

ABSTRACT ALGEBRA

Second Edition

David S. Dummit
University of Vermont

Richard M. Foote
University of Vermont



John Wiley & Sons, Inc.
New York / Chichester / Weinheim / Brisbane / Singapore / Toronto

Cover photo: Rudolf Bauer, "Invention" (Composition 31), 1933. 51 3/8 × 51 3/8 inches (130.5 X 130.5 cms). Solomon R. Guggenheim Museum, New York. Gift, Solomon R. Guggenheim, 1941. Photo by David Heald. Copyright Solomon R. Guggenheim Foundation, New York. (FN 41.149)

This book was typeset using the Y&Y TeX System with DVIWindo. The text was set in Times Roman using *MathTime* from Y&Y, Inc. Titles were set in OceanSans. Printed and bound by Quebecor-Fairfield. The cover was printed by Lehigh Press Lithographers, Inc.

The paper in this book was manufactured by a mill whose forest management programs include sustained yield harvesting of its timberlands. Sustained yield harvesting principles ensure that the number of trees cut each year does not exceed the amount of new growth.

This book is printed on acid-free paper.

Copyright © 1999 by John Wiley and Sons, Inc. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (508) 750-8400, fax (508) 750-4470. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc. 605 Third Avenue, New York, NY 10158-0012, (212) 850-6008, E-mail: PERMREQ@WILEY.COM. To order books or for customer service call 1-800-CALL-WILEY(225-5945).

Library of Congress Cataloging-in-Publication Data

Dummit, David Steven.

Abstract algebra / David S. Dummit, Richard M. Foote. — 2nd ed.
p. cm.

Includes index.

ISBN 0-471-36857-1

I. Algebra, Abstract. I. Foote, Richard M.

II.

Title
QA162.D85 1999
512'.02—dc21

98-41445
CIP

Printed in the United States of America.

10 9 8 7 6 5 4 3

*Dedicated to our families
especially our wives
Janice and Zsuzsanna*

Contents

Preface to the Second Edition xi

Preface to the First Edition xiii

Preliminaries 1

- 0.1 Basics 1
- 0.2 Properties of the Integers 4
- 0.3 $\mathbb{Z} / n\mathbb{Z}$: The Integers Modulo n 8

Part I – GROUP THEORY 13

Chapter 1 Introduction to Groups 16

- 1.1 Basic Axioms and Examples 16
- 1.2 Dihedral Groups 23
- 1.3 Symmetric Groups 29
- 1.4 Matrix Groups 34
- 1.5 The Quaternion Group 36
- 1.6 Homomorphisms and Isomorphisms 37
- 1.7 Group Actions 42

Chapter 2 Subgroups 47

- 2.1 Definition and Examples 47
- 2.2 Centralizers and Normalizers, Stabilizers and Kernels 50
- 2.3 Cyclic Groups and Cyclic Subgroups 55
- 2.4 Subgroups Generated by Subsets of a Group 62
- 2.5 The Lattice of Subgroups of a Group 67

Chapter 3	Quotient Groups and Homomorphisms	74
3.1	Definitions and Examples	74
3.2	More on Cosets and Lagrange's Theorem	90
3.3	The Isomorphism Theorems	98
3.4	Composition Series and the Hölder Program	103
3.5	Transpositions and the Alternating Group	108
Chapter 4	Group Actions	114
4.1	Group Actions and Permutation Representations	114
4.2	Groups Acting on Themselves by Left Multiplication—Cayley's Theorem	120
4.3	Groups Acting on Themselves by Conjugation—The Class Equation	124
4.4	Automorphisms	135
4.5	The Sylow Theorems	141
4.6	The Simplicity of A_n	152
Chapter 5	Direct and Semidirect Products and Abelian Groups	154
5.1	Direct Products	154
5.2	The Fundamental Theorem of Finitely Generated Abelian Groups	160
5.3	Table of Groups of Small Order	169
5.4	Recognizing Direct Products	171
5.5	Semidirect Products	177
Chapter 6	Further Topics in Group Theory	190
6.1	p -groups, Nilpotent Groups, and Solvable Groups	190
6.2	Applications in Groups of Medium Order	203
6.3	A Word on Free Groups	216

