stieltjes Integral: A Practical Introduction.
- Cederberg:** A Course in Modern Geometries. Second edition.
- Chambert-Loir:** A Field Guide to Algebra
- Childs:** A Concrete Introduction to Higher Algebra. Second edition.
- Chung/AitSahlia:** Elementary Probability Theory: With Stochastic Processes and an Introduction to Mathematical Finance. Fourth edition.
- Cox/Little/O’Shea:** Ideals, Varieties, and Algorithms. Second edition.
- Croom:** Basic Concepts of Algebraic Topology.
- Curtis:** Linear Algebra: An Introductory Approach. Fourth edition.
- Daepf/Gorkin:** Reading, Writing, and Proving: A Closer Look at Mathematics.
- Devlin:** The Joy of Sets: Fundamentals of Contemporary Set Theory. Second edition.
- Dixmier:** General Topology.
- Driver:** Why Math?
- Ebbinghaus/Flum/Thomas:** Mathematical Logic. Second edition.
- Edgar:** Measure, Topology, and Fractal Geometry.
- Elaydi:** An Introduction to Difference Equations. Second edition.
- Erdős/Surányi:** Topics in the Theory of Numbers.
- Estep:** Practical Analysis in One Variable.
- Exner:** An Accompaniment to Higher Mathematics.
- Exner:** Inside Calculus.
- Fine/Rosenberger:** The Fundamental Theory of Algebra.
- Fischer:** Intermediate Real Analysis.
- Flanigan/Kazdan:** Calculus Two: Linear and Nonlinear Functions. Second edition.
- Fleming:** Functions of Several Variables. Second edition.
- Foulds:** Combinatorial Optimization for Undergraduates.
- Foulds:** Optimization Techniques: An Introduction.
- Franklin:** Methods of Mathematical Economics.

(continued after index)

Lindsay N. Childs

A Concrete Introduction to Higher Algebra

Second Edition

 Springer

Lindsay N. Childs
Department of Mathematics
SUNY at Albany
Albany, NY 12222
USA

Editorial Board

S. Axler
Mathematics Department
San Francisco State
University
San Francisco, CA 94132
USA

F.W. Gehring
Mathematics Department
East Hall
University of Michigan
Ann Arbor, MI 48109
USA

K.A. Ribet
Mathematics Department
University of California
at Berkeley
Berkeley, CA 94720-3840
USA

Mathematics Subject Classification (2000): 12-01

Library of Congress Cataloging-in-Publication Data
Childs, Lindsay.

A concrete introduction to higher algebra / Lindsay N. Childs. —
2nd ed.

p. cm.

Includes bibliographical references (p. —) and index.

ISBN 978-0-387-98999-0

ISBN 978-1-4419-8702-0 (eBook)

DOI 10.1007/978-1-4419-8702-0

1. Algebra. I. Title.

QA155.C53 1995

512'.7—dc20

95-5934

ISBN 978-0-387-98999-0

Printed on acid-free paper.

With 9 Illustrations

First softcover printing, 2000

©1995,1979 Springer Science+Business Media New York

Originally published by Springer Science+Business Media, Inc. in 1995

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher Springer Science+Business Media, LLC except for brief excerpts in connection with

reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use in this publication of trade names, trademarks, service marks and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

9 8 7 6

springeronline.com

To Rhonda

Introduction

This book is written as an introduction to higher algebra for students with a background of a year of calculus. The first edition of this book emerged from a set of notes written in the 1970s for a sophomore–junior level course at the University at Albany entitled “Classical Algebra.”

The objective of the course, and the book, is to give students enough experience in the algebraic theory of the integers and polynomials to appreciate the basic concepts of abstract algebra. The main theoretical thread is to develop algebraic properties of the ring of integers: unique factorization into primes, congruences and congruence classes, Fermat’s theorem, the Chinese remainder theorem; and then again for the ring of polynomials. Doing so leads to the study of simple field extensions, and, in particular, to an exposition of finite fields. Elementary properties of rings, fields, groups, and homomorphisms of these objects are introduced and used as needed in the development.

Concurrently with the theoretical development, the book presents a broad variety of applications, to cryptography, error-correcting codes, Latin squares, tournaments, techniques of integration, and especially to elementary and computational number theory. A student who asks, “Why am I learning this?,” will find answers usually within a chapter or two.

For a first course in algebra, the book offers a couple of advantages.

- By building the algebra out of numbers and polynomials, the book takes maximal advantage of the student’s prior experience in algebra and arithmetic. New concepts arise in a familiar context.
- The early introduction and extensive use of congruence classes prepares the student well to understand quotient structures in subsequent courses.

