Cornerstones

Anthony W. Knapp

Basic Algebra

Along with a companion volume
Advanced Algebra

Birkhäuser
Boston • Basel • Berlin

Anthony W. Knapp
81 Upper Sheep Pasture Road
East Setauket, NY 11733-1729
U.S.A.
e-mail to: aknapp@math.sunysb.edu
http://www.math.sunysb.edu/˜aknapp/books/b-alg.html

Cover design by Mary Burgess.

Mathematics Subject Classicification (2000): 15-01, 20-02, 13-01, 12-01, 16-01, 08-01, 18A05, 68P30

Library of Congress Control Number: 2006932456

ISBN-10 0-8176-3248-4 eISBN-10 0-8176-4529-2
ISBN-13 978-0-8176-3248-9 eISBN-13 978-0-8176-4529-8

Advanced Algebra ISBN 0-8176-4522-5
Basic Algebra and *Advanced Algebra* (Set) ISBN 0-8176-4533-0

Printed on acid-free paper.

9 8 7 6 5 4 3 2 1

www.birkhauser.com (EB)

To Susan

and

To My Algebra Teachers:

Ralph Fox, John Fraleigh, Robert Gunning,
John Kemeny, Bertram Kostant, Robert Langlands,
Goro Shimura, Hale Trotter, Richard Williamson

CONTENTS

CONTENTS OF *ADVANCED ALGEBRA*

LIST OF FIGURES

PREFACE

Basic Algebra and its companion volume *Advanced Algebra* systematically develop concepts and tools in algebra that are vital to every mathematician, whether pure or applied, aspiring or established. These two books together aim to give the reader a global view of algebra, its use, and its role in mathematics as a whole. The idea is to explain what the young mathematician needs to know about algebra in order to communicate well with colleagues in all branches of mathematics.

The books are written as textbooks, and their primary audience is students who are learning the material for the first time and who are planning a career in which they will use advanced mathematics professionally. Much of the material in the books, particularly in *Basic Algebra* but also in some of the chapters of *Advanced Algebra*, corresponds to normal course work. The books include further topics that may be skipped in required courses but that the professional mathematician will ultimately want to learn by self-study. The test of each topic for inclusion is whether it is something that a plenary lecturer at a broad international or national meeting is likely to take as known by the audience.

The key topics and features of *Basic Algebra* are as follows:

- Linear algebra and group theory build on each other throughout the book. A small amount of linear algebra is introduced first, as the topic likely to be better known by the reader ahead of time, and then a little group theory is introduced, with linear algebra providing important examples.
- Chapters on linear algebra develop notions related to vector spaces, the theory of linear transformations, bilinear forms, classical linear groups, and multilinear algebra.
- Chapters on modern algebra treat groups, rings, fields, modules, and Galois groups, including many uses of Galois groups and methods of computation.
- Three prominent themes recur throughout and blend together at times: the analogy between integers and polynomials in one variable over a field, the interplay between linear algebra and group theory, and the relationship between number theory and geometry.
- The development proceeds from the particular to the general, often introducing examples well before a theory that incorporates them.
- More than 400 problems at the ends of chapters illuminate aspects of the text, develop related topics, and point to additional applications. A separate

90-page section "Hints for Solutions of Problems" at the end of the book gives detailed hints for most of the problems, complete solutions for many.

- Applications such as the fast Fourier transform, the theory of linear error-correcting codes, the use of Jordan canonical form in solving linear systems of ordinary differential equations, and constructions of interest in mathematical physics arise naturally in sequences of problems at the ends of chapters and illustrate the power of the theory for use in science and engineering.

Basic Algebra endeavors to show some of the interconnections between different areas of mathematics, beyond those listed above. Here are examples: Systems of orthogonal functions make an appearance with inner-product spaces. Covering spaces naturally play a role in the examination of subgroups of free groups. Cohomology of groups arises from considering group extensions. Use of the power-series expansion of the exponential function combines with algebraic numbers to prove that π is transcendental. Harmonic analysis on a cyclic group explains the mysterious method of Lagrange resolvents in the theory of Galois groups.