Part II – RING THEORY 223

Chapter 7	Introduction to Rings	224
7.1	Basic Definitions and Examples	224
7.2	Examples: Polynomial Rings, Matrix Rings, and Group Rings	234
7.3	Ring Homomorphisms and Quotient Rings	240
7.4	Properties of Ideals	252
7.5	Rings of Fractions	261
7.6	The Chinese Remainder Theorem	266

Chapter 8 Euclidean Domains, Principal Ideal Domains and Unique Factorization Domains 271

- 8.1 Euclidean Domains 271
- 8.2 Principal Ideal Domains (P.I.D.s) 280
- 8.3 Unique Factorization Domains (U.F.D.s) 284

Chapter 9 Polynomial Rings 296

- 9.1 Definitions and Basic Properties 296
- 9.2 Polynomial Rings over Fields I 300
- 9.3 Polynomial Rings that are Unique Factorization Domains 304
- 9.4 Irreducibility Criteria 308
- 9.5 Polynomial Rings over Fields II 314

Part III – MODULES AND VECTOR SPACES 317

Chapter 10 Introduction to Module Theory 318

- 10.1 Basic Definitions and Examples 318
- 10.2 Quotient Modules and Module Homomorphisms 326
- 10.3 Generation of Modules, Direct Sums, and Free Modules 332
- 10.4 Tensor Products of Modules 339
- 10.5 Exact Sequences—Projective, Injective, and Flat Modules 358

Chapter 11 Vector Spaces 388

- 11.1 Definitions and Basic Theory 388
- 11.2 The Matrix of a Linear Transformation 395
- 11.3 Dual Vector Spaces 411
- 11.4 Determinants 415
- 11.5 Tensor Algebras, Symmetric and Exterior Algebras 421

Chapter 12 Modules over Principal Ideal Domains 436

- 12.1 The Basic Theory 438
- 12.2 The Rational Canonical Form 452
- 12.3 The Jordan Canonical Form 471

Part IV – FIELD THEORY AND GALOIS THEORY 489

Chapter 13 Field Theory 490

- 13.1 Basic Theory of Field Extensions 490
- 13.2 Algebraic Extensions 500
- 13.3 Classical Straightedge and Compass Constructions 511
- 13.4 Splitting Fields and Algebraic Closures 516
- 13.5 Separable and Inseparable Extensions 525
- 13.6 Cyclotomic Polynomials and Extensions 532

Chapter 14 Galois Theory 538

- 14.1 Basic Definitions 538
- 14.2 The Fundamental Theorem of Galois Theory 547
- 14.3 Finite Fields 565
- 14.4 Composite Extensions and Simple Extensions 571
- 14.5 Cyclotomic Extensions and Abelian Extensions over \mathbb{Q} 577
- 14.6 Galois Groups of Polynomials 587
- 14.7 Solvable and Radical Extensions: Insolvability of the Quintic 606
- 14.8 Computation of Galois Groups over \mathbb{Q} 621
- 14.9 Transcendental Extensions, Inseparable Extensions, Infinite Galois Groups 626

**Part V – AN INTRODUCTION TO COMMUTATIVE RINGS,
ALGEBRAIC GEOMETRY, AND
HOMOLOGICAL ALGEBRA 636**

Chapter 15 Commutative Rings and Algebraic Geometry 637

- 15.1 Noetherian Rings and Affine Algebraic Sets 637
- 15.2 Radicals and Affine Varieties 650
- 15.3 Integral Extensions and Hilbert's Nullstellensatz 665
- 15.4 Localization 677
- 15.5 The Prime Spectrum of a Ring 697

**Chapter 16 Artinian Rings, Discrete Valuation Rings, and
Dedekind Domains 716**

- 16.1 Artinian Rings 716
- 16.2 Discrete Valuation Rings 721
- 16.3 Dedekind Domains 730

Chapter 17	Introduction to Homological Algebra and Group Cohomology	743
17.1	Introduction to Homological Algebra—Ext and Tor	744
17.2	The Cohomology of Groups	764
17.3	Crossed Homomorphisms and $H^1(G, A)$	780
17.4	Group Extensions, Factor Sets and $H^2(G, A)$	790

**Part VI – INTRODUCTION TO THE REPRESENTATION
THEORY OF FINITE GROUPS 805**

Chapter 18	Representation Theory and Character Theory	806
18.1	Linear Actions and Modules over Group Rings	806
18.2	Wedderburn’s Theorem and Some Consequences	820
18.3	Character Theory and the Orthogonality Relations	830
Chapter 19	Examples and Applications of Character Theory	846
19.1	Characters of Groups of Small Order	846
19.2	Theorems of Burnside and Hall	852
19.3	Introduction to the Theory of Induced Characters	858