In addition, for a first course in algebra, and especially for the only course in algebra a student might take, the subject-matter of the book has other intrinsic advantages: elegance, relevance, and vitality.

Elegance. Einstein once wrote, “Pure mathematics is, in its way, the poetry of logical ideas.” The ideas in this book, I believe, display a beauty which is inherent in all great mathematics. Number theory arose out of the religious environment of the Pythagoreans, and attracted the best efforts of Fermat, Euler, and Gauss, among the greatest mathematicians in history, not because of any external stimulus, but because of its intrinsic attractiveness.

Relevance. The development of computing power and the discovery of the RSA cryptosystem have led to an explosion of research interest in computational number theory. Since the first edition appeared, the study of factoring and primality testing, and related questions in number theory, have entered the mainstream of mathematical research. The most striking advances have appeared in the most prestigious research journals, as well as in the daily newspapers.

Many of the advances in computational number theory are built on the mathematics which is presented in this book.

Thus the book may be used as a first course in higher algebra, as originally intended, but may also serve as an introduction to modern computational number theory, or to applied algebra.

Vitality. Lynn Steen wrote not so long ago that in contrast to most other sciences, a typical mathematics undergraduate is exposed to very little mathematics discovered since 1800, and hence gets no sense that mathematics is a rapidly growing science.

While much of the basic theory in this book dates from the eighteenth century or before, many of the applications date from the last two decades. I found it exciting to discover and present many of these newer applications while writing this book. I hope the reader will gain from the book some sense of the vitality of this branch of contemporary mathematics.

Notes on the Second Edition

The first edition of this book has been in print for 15 years, a gratifyingly long time. However, extensive classroom experience with the first edition, as well as advances in mathematics, has made a new edition desirable. I have been rewriting sections of the book, off and on, over the last 10 years: improving the exposition, adjusting the emphasis, adding (and subtracting) applications, changing the exercises. The result is that nearly every chapter has been rewritten—it is almost a new book.

The new edition retains the overall organization of the original. The first part, now Chapters 1–13, presents elementary number theory, the second

part, now Chapters 14–22, studies polynomials, and the third part, now Chapters 23–30, offers applications of the primitive element theorem and develops finite fields.

New features include:

- a greater emphasis on aspects of finite groups—orders of elements, subgroups, cyclic groups, Lagrange’s theorem, the primary decomposition theorem;
- development of primality testing and factoring as a theme in the applications, with several new sections on factoring and several on primality testing, culminating in a proof of Rabin’s theorem on strong a -pseudoprime testing;
- increased use of the Chinese remainder theorem for both numbers and polynomials, as an important tool in applications;
- more explicit use of homomorphisms;
- a new treatment of quadratic reciprocity, and with added applications;
- a new chapter on the fundamental theorem of algebra which includes treatments of the cubic (Cardano) and quartic (Ferrari, Euler); and
- two applications (fast polynomial multiplication, Reed–Solomon codes) which use the discrete Fourier transform.

In an area moving as rapidly as computational number theory, many of the applications presented will, in practice, not be “the state of the art.” For example, probabilistic improvements on Berlekamp’s algorithm for factoring polynomials over finite fields have recently appeared (see von der Gathen and Schoup (1992), Kaltofen and Lobo (1994)); Rabin’s test is only one of the tools now used to test primality of large numbers (see Pinch (1993)); and Arjen Lenstra, on top of his team’s success in factoring the 129 digit number RSA-129 in 1994, promises dramatic improvements in the factorization of large numbers (see Lenstra and Lenstra (1993)). But while the applications we present may not represent the latest word, even as I write this Preface, they are nonetheless worthwhile pedagogically, as significant applications of the theory and as prerequisites for understanding the newer algorithms, and because in almost all cases they are elegant mathematics.

Prerequisites

The explicit prerequisite consists of precalculus algebra. However, experience with the first edition suggests that three or four semesters of college level mathematics, such as the calculus sequence and a semester of linear algebra, is helpful. Only a few sections of the book use calculus or linear algebra, and a course can easily be designed to avoid those sections. Elementary matrix theory is summarized in Chapter 13, and used to some extent in chapters 11E, 13E and F, 21B, 22A, 28E, 29, and 30B.

Designing a Course

There is enough material in this book for a full two-semester course in higher algebra and applications.

For a one-semester course there are a number of options.

The basic theory is found in Chapters 2A–D, 3A–C, 4A–B, 5, 6, 8, 9, 11A–B, 12A–B, 14, 15, 20, 23, 24, 28, and 30.