Algebra plays a singular role in mathematics by having been developed so extensively at such an early date. Indeed, the major discoveries of algebra even from the days of Hilbert are well beyond the knowledge of most nonalgebraists today. Correspondingly most of the subject matter of the present book is at least 100 years old. What has changed over the intervening years concerning algebra books at this level is not so much the mathematics as the point of view toward the subject matter and the relative emphasis on and generality of various topics. For example, in the 1920s Emmy Noether introduced vector spaces and linear mappings to reinterpret coordinate spaces and matrices, and she defined the ingredients of what was then called "modern algebra"—the axiomatically defined rings, fields, and modules, and their homomorphisms. The introduction of categories and functors in the 1940s shifted the emphasis even more toward the homomorphisms and away from the objects themselves. The creation of homological algebra in the 1950s gave a unity to algebraic topics cutting across many fields of mathematics. Category theory underwent a period of great expansion in the 1950s and 1960s, followed by a contraction and a return more to a supporting role. The emphasis in topics shifted. Linear algebra had earlier been viewed as a separate subject, with many applications, while group theory and the other topics had been viewed as having few applications. Coding theory, cryptography, and advances in physics and chemistry have changed all that, and now linear algebra and group theory together permeate mathematics and its applications. The other subjects build on them, and they too have extensive applications in science and engineering, as well as in the rest of mathematics.

Basic Algebra presents its subject matter in a forward-looking way that takes this evolution into account. It is suitable as a text in a two-semester advanced undergraduate or first-year graduate sequence in algebra. Depending on the graduate school, it may be appropriate to include also some material from *Advanced Algebra*. Briefly the topics in *Basic Algebra* are linear algebra and group theory, rings, fields, and modules. A full list of the topics in *Advanced Algebra* appears on page x; of these, the Wedderburn theory of semisimple algebras, homological algebra, and foundational material for algebraic geometry are the ones that most commonly appear in syllabi of first-year graduate courses.

A chart on page xvii tells the dependence among chapters and can help with preparing a syllabus. Chapters I–VII treat linear algebra and group theory at various levels, except that three sections of Chapter IV and one of Chapter V introduce rings and fields, polynomials, categories and functors, and determinants over commutative rings with identity. Chapter VIII concerns rings, with emphasis on unique factorization; Chapter IX concerns field extensions and Galois theory, with emphasis on applications of Galois theory; and Chapter X concerns modules and constructions with modules.

For a graduate-level sequence the syllabus is likely to include all of Chapters I–V and parts of Chapters VIII and IX, at a minimum. Depending on the knowledge of the students ahead of time, it may be possible to skim much of the first three chapters and some of the beginning of the fourth; then time may allow for some of Chapters VI and VII, or additional material from Chapters VIII and IX, or some of the topics in *Advanced Algebra*. For many of the topics in *Advanced Algebra*, parts of Chapter X of *Basic Algebra* are prerequisite.

For an advanced undergraduate sequence the first semester can include Chapters I through III except Section II.9, plus the first six sections of Chapter IV and as much as reasonable from Chapter V; the notion of category does not appear in this material. The second semester will involve categories very gently; the course will perhaps treat the remainder of Chapter IV, the first five or six sections of Chapter VIII, and at least Sections 1–3 and 5 of Chapter IX.

More detailed information about how the book can be used with courses can be deduced by using the chart on page xvii in conjunction with the section "Guide for the Reader" on pages xix–xxii. In my own graduate teaching, I have built one course around Chapters I–III, Sections 1–6 of Chapter IV, all of Chapter V, and about half of Chapter VI. A second course dealt with the remainder of Chapter IV, a little of Chapter VII, Sections 1–6 of Chapter VIII, and Sections 1–11 of Chapter IX.