Appendix I:	Cartesian Products and Zorn’s Lemma	871
--------------------	--	------------

Appendix II:	Category Theory	877
---------------------	------------------------	------------

Index	885
--------------	------------

Preface to the Second Edition

In response to comments from readers of the first edition, this second edition contains a considerable amount of new material. We have continued to strive to make the material accessible to undergraduates but increased the scope of topics to make the book more attractive to graduate students. The emphasis throughout has been to motivate the introduction and development of important algebraic concepts using as many examples as possible.

Although the second edition contains substantially more than can normally be covered in a one year course, the new topics provide significantly greater flexibility for students and instructors wishing to pursue a number of important areas of modern algebra. The authors use the text both for the introductory undergraduate algebra course and also for topics courses at the graduate level.

Material has been added to Chapter 8 and more emphasis has been given to quadratic integer rings, which are introduced in Section 7.1 and developed more thoroughly through the text. The new sections 10.4 and 11.5 introduce tensor products of modules and tensor algebras. Section 10.5 discusses extensions, exact sequences and their behavior with respect to the Hom and tensor product functors, topics that are continued in Chapter 17 with an introduction to the basic notions of homological algebra. Chapter 17 also contains a relatively self-contained treatment of group cohomology. The added sections in Chapter 10 are at a slightly higher level of difficulty than the remainder of Chapter 10, and can be deferred on a first reading.

Chapters 15 and 16 are entirely new. These extend the early ring theory chapters and introduce relations between commutative algebra and geometry. Chapter 15 begins the exposition of some central concepts in commutative algebra and each section in this chapter is organized so that the abstract algebraic ideas are followed by their application in algebraic geometry. We focus on affine algebraic spaces, working from the basic definitions up to the definition of an affine scheme. Chapter 16 continues with commutative algebra and parallels Chapter 8 in layout, studying three families of rings (of Krull dimensions 0 and 1), culminating in the classification of finitely generated modules over Dedekind Domains.

The original chapters on representation theory of finite groups have now been moved to Part VI and updated in light of the new material now covered in earlier chapters. Categories and functors appear in Appendix II, not as an add-on but rather to signal that individuals may read (and reread) this material at almost any point in their

progress through the book. We have purposely minimized the functorial language in the text in order to keep the presentation as elementary as possible.

The remaining sections of the book are essentially the same as in the first edition, with the exception of a few added exercises such as ones that incorporate the new material into the old (exercises on tensor products of fields, for example), and an expanded explanation of some of the subtleties of generators and relations in Section 1.2. In some instances material that was in the exercises now appears in the text. Instructors may still offer a standard introduction to abstract algebra, as outlined at the end of the Preface to the First Edition. Another possibility is to cover the basic material on groups and rings from Parts I and II, Sections 10.1–10.3, 11.1, and then Chapters 15 and 16. These latter chapters are, for the most part, independent of Part IV, although basic knowledge of minimal polynomials and the definition of an algebraically closed field are required in Sections 15.3 and 15.4; tensor products are used occasionally to simplify proofs but can be avoided at the expense of some additional labor. Yet another stream is to include material through all of Chapter 10 and 11.1 followed then by Chapter 17 (which is essentially independent of the intervening chapters, except for examples involving Galois cohomology). Well integrated one semester courses for students previously having had some algebra might include Parts III and V, or Parts III and VI. This would provide a solid background for a second semester course delving more deeply into one of many possible areas: algebraic number theory, algebraic topology, algebraic geometry, representation theory, Lie groups, etc.

We have chosen the additional material and the style for developing it to reinforce a basic theme in the book: the power and beauty that accrues from a rich interplay between different areas of mathematics. We have not attempted to be encyclopedic, but have tried to touch on many of the central themes in elementary algebra in a manner suggesting the very natural development of these ideas. As in the first edition, a number of important ideas appear in the exercises. This is not because they are not significant, rather because they did not fit easily into the flow of the text but were too important to leave out entirely. Sequences of exercises on one topic are prefaced with some remarks and are structured so that they may be read without actually doing the exercises.