For the one-semester course I try to cover most of the basic theory, plus Chapter 10B and other applications as time allows. Other instructors do less theory and more applications.

A nice course on computational number theory can be taught from Chapters 1–12 and 23–27. Such a course, while not bringing out the parallelism of the theory for numbers and polynomials, would use group theory and the Chinese remainder theorem in significant ways in studying primality testing.

A course emphasizing polynomials could cover the basic theory through Chapter 12B and then focus on Chapters 14–22 and 28–30.

Acknowledgments

My thanks to the numerous colleagues and students at Albany who have used and commented on the book over the years, including Ed Davis, Bill Hammond, Ted Turner, Hugh Gordon, Malcolm Smiley, Lou Brickman, Tom MacGregor, Don Wilken, Ben Jamison, and Anupam Srivastav. Among those elsewhere who have commented on the book, I wish to acknowledge with appreciation Keith Conrad, Linda Dineen, David Ford, Irving Kaplansky, Keith Kendig, Richard Patterson, Michael Rosen, Alan Sprague, Mel Thornton, and S. Wang. I particularly thank David Drasin, for his comprehensive reading of the manuscript for the first edition; Hyman Bass, for his useful remarks on the need for more group theory in the book; and Ernst S. Selmer and Frank Gerrish, for their extensive lists of comments on the first edition. My thanks also to Michelle Palleschi, Mrs. Betty Turner, and Ellen Fisher for their assistance in preparing various versions of the manuscript. Finally, my greatest thanks go to Rhonda, for her love, understanding, and support while I worked on the manuscript over the years.

August 1995

LINDSAY N. CHILDS

Thanks to Tat-Hung Chan of Fredonia, Donald Crowe of Wisconsin (Madison), Richard Ehrenborg of Cornell, Bill Hammond of Albany, Olav Hjortaa of Bergen and Morris Orzech of Queen's for comments and corrections to the first printing. Errata and comments for this printing may be found at the home page of the Department of Mathematics, University at Albany (<http://math.albany.edu>).

May 1997

Lindsay N. Childs

Contents

Introduction	vii
CHAPTER 1	
Numbers	1
CHAPTER 2	
Induction	8
A. Induction	8
B. Another Form of Induction	13
C. Well-Ordering	16
D. Division Theorem	18
E. Bases	20
F. Operations in Base a	23
CHAPTER 3	
Euclid's Algorithm	25
A. Greatest Common Divisors	25
B. Euclid's Algorithm	27
C. Bezout's Identity	29
D. The Efficiency of Euclid's Algorithm	36
E. Euclid's Algorithm and Incommensurability	40
CHAPTER 4	
Unique Factorization	47
A. The Fundamental Theorem of Arithmetic	47
B. Exponential Notation	50
C. Primes	55
D. Primes in an Interval	59

CHAPTER 5	
Congruences	63
A. Congruence Modulo m	63
B. Basic Properties	65
C. Divisibility Tricks	68
D. More Properties of Congruence	71
E. Linear Congruences and Bezout's Identity	72
CHAPTER 6	
Congruence Classes	76
A. Congruence Classes (mod m): Examples	76
B. Congruence Classes and $\mathbb{Z}/m\mathbb{Z}$	80
C. Arithmetic Modulo m	82
D. Complete Sets of Representatives	86
E. Units	88
CHAPTER 7	
Applications of Congruences	91
A. Round Robin Tournaments	91
B. Pseudorandom Numbers	92
C. Factoring Large Numbers by Trial Division	100
D. Sieves	103
E. Factoring by the Pollard Rho Method	105
F. Knapsack Cryptosystems	111
CHAPTER 8	
Rings and Fields	118
A. Axioms	118
B. $\mathbb{Z}/m\mathbb{Z}$	124
C. Homomorphisms	127
CHAPTER 9	
Fermat's and Euler's Theorems	134
A. Orders of Elements	134
B. Fermat's Theorem	138
C. Euler's Theorem	141
D. Finding High Powers Modulo m	145
E. Groups of Units and Euler's Theorem	147
F. The Exponent of an Abelian Group	152
CHAPTER 10	
Applications of Fermat's and Euler's Theorems	155
A. Fractions in Base a	155
B. RSA Codes	164
C. 2-Pseudoprimes	169
D. Trial a -Pseudoprime Testing	175
E. The Pollard $p - 1$ Algorithm	177

