Abstract Algebra

A Comprehensive Introduction

Through this book, upper undergraduate mathematics majors will master a challenging yet rewarding subject, and approach advanced studies in algebra, number theory and geometry with confidence. Groups, rings and fields are covered in depth with a strong emphasis on irreducible polynomials, a fresh approach to modules and linear algebra, a fresh take on Gröbner theory, and a group theoretic treatment of Rejewski's deciphering of the Enigma machine. It includes a detailed treatment of the basics on finite groups, including Sylow theory and the structure of finite abelian groups. Galois theory and its applications to polynomial equations and geometric constructions are treated in depth. Those interested in computations will appreciate the novel treatment of division algorithms. This rigorous text "gets to the point," focusing on concisely demonstrating the concept at hand, taking a "definitions first, examples next" approach. Exercises reinforce the main ideas of the text and encourage students' creativity.

John W. Lawrence is Professor Emeritus at the University of Waterloo. He was born in Ottawa, Canada, and received degrees from Carleton University and McGill University. After a year of postdoctoral work at the University of Chicago, he joined the Pure Mathematics Department of the University of Waterloo. He now lives with his wife Louise, in Thornhill Canada, where he continues his research in mathematics and probability.

Frank A. Zorzitto is Professor Emeritus at the University of Waterloo. After receiving his doctorate at Queen's University in Kingston, Canada, he served for forty years as a researcher in algebra and a professor in the Pure Mathematics Department at the University of Waterloo, and served as Department Chair for twelve years. In recognition of his commitment to the education of students, he received the University's Distinguished Teaching Award. Upon his retirement he was made an Honorary Member of the University. Currently he offers an online course to high school math teachers, based on his ebook *A Taste of Number Theory*. He continues to teach and to write in his retirement.

CAMBRIDGE MATHEMATICAL TEXTBOOKS

Cambridge Mathematical Textbooks is a program of undergraduate and beginning graduate-level textbooks for core courses, new courses, and interdisciplinary courses in pure and applied mathematics. These texts provide motivation with plenty of exercises of varying difficulty, interesting examples, modern applications, and unique approaches to the material.

A complete list of books in the series can be found at www.cambridge.org/mathematics
Recent titles include the following:

Chance, Strategy, and Choice: An Introduction to the Mathematics of Games and Elections, S. B. Smith
Set Theory: A First Course, D. W. Cunningham
Chaotic Dynamics: Fractals, Tilings, and Substitutions, G. R. Goodson
A Second Course in Linear Algebra, S. R. Garcia & R. A. Horn
Introduction to Experimental Mathematics, S. Eilers & R. Johansen
Exploring Mathematics: An Engaging Introduction to Proof, J. Meier & D. Smith
A First Course in Analysis, J. B. Conway
Introduction to Probability, D. F. Anderson, T. Seppäläinen & B. Valkó
Linear Algebra, E. S. Meckes & M. W. Meckes
A Short Course in Differential Topology, B. I. Dundas
Abstract Algebra with Applications, A. Terras
Complex Analysis, D. E. Marshall
Abstract Algebra: A Comprehensive Introduction, J. W. Lawrence & F. A. Zorzitto

Abstract Algebra

A Comprehensive Introduction

John W. Lawrence
University of Waterloo, Ontario

Frank A. Zorzitto
University of Waterloo, Ontario

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre,
New Delhi – 110025, India

79 Anson Road, #06–04/06, Singapore 079906

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning, and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781108836654
DOI: 10.1017/9781108874328

First published 2021

Printed in the United Kingdom by TJ Books Limited, Padstow Cornwall

A catalogue record for this publication is available from the British Library.

ISBN 978-1-108-83665-4 Hardback

Additional resources for this publication at www.cambridge.org/abstract-algebra

Dedicated to our families...