We have refrained from providing specific references for additional reading when there are many fine choices readily available. Also, while we have endeavored to include as many fundamental topics as possible, we apologize if for reasons of space or personal taste we have neglected any of the reader's particular favorites.

We again thank the many students and colleagues who have offered valuable comments on the first edition — it is their support and interest which has energized the writing of this second edition. We thank George Lobell of Prentice–Hall for his unfailing encouragement and support for the writing of this second edition. We would also like to thank Ken Brown, David Flath, Donald Passman, and Emma Previato for their useful comments on this second edition. Finally, we thank Louis Vosloo of Y&Y TeX, Inc., for his help.

David Dummit
Richard Foote

Preface to the First Edition

This book evolved out of notes by the authors from courses given at various universities over a period of about thirteen years. The backgrounds of students in these courses were quite diverse, ranging from first and second year undergraduates to beginning graduate students, and included computer science and other science and engineering majors in addition to mathematics majors. The expectations of the students were quite varied. For some, the algebra course was to be an introduction with no follow up (some took only one semester of the full year sequence) and for some the course was intended to be the foundation for future work in mathematics. We felt that all of these students should be given some insight into the main themes in abstract algebra and some understanding of how these themes provide a unifying framework for the study of the basic algebraic structures: groups, rings, and fields. One of our guiding principles has therefore been to introduce as early as possible notions such as homomorphisms, isomorphisms, actions, classifications, and the notion of the structure of an algebraic object. We point out how these themes recur as we pass from the study of one algebraic system to another and provide a natural flow for the development of basic abstract algebra. To a certain extent this has influenced our choice of material as well. We have made no attempt at being encyclopedic, but rather we have delved more deeply into a few areas in order that students may achieve a better grasp of how the structure of algebraic objects is unravelled in greater depth. Wherever possible we have attempted to broaden students' horizons by pointing out connections of one subject to other areas of algebra and mathematics and by mentioning results at the forefront of research. We also introduce new material in a form which students do not subsequently have to dislodge in favor of more sophisticated versions. So, for example, permutations are introduced in cycle notation format and quotients are developed as fibers of homomorphisms. In this way students are immediately exposed to concepts the way an algebraist (or mathematician) envisions and works with them.

The book contains a wealth of examples and exercises. The exercises range from routine computations to fairly sophisticated theoretical ones. All the exercises, however, are within the scope of the text and hints are given [in brackets] where we felt they were needed to make them accessible. The main results in the text do not rely on material in the exercises, although some details in proofs in the text are occasionally

left to the reader and some examples use results from the exercises. In many instances, new material is introduced first in the exercises (often a few sections before it appears in the text) so that students may obtain an easier introduction to it by doing these exercises (e.g., Lagrange's Theorem appears in the exercises in Section 1.7 and in the text in Section 3.2). The exercises also contain a considerable amount of material not covered in the text. Some exercises lead through a series of steps to new results such as Wedderburn's Theorem on finite division rings or Hilbert's Basis Theorem. There sometimes appear sequences of exercises on one topic; these problems are prefaced with some remarks and are structured so that they may be read as text without actually doing the exercises. Some of these sequences are reviews (such as the exercises on Gauss–Jordan elimination in Chapter 11) and others contain new material relating to another area (such as the exercises on the exponential of a matrix and its application to systems of differential equations in Section 12.3). In addition, a number of exercises describe useful computational techniques (for example, Berlekamp's Algorithm for factoring polynomials mod p in Section 14.3).

Notationally, Proposition 2 in Chapter 4 is referred to simply as Proposition 2 within Chapter 4 and as Proposition 4.2 in other chapters.

It is not usually possible to cover the entire text in one academic year, although the authors have been able to cover the bulk of the material in one year, including all of Part III and much of Part V. A basic introductory (one year) course should include Chapters 1 to 3, Sections 4.1 to 4.3, 5.1 to 5.3, Chapters 7 to 9, Sections 10.1, 11.1 and Chapters 13 and 14, returning to pick up Sections 4.4 to 4.6 if they are not covered initially. Parts III and V may also be used as a well integrated one semester course. We note that linear algebra is not assumed to be a prerequisite although knowledge of it does increase the repertoire of examples in group theory. The basic linear algebra covered in Chapter 11 provides the background mainly for the theory of canonical forms in Chapter 12.

Finally, we would like to thank D. Dorman, H. Kisilevsky, J. Sands, L. Simons and our students over the past few years for helpful suggestions and comments.