The problems at the ends of chapters are intended to play a more important role than is normal for problems in a mathematics book. Almost all problems are solved in the section of hints at the end of the book. This being so, some blocks of problems form additional topics that could have been included in the text but were not; these blocks may either be regarded as optional topics, or they may be treated as challenges for the reader. The optional topics of this kind usually either carry out further development of the theory or introduce significant applications. For example one block of problems at the end of Chapter VII carries the theory of representations of finite groups a little further by developing the Poisson summation formula and the fast Fourier transform. For a second example blocks of problems at the ends of Chapters IV, VII, and IX introduce linear error-correcting codes as an application of the theory in those chapters.

Not all problems are of this kind, of course. Some of the problems are really pure or applied theorems, some are examples showing the degree to which hypotheses can be stretched, and a few are just exercises. The reader gets no indication which problems are of which type, nor of which ones are relatively easy. Each problem can be solved with tools developed up to that point in the book, plus any additional prerequisites that are noted.

Beyond a standard one-variable calculus course, the most important prerequisite for using *Basic Algebra* is that the reader already know what a proof is, how to read a proof, and how to write a proof. This knowledge typically is obtained from honors calculus courses, or from a course in linear algebra, or from a first junior–senior course in real variables. In addition, it is assumed that the reader is comfortable with a small amount of linear algebra, including matrix computations, row reduction of matrices, solutions of systems of linear equations, and the associated geometry. Some prior exposure to groups is helpful but not really necessary.

The theorems, propositions, lemmas, and corollaries within each chapter are indexed by a single number stream. Figures have their own number stream, and one can find the page reference for each figure from the table on pages xi–xii. Labels on displayed lines occur only within proofs and examples, and they are local to the particular proof or example in progress. Some readers like to skim or skip proofs on first reading; to facilitate this procedure, each occurrence of the word "PROOF" or "PROOF" is matched by an occurrence at the right margin of the symbol □ to mark the end of that proof.

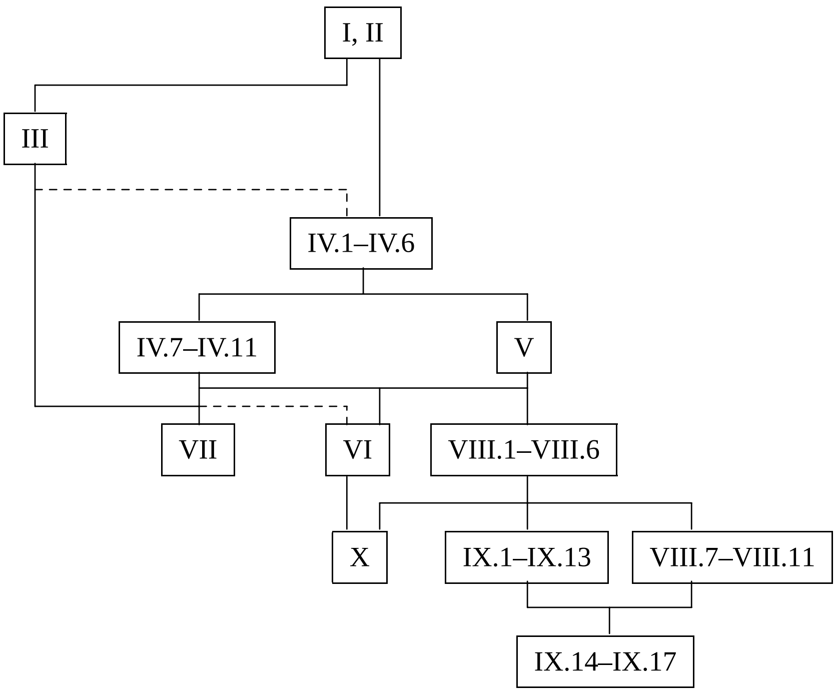
I am grateful to Ann Kostant and Steven Krantz for encouraging this project and for making many suggestions about pursuing it. I am especially indebted to an anonymous referee, who made detailed comments about many aspects of a preliminary version of the book, and to David Kramer, who did the copyediting. The typesetting was by AMS-TEX, and the figures were drawn with Mathematica.