Louise, Donna, Lisa, Joanna, Angela and Alex

Cambridge University Press
978-1-108-83665-4 — Abstract Algebra
John W. Lawrence , Frank A. Zorzitto
Frontmatter
More Information

Contents

Preface

Every practitioner of mathematics, pure or applied, could use some algebra. Algebra includes an adherence to precise definitions, a willingness to examine concrete problems through meaningful abstractions, and a thirst for lucid proofs based on the axiomatic method. Despite its challenges, algebra has for a long time now been a mainstay of the curriculum in mathematics programs. Not to mention that some people are actually drawn to its puzzles and surprises. Since Bartel Leendert van der Waerden's seminal book *Moderne Algebra* was published in 1930, a multitude of authors have offered their take on this subject. By means of this book we hope to make our contribution.

Our book is intended for senior undergraduate students of modern abstract algebra. Those more gifted in mathematics can well profit from it sooner. Beginning graduate students who need a refresher could find it useful as well. We expect that our reader comes with a bit of exposure to rigorous proofs, some familiarity with the common language of sets such as injective and surjective mappings, and some understanding of linear algebra including such notions as finite-dimensional vector spaces, non-singular matrices, and linear transformations.

In order for any mathematics book to be effective, it must be precise with the mathematics but also approachable to the student. We have tried to meet this goal by walking a fine line between proper mathematical formality and reader friendliness. We hope to have not written too much, but also not too little. There seem to be two points of view regarding the introduction of a concept. One is that the student should be gently exposed to motivating examples first. Another aims for efficiency, presenting the definitions and theorems at the outset. By and large we have taken a "definitions first – examples next" approach, thinking that too much effort at motivation can in its own way be distracting. Yet we have tried not to go overboard with this approach, and to offer motivating examples soon enough.

Obviously, the exercises are for learning. If the exercises in a book are too easy, the student will not learn enough, and quickly become bored. If they are too hard, discouragement can set in. We have decided to limit the number of exercises that are utterly routine. Yet once a student has digested a section, the bulk of the exercises that follow it should be of reasonable difficulty. Those exercises which might be considered hard are marked with an asterisk. In the end, the difficulty of the exercises will depend on the preparation, skill and stamina of the student.

Algebra now comprises several large areas and many special topics within them. This makes it challenging for authors to select which topics will meet the expectations of a broad segment of algebra instructors, whose task it is to pick a book for their students. We structured our book along the traditional lines of groups, rings, fields and Galois theory. For something extra we offer an in depth discussion of modules over principal ideal domains and of Gröbner bases, a subject which may be of interest to those who relish computing.

We open our book with a short discussion on the integers, primes and congruences, in order to ensure the student sees the ways of algebra within a truly basic example. These matters are treated in the spirit of a review, which could well be familiar to many a reader.

Our book more properly begins with Chapter 2 where we discuss groups, with an emphasis on finite groups, using a well trodden approach. The symmetric group gets a careful discussion. The fundamentals of Lagrange's theorem (including the failure of its converse), normal subgroups, homomorphisms, quotient groups, the first isomorphism theorem, internal and external products of groups, are covered along familiar lines. We close the chapter with a proof of the structure theorem for finite abelian groups. Since by its very nature this will demand a bit more of the student, we go at it with patience.

Chapter 3 focuses on group actions, orbits, stabilizers, some counting problems, the class equation, and the substantial Sylow theory. We introduce semi-direct products as a way to describe some groups. In anticipation of their use in Galois theory the chapter closes with the basics about solvable groups. Even though this is primarily a book in pure mathematics, we decided to close Chapter 3 with a discussion of the Enigma machine and how group theory was used to break the Enigma code. This is an interesting story of how abstract algebra influenced history.

Chapters 4 and 5 are about rings, with commutative domains as the primary focus. In Chapter 4 we cover the essential notions of units, zero divisors, ideals, integral domains, quotient rings, homomorphisms, the first isomorphism theorem, the correspondence theorem, maximal and prime ideals, and fraction fields. We also offer a somewhat more leisurely treatment of the notion of polynomials, which of course can be glossed over by those who feel it might be unnecessary. Chapter 5 is about primes, unique factorization, Euclidean domains, Gauss' lemma, irreducibility of polynomials, and the Hilbert basis theorem for Noetherian rings. We also introduce a souped up version of Eisenstein's criterion, which can be used in unexpected ways to compute degrees of field extensions.