Contents	xiii
CHAPTER 11	
On Groups	180
A. Subgroups	180
B. Lagrange's Theorem	182
C. A Probabilistic Primality Test	185
D. Homomorphisms	186
E. Some Nonabelian Groups	189
CHAPTER 12	
The Chinese Remainder Theorem	194
A. The Theorem	194
B. Products of Rings and Euler's ϕ -Function	202
C. Square Roots of 1 Modulo m	205
CHAPTER 13	
Matrices and Codes	208
A. Matrix Multiplication	209
B. Linear Equations	212
C. Determinants and Inverses	214
D. $M_n(R)$	215
E. Error-Correcting Codes, I	217
F. Hill Codes	224
CHAPTER 14	
Polynomials	231
CHAPTER 15	
Unique Factorization	239
A. Division Theorem	239
B. Primitive Roots	243
C. Greatest Common Divisors	245
D. Factorization into Irreducible Polynomials	249
CHAPTER 16	
The Fundamental Theorem of Algebra	253
A. Rational Functions	254
B. Partial Fractions	255
C. Irreducible Polynomials over \mathbb{R}	258
D. The Complex Numbers	260
E. Root Formulas	263
F. The Fundamental Theorem	269
G. Integrating	273
CHAPTER 17	
Derivatives	277
A. The Derivative of a Polynomial	277
B. Sturm's Algorithm	280

CHAPTER 18	
Factoring in $\mathbb{Q}[x]$, I	286
A. Gauss's Lemma	286
B. Finding Roots	289
C. Testing for Irreducibility	291
CHAPTER 19	
The Binomial Theorem in Characteristic p	293
A. The Binomial Theorem	293
B. Fermat's Theorem Revisited	297
C. Multiple Roots	300
CHAPTER 20	
Congruences and the Chinese Remainder Theorem	302
A. Congruences Modulo a Polynomial	302
B. The Chinese Remainder Theorem	308
CHAPTER 21	
Applications of the Chinese Remainder Theorem	310
A. The Method of Lagrange Interpolation	310
B. Fast Polynomial Multiplication	313
CHAPTER 22	
Factoring in $\mathbb{F}_p[x]$ and in $\mathbb{Z}[x]$	323
A. Berlekamp's Algorithm	323
B. Factoring in $\mathbb{Z}[x]$ by Factoring mod M	333
C. Bounding the Coefficients of Factors of a Polynomial	334
D. Factoring Modulo High Powers of Primes	338
CHAPTER 23	
Primitive Roots	346
A. Primitive Roots Modulo m	346
B. Polynomials Which Factor Modulo Every Prime	351
CHAPTER 24	
Cyclic Groups and Primitive Roots	353
A. Cyclic Groups	353
B. Primitive Roots Modulo p^e	356
CHAPTER 25	
Pseudoprimes	363
A. Lots of Carmichael Numbers	363
B. Strong a -Pseudoprimes	368
C. Rabin's Theorem	372

CHAPTER 26

Roots of Unity in $\mathbb{Z}/m\mathbb{Z}$	378
A. For Which a Is m an a -Pseudoprime?	378
B. Square Roots of -1 in $\mathbb{Z}/p\mathbb{Z}$	381
C. Roots of -1 in $\mathbb{Z}/m\mathbb{Z}$	382
D. False Witnesses	385
E. Proof of Rabin's Theorem	388
F. RSA Codes and Carmichael Numbers	392

CHAPTER 27

Quadratic Residues	397
A. Reduction to the Odd Prime Case	397
B. The Legendre Symbol	399
C. Proof of Quadratic Reciprocity	405
D. Applications of Quadratic Reciprocity	407

CHAPTER 28

Congruence Classes Modulo a Polynomial	414
A. The Ring $F[x]/m(x)$	414
B. Representing Congruence Classes mod $m(x)$	418
C. Orders of Elements	422
D. Inventing Roots of Polynomials	426
E. Finding Polynomials with Given Roots	428

CHAPTER 29

Some Applications of Finite Fields	432
A. Latin Squares	432
B. Error Correcting Codes	438
C. Reed–Solomon Codes	450

CHAPTER 30

Classifying Finite Fields	464
A. More Homomorphisms	464
B. On Berlekamp's Algorithm	468
C. Finite Fields Are Simple	469
D. Factoring $x^{p^n} - x$ in $\mathbb{F}_p[x]$	471
E. Counting Irreducible Polynomials	474
F. Finite Fields	477
G. Most Polynomials in $\mathbb{Z}[x]$ Are Irreducible	479

Hints to Selected Exercises	483
------------------------------------	------------

References	509
-------------------	------------

Index	513
--------------	------------