I invite corrections and other comments from readers. I plan to maintain a list of known corrections on my own Web page.

A. W. KNAPP
August 2006

DEPENDENCE AMONG CHAPTERS

Below is a chart of the main lines of dependence of chapters on prior chapters. The dashed lines indicate helpful motivation but no logical dependence. Apart from that, particular examples may make use of information from earlier chapters that is not indicated by the chart.



STANDARD NOTATION

See the Index of Notation, pp. 699–701, for symbols defined starting on page 1.

Item	**Meaning**
$\#S$ or $\|S\|$	number of elements in S
$\varnothing$	empty set
$\{x \in E \mid P\}$	the set of x in E such that P holds
E^c	complement of the set E
$E \cup F,\ E \cap F,\ E - F$	union, intersection, difference of sets
$\bigcup_\alpha E_\alpha,\ \bigcap_\alpha E_\alpha$	union, intersection of the sets E_α
$E \subseteq F,\ E \supseteq F$	E is contained in F, E contains F
$E \subsetneqq F,\ E \supsetneqq F$	E properly contained in F, properly contains F
$E \times F,\ \bigtimes_{s \in S} X_s$	products of sets
$(a_1, \ldots, a_n),\ \{a_1, \ldots, a_n\}$	ordered n-tuple, unordered n-tuple
$f : E \to F,\ x \mapsto f(x)$	function, effect of function
$f \circ g$ or $fg,\ f\big\|_E$	composition of g followed by f, restriction to E
$f(\,\cdot\,, y)$	the function $x \mapsto f(x, y)$
$f(E),\ f^{-1}(E)$	direct and inverse image of a set
δ_{ij}	Kronecker delta: 1 if $i = j$, 0 if $i \neq j$
$\binom{n}{k}$	binomial coefficient
n positive, n negative	$n > 0$, $n < 0$
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	integers, rationals, reals, complex numbers
max (and similarly min)	maximum of a finite subset of a totally ordered set
$\sum$ or $\prod$	sum or product, possibly with a limit operation
countable	finite or in one-one correspondence with $\mathbb{Z}$
$[x]$	greatest integer $\leq x$ if x is real
Re z, Im z	real and imaginary parts of complex z
$\bar{z}$	complex conjugate of z
$\|z\|$	absolute value of z
1	multiplicative identity
1 or I	identity matrix or operator
1_X	identity function on X
$\mathbb{Q}^n, \mathbb{R}^n, \mathbb{C}^n$	spaces of column vectors
$\operatorname{diag}(a_1, \ldots, a_n)$	diagonal matrix
$\cong$	is isomorphic to, is equivalent to

GUIDE FOR THE READER

This section is intended to help the reader find out what parts of each chapter are most important and how the chapters are interrelated. Further information of this kind is contained in the abstracts that begin each of the chapters.

The book pays attention to at least three recurring themes in algebra, allowing a person to see how these themes arise in increasingly sophisticated ways. These are the analogy between integers and polynomials in one indeterminate over a field, the interplay between linear algebra and group theory, and the relationship between number theory and geometry. Keeping track of how these themes evolve will help the reader understand the mathematics better and anticipate where it is headed.

In Chapter I the analogy between integers and polynomials in one indeterminate over the rationals, reals, or complex numbers appears already in the first three sections. The main results of these sections are theorems about unique factorization in each of the two settings. The relevant parts of the underlying structures for the two settings are the same, and unique factorization can therefore be proved in both settings by the same argument. Many readers will already know this unique factorization, but it is worth examining the parallel structure and proof at least quickly before turning to the chapters that follow.

