

# Abstract Algebra: The Basic Graduate Year

Robert B. Ash

## PREFACE

This is a text for the basic graduate sequence in abstract algebra, offered by most universities. We study fundamental algebraic structures, namely groups, rings, fields and modules, and maps between these structures. The techniques are used in many areas of mathematics, and there are applications to physics, engineering and computer science as well. In addition, I have attempted to communicate the intrinsic beauty of the subject. Ideally, the reasoning underlying each step of a proof should be completely clear, but the overall argument should be as brief as possible, allowing a sharp overview of the result. These two requirements are in opposition, and it is my job as expositor to try to resolve the conflict.

My primary goal is to help the reader learn the subject, and there are times when informal or intuitive reasoning leads to greater understanding than a formal proof. In the text, there are three types of informal arguments:

1. The concrete or numerical example with all features of the general case. Here, the example indicates how the proof should go, and the formalization amounts to substituting Greek letters for numbers. There is no essential loss of rigor in the informal version.
2. Brief informal surveys of large areas. There are two of these,  $p$ -adic numbers and group representation theory. References are given to books accessible to the beginning graduate student.
3. Intuitive arguments that replace lengthy formal proofs which do not reveal why a result is true. In this case, explicit references to a precise formalization are given. I am not saying that the formal proof should be avoided, just that the basic graduate year, where there are many pressing matters to cope with, may not be the appropriate place, especially when the result rather than the proof technique is used in applications.

I would estimate that about 90 percent of the text is written in conventional style, and I hope that the book will be used as a classroom text as well as a supplementary reference.

Solutions to all problems are included in the text; in my experience, most students find this to be a valuable feature. The writing style for the solutions is similar to that of the main text, and this allows for wider coverage as well as reinforcement of the basic ideas.

Chapters 1–4 cover basic properties of groups, rings, fields and modules. The typical student will have seen some but not all of this material in an undergraduate algebra course. [It should be possible to base an undergraduate course on Chapters 1–4, traversed at a suitable pace with detailed coverage of the exercises.] In Chapter 4, the fundamental structure theorems for finitely generated modules over a principal ideal domain are developed concretely with the aid of the Smith normal form. Students will undoubtedly be

comfortable with elementary row and column operations, and this will significantly aid the learning process.

In Chapter 5, the theme of groups acting on sets leads to a nice application to combinatorics as well as the fundamental Sylow theorems and some results on simple groups. Analysis of normal and subnormal series leads to the Jordan-Hölder theorem and to solvable and nilpotent groups. The final section, on defining a group by generators and relations, concentrates on practical cases where the structure of a group can be deduced from its presentation. Simplicity of the alternating groups and semidirect products are covered in the exercises.

Chapter 6 goes quickly to the fundamental theorem of Galois theory; this is possible because the necessary background has been covered in Chapter 3. After some examples of direct calculation of a Galois group, we proceed to finite fields, which are of great importance in applications, and cyclotomic fields, which are fundamental in algebraic number theory. The Galois group of a cubic is treated in detail, and the quartic is covered in an appendix. Sections on cyclic and Kummer extensions are followed by Galois' fundamental theorem on solvability by radicals. The last section of the chapter deals with transcendental extensions and transcendence bases.

In the remaining chapters, we begin to apply the results and methods of abstract algebra to related areas. The title of each chapter begins with "Introducing . . .", and the areas to be introduced are algebraic number theory, algebraic geometry, noncommutative algebra and homological algebra (including categories and functors).

Algebraic number theory and algebraic geometry are the two major areas that use the tools of commutative algebra (the theory of commutative rings). In Chapter 7, after an example showing how algebra can be applied in number theory, we assemble some algebraic equipment: integral extensions, norms, traces, discriminants, Noetherian and Artinian modules and rings. We then prove the fundamental theorem on unique factorization of ideals in a Dedekind domain. The chapter concludes with an informal introduction to  $p$ -adic numbers and some ideas from valuation theory.

Chapter 8 begins geometrically with varieties in affine space. This provides motivation for Hilbert's fundamental theorems, the basis theorem and the Nullstellensatz. Several equivalent versions of the Nullstellensatz are given, as well as some corollaries with geometric significance. Further geometric considerations lead to the useful algebraic techniques of localization and primary decomposition. The remainder of the chapter is concerned with the tensor product and its basic properties.