In Chapter 6 we cover algebraic field extensions, splitting fields, separable polynomials, and the Galois group. Here the reader will find an unhurried treatment of the Galois correspondence. Some of the more important applications of Galois theory are offered in Chapter 7, including, of course, Galois' contribution on the solvability of polynomial equations by radicals. There is also a comprehensive treatment of ruler and compass constructions, which at one point uses a bit of Galois theory.

Chapter 8 deals with the structure theorem for finitely generated modules over principal ideal domains along with its application to the Jordan canonical form for matrices. Of course it also applies to finite (and even finitely generated) abelian groups, but that topic is dealt with in Chapter 2. A small bit of redundancy is useful because not every student will get to Chapter 8, and because students can benefit from seeing the same ideas more than once.

An expert may notice that our proofs of a few difficult points differ somewhat from the mainstream. We hope that the reader will like the way we have organized this challenging material.

Our treatment of Gröbner bases in Chapter 9 is more daring. We want to present the concept of a Gröbner basis in the setting of abstract algebra. For this reason we open up with a discussion of what we call a Gröbner domain. These can be seen as a generalization of Euclidean domains, which permits division algorithms in a larger context. Even though our chief example is the ring of polynomials in several variables over a field, we try to remain within the abstraction of Gröbner domains as much as possible.

Our closing Appendix A offers some informal set theory, including the equivalence of the axiom of choice and Zorn's lemma, a discussion of cardinality, and the use of these ideas to build the algebraic closure of any field. The preceding chapters do not make significant use of Appendix A. The proof that rings have maximal ideals is the main (and easy) application of Zorn's lemma. The material of Appendix A is offered for the student who might find it handy to have it here, and might appreciate our effort to make this abstract material approachable.

The book contains more than enough material for two semesters of instruction. We find it difficult to advise how much is to be covered in a given semester. This is because the length of a semester can differ across various jurisdictions, and also because classes can differ in their abilities and institutions can differ in their expectations. In our home university in a third year one semester course we typically would assume Chapter 1, and then cover much of Chapters 2, 3, 4 and 5 on groups and rings, possibly skipping a few themes such as semi-direct products, solvable groups, the Enigma machine, and irreducibility over Noetherian domains. This would be followed up in a second semester with an in depth discussion of field and Galois theory including a discussion of solvable groups. If the class is up to it, we might also treat Chapter 9 on Gröbner bases or possibly modules over principal ideal domains.

Here are some suggested ways to use our book for a one semester course:

- Chapters 1, 2, 3 for a course on groups
- Chapters 1, 4, 5, 6, 7 for a substantial course on commutative rings, fields and Galois theory
- Chapters 1, 4, 5, 8 for a course on commutative rings and modules
- Chapters 1, 4, 5, 9 for a course on rings and division algorithms.

Some instructors believe it is better to teach commutative rings before groups. Even though we have followed the common order of groups-rings-fields, an instructor who wishes to teach rings first should be able to jump into Chapter 4 from the get go. Our treatment of rings makes a small use of the basic facts about groups, but the very slight amount of group theory needed can readily be filled in by the instructor.

The book can also be used in algebra courses of a more general nature. We have tried to adopt a style that is student friendly by explaining the ideas and proofs in a detailed and self contained manner.

One irritant which we have tried to minimize is the somewhat distracting practice of referring to exercises or to other proofs within the proof of a result. Another distracting habit is to leave steps within a proof as an exercise. Of course this is deemed to encourage the student to work through some details. It can also be a reflection of an author's impatience. These features cannot be avoided entirely, but by proving virtually everything we claim at the moment we claim it, we think that reading our text will lead to a more seamless experience.

Our gratitude goes out to our Pure Mathematics Department at the University of Waterloo, which gave us the opportunity to teach courses in algebra and thereby come to appreciate what might be interesting, what might be important, and what might be fun. Our never ending streams of committed and often brilliant students taught us that algebra can be a pleasure to learn and to teach.