Before proceeding very far into the book, it is worth looking also at the appendix to see whether all its topics are familiar. Readers will find Section A1 useful at least for its summary of set-theoretic notation and for its emphasis on the distinction between range and image for a function. This distinction is usually unimportant in analysis but becomes increasingly important as one studies more advanced topics in algebra. Readers who have not specifically learned about equivalence relations and partial orderings can learn about them from Sections A2 and A5. Sections A3 and A4 concern the real and complex numbers; the emphasis is on notation and the Intermediate Value Theorem, which plays a role in proving the Fundamental Theorem of Algebra. Zorn's Lemma and cardinality in Sections A5 and A6 are usually unnecessary in an undergraduate course. They arise most importantly in Sections II.9 and IX.4, which are normally omitted in an undergraduate course, and in Proposition 8.8, which is invoked only in the last few sections of Chapter VIII.

The remainder of this section is an overview of individual chapters and pairs of chapters.

Chapter I is in three parts. The first part, as mentioned above, establishes unique factorization for the integers and for polynomials in one indeterminate over the rationals, reals, or complex numbers. The second part defines permutations and shows that they have signs such that the sign of any composition is the product of the signs; this result is essential for defining general determinants in Section II.7. The third part will likely be a review for all readers. It establishes notation for row reduction of matrices and for operations on matrices, and it uses row reduction to show that a one-sided inverse for a square matrix is a two-sided inverse.

Chapters II–III treat the fundamentals of linear algebra. Whereas the matrix computations in Chapter I were concrete, Chapters II–III are relatively abstract. Much of this material is likely to be a review for graduate students. The geometric interpretation of vectors spaces, subspaces, and linear mappings is not included in the chapter, being taken as known previously. The fundamental idea that a newly constructed object might be characterized by a "universal mapping property" appears for the first time in Chapter II, and it appears more and more frequently throughout the book. One aspect of this idea is that it is sometimes not so important what certain constructed objects are, but what they do. A related idea being emphasized is that the mappings associated with a newly constructed object are likely to be as important as the object, if not more so; at the least, one needs to stop and find what those mappings are. Section II.9 uses Zorn's Lemma and can be deferred until Chapter IX if one wants. Chapter III discusses special features of real and complex vector spaces endowed with inner products. The main result is the Spectral Theorem in Section 3. Many of the problems at the end of the chapter make contact with real analysis. The subject of linear algebra continues in Chapter V.

Chapter IV is the primary chapter on group theory and may be viewed as in three parts. Sections 1–6 form the first part, which is essential for all later chapters in the book. Sections 1–3 introduce groups and some associated constructions, along with a number of examples. Many of the examples will be seen to be related to specific or general vector spaces, and thus the theme of the interplay between group theory and linear algebra is appearing concretely for the first time. In practice, many examples of groups arise in the context of group actions, and abstract group actions are defined in Section 6. Of particular interest are group representations, which are group actions on a vector space by linear mappings. Sections 4–5 are a digression to define rings, fields, and ring homomorphisms, and to extend the theories concerning polynomials and vector spaces as presented in Chapters I–II. The immediate purpose of the digression is to make prime fields, their associated multiplicative groups, and the notion of characteristic available for the remainder of the chapter. The definition of vector space is extended to allow scalars from any field. The definition of polynomial is extended to allow coefficients from any commutative ring with identity, rather than just the rationals or reals or complex numbers, and to allow more than one indeterminate. Universal mapping properties for polynomial rings are proved. Sections 7–10 form the second part of the chapter and are a continuation of group theory. The main result is the Fundamental Theorem of Finitely Generated Abelian Groups, which is in Section 9. Section 11 forms the third part of the chapter. This section is a gentle introduction to categories and functors, which are useful for working with parallel structures in different settings within algebra. As S. Mac Lane says in his book, "Category theory asks of every type of Mathematical object: 'What are the morphisms?'; it suggests that these morphisms should be described at the same time as the objects. . . . This emphasis on (homo)morphisms is largely due to Emmy Noether, who emphasized the use of homomorphisms of groups and rings." The simplest parallel structure reflected in categories is that of an isomorphism. The section also discusses general notions of product and coproduct functors. Examples of products are direct products in linear algebra and in group theory. Examples of coproducts are direct sums in linear algebra and in *abelian* group theory, as well as disjoint unions in set theory. The theory in this section helps in unifying the mathematics that is to come in Chapters VI–VIII and X. The subject of group theory in continued in Chapter VII, which assumes knowledge of the material on category theory.