Chapter 9 begins the study of noncommutative rings and their modules. The basic theory of simple and semisimple rings and modules, along with Schur's lemma and Jacobson's theorem, combine to yield Wedderburn's theorem on the structure of semisimple rings. We indicate the precise connection between the two popular definitions of simple ring in the literature. After an informal introduction to group representations, Maschke's theorem on semisimplicity of modules over the group algebra is proved. The introduction of the Jacobson radical gives more insight into the structure of rings and modules. The chapter ends with the Hopkins-Levitzki theorem that an Artinian ring is Noetherian, and the useful lemma of Nakayama.

In Chapter 10, we introduce some of the tools of homological algebra. Waiting until the last chapter for this is a deliberate decision. Students need as much exposure as possible to specific algebraic systems before they can appreciate the broad viewpoint of

category theory. Even experienced students may have difficulty absorbing the abstract definitions of kernel, cokernel, product, coproduct, direct and inverse limit. To aid the reader, functors are introduced via the familiar examples of hom and tensor. No attempt is made to work with general abelian categories. Instead, we stay within the category of modules and study projective, injective and flat modules.

In a supplement, we go much farther into homological algebra than is usual in the basic algebra sequence. We do this to help students cope with the massive formal machinery that makes it so difficult to gain a working knowledge of this area. We concentrate on the results that are most useful in applications: the long exact homology sequence and the properties of the derived functors Tor and Ext. There is a complete proof of the snake lemma, a rarity in the literature. In this case, going through a long formal proof is entirely appropriate, because doing so will help improve algebraic skills. The point is not to avoid difficulties, but to make most efficient use of the finite amount of time available.

Robert B. Ash  
October 2000

### **Further Remarks**

Many mathematicians believe that formalism aids understanding, but I believe that when one is learning a subject, formalism often prevents understanding. The most important skill is the ability to think intuitively. This is true even in a highly abstract field such as homological algebra. My writing style reflects this view.

Classroom lectures are inherently inefficient. If the pace is slow enough to allow comprehension as the lecture is delivered, then very little can be covered. If the pace is fast enough to allow decent coverage, there will unavoidably be large gaps. Thus the student must depend on the textbook, and the current trend in algebra is to produce massive encyclopedias, which are likely to be quite discouraging to the beginning graduate student. Instead, I have attempted to write a text of manageable size, which can be read by students, including those working independently.

Another goal is to help the student reach an advanced level as quickly and efficiently as possible. When I omit a lengthy formal argument, it is because I judge that the increase in algebraic skills is insufficient to justify the time and effort involved in going through the formal proof. In all cases, I give explicit references where the details can be found. One can argue that learning to write formal proofs is an essential part of the student's mathematical training. I agree, but the ability to think intuitively is fundamental and must come first. I would add that the way things are today, there is absolutely no danger that the student will be insufficiently exposed to formalism and abstraction. In fact there is quite a bit of it in this book, although not 100 percent.

I offer this text in the hope that it will make the student's trip through algebra more enjoyable. I have done my best to avoid gaps in the reasoning. I never use the phrase "it is easy to see" under any circumstances. I welcome comments and suggestions for improvement.

Copyright © 2000, by Robert B. Ash

Paper or electronic copies for noncommercial use may be made freely without explicit permission of the author. All other rights are reserved.

# ABSTRACT ALGEBRA: THE BASIC GRADUATE YEAR

## TABLE OF CONTENTS

### CHAPTER 0 PREREQUISITES

- 0.1 Elementary Number Theory
- 0.2 Set Theory
- 0.3 Linear Algebra

### CHAPTER 1 GROUP FUNDAMENTALS

- 1.1 Groups and Subgroups
- 1.2 Permutation Groups
- 1.3 Cosets, Normal Subgroups and Homomorphisms
- 1.4 The Isomorphism Theorems
- 1.5 Direct Products

### CHAPTER 2 RING FUNDAMENTALS

- 2.1 Basic Definitions and Properties
- 2.2 Ideals, Homomorphisms and Quotient Rings
- 2.3 The Isomorphism Theorems For Rings
- 2.4 Maximal and Prime Ideals
- 2.5 Polynomial Rings
- 2.6 Unique Factorization
- 2.7 Principal Ideal Domains and Euclidean Domains
- 2.8 Rings of Fractions
- 2.9 Irreducible Polynomials

### CHAPTER 3 FIELD FUNDAMENTALS

- 3.1 Field Extensions
- 3.2 Splitting Fields
- 3.3 Algebraic Closures
- 3.4 Separability
- 3.5 Normal Extensions

### CHAPTER 4 MODULE FUNDAMENTALS

- 4.1 Modules and Algebras
- 4.2 The Isomorphism Theorems For Modules
- 4.3 Direct Sums and Free Modules
- 4.4 Homomorphisms and Matrices
- 4.5 Smith Normal Form
- 4.6 Fundamental Structure Theorems
- 4.7 Exact Sequences and Diagram Chasing

### CHAPTER 5 SOME BASIC TECHNIQUES OF GROUP THEORY

- 5.1 Groups Acting on Sets
- 5.2 The Orbit-Stabilizer Theorem
- 5.3 Applications to Combinatorics
- 5.4 The Sylow Theorems
- 5.5 Applications of the Sylow Theorems
- 5.6 Composition Series
- 5.7 Solvable and Nilpotent Groups

5.8 Generators and Relations

**CHAPTER 6 GALOIS THEORY**

- 6.1 Fixed Fields and Galois Groups
- 6.2 The Fundamental Theorem
- 6.3 Computing a Galois Group Directly
- 6.4 Finite Fields
- 6.5 Cyclotomic Fields
- 6.6 The Galois Group of a Cubic
- 6.7 Cyclic and Kummer Extensions
- 6.8 Solvability by Radicals
- 6.9 Transcendental Extensions
- Appendix to Chapter 6

**CHAPTER 7 INTRODUCING ALGEBRAIC NUMBER THEORY**

- 7.1 Integral Extensions
- 7.2 Quadratic Extensions of the Rationals
- 7.3 Norms and Traces
- 7.4 The Discriminant
- 7.5 Noetherian and Artinian Modules and Rings
- 7.6 Fractional Ideals
- 7.7 Unique Factorization of Ideals in a Dedekind Domain
- 7.8 Some Arithmetic in Dedekind Domains
- 7.9  $p$ -adic Numbers

**CHAPTER 8 INTRODUCING ALGEBRAIC GEOMETRY**

- 8.1 Varieties
- 8.2 The Hilbert Basis Theorem
- 8.3 The Nullstellensatz: Preliminaries
- 8.4 The Nullstellensatz: Equivalent Versions and Proof
- 8.5 Localization
- 8.6 Primary Decomposition
- 8.7 Tensor Product of Modules Over a Commutative Ring
- 8.8 General Tensor Products

**CHAPTER 9 INTRODUCING NONCOMMUTATIVE ALGEBRA**

- 9.1 Semisimple Modules
- 9.2 Two Key Theorems
- 9.3 Simple and Semisimple Rings
- 9.4 Further Properties of Simple Rings, Matrix Rings, and Endomorphisms
- 9.5 The Structure of Semisimple Rings
- 9.6 Maschke's Theorem
- 9.7 The Jacobson Radical
- 9.8 Theorems of Hopkins-Levitzki and Nakayama

**CHAPTER 10 INTRODUCING HOMOLOGICAL ALGEBRA**

- 10.1 Categories
- 10.2 Products and Coproducts
- 10.3 Functors
- 10.4 Exact Functors
- 10.5 Projective Modules
- 10.6 Injective Modules

10.7 Embedding into an Injective Module  
10.8 Flat Modules  
10.9 Direct and Inverse Limits  
Appendix to Chapter 10

**SUPPLEMENT**

S1 Chain Complexes  
S2 The Snake Lemma  
S3 The Long Exact Homology Sequence  
S4 Projective and Injective Resolutions  
S5 Derived Functors  
S6 Some Properties of Ext and Tor  
S7 Base Change in the Tensor Product

**SOLUTIONS TO PROBLEMS**