Chapters V and VI continue the development of linear algebra. Chapter VI uses categories, but Chapter V does not. Most of Chapter V concerns the analysis of a linear transformation carrying a finite-dimensional vector space over a field into itself. The questions are to find invariants of such transformations and to classify the transformations up to similarity. Section 2 at the start extends the theory of determinants so that the matrices are allowed to have entries in a commutative ring with identity; this extension is necessary in order to be able to work easily with characteristic polynomials. The extension of this theory is carried out by an important principle known as the "permanence of identities." Chapter VI largely concerns bilinear forms and tensor products, again in the context that the coefficients are from a field. This material is necessary in many applications to geometry and physics, but it is not needed in Chapters VII–IX. Many objects in the chapter are constructed in such a way that they are uniquely determined by a universal mapping property. Problems 18–22 at the end of the chapter discuss universal mapping properties in the general context of category theory, and they show that a uniqueness theorem is automatic in all cases.

Chapter VII continues the development of group theory, making use of category theory. It is in two parts. Sections 1–3 concern free groups and the topic of generators and relations; they are essential for abstract descriptions of groups and for work in topology involving fundamental groups. Section 3 constructs a notion of free product and shows that it is the coproduct functor for the category of groups. Sections 4–6 continue the theme of the interplay of group theory and linear algebra. Section 4 analyzes group representations of a finite group when the underlying field is the complex numbers, and Section 5 applies this theory to obtain a conclusion about the structure of finite groups. Section 6 studies extensions of groups and uses them to motivate the subject of cohomology of groups.

Chapter VIII introduces modules, giving many examples in Section 1, and then goes on to discuss questions of unique factorization in integral domains. Section 6 obtains a generalization for principal ideal domains of the Fundamental Theorem of Finitely Generated Abelian Groups, once again illustrating the first theme—similarities between the integers and certain polynomial rings. Section 7 introduces the third theme, the relationship between number theory and geometry, as a more sophisticated version of the first theme. The section compares a certain polynomial ring in two variables with a certain ring of algebraic integers that extends the ordinary integers. Unique factorization of elements fails for both, but the geometric setting has a more geometrically meaningful factorization in terms of ideals that is evidently unique. This kind of unique factorization turns out to work for the ring of algebraic integers as well. Sections 8–11 expand the examples in Section 7 into a theory of unique factorization of ideals in any integrally closed Noetherian domain whose nonzero prime ideals are all maximal.

Chapter IX analyzes algebraic extensions of fields. The first 13 sections make use only of Sections 1–6 in Chapter VIII. Sections 1–5 of Chapter IX give the foundational theory, which is sufficient to exhibit all the finite fields and to prove that certain classically proposed constructions in Euclidean geometry are impossible. Sections 6–8 introduce Galois theory, but Theorem 9.28 and its three corollaries may be skipped if Sections 14–17 are to be omitted. Sections 9–11 give a first round of applications of Galois theory: Gauss's theorem about which regular n-gons are in principle constructible with straightedge and compass, the Fundamental Theorem of Algebra, and the Abel–Galois theorem that solvability of a polynomial equation with rational coefficients in terms of radicals implies solvability of the Galois group. Sections 12–13 give a second round of applications: Gauss's method in principle for actually constructing the constructible regular n-gons and a converse to the Abel–Galois theorem. Sections 14–17 make use of Sections 7–11 of Chapter VIII, proving that π is transcendental and obtaining two methods for computing Galois groups.

Chapter X is a relatively short chapter developing further tools for dealing with modules over a ring with identity. The main construction is that of the tensor product over a ring of a unital right module and a unital left module, the result being an abelian group. The chapter makes use of material from Chapters VI and VIII, but not from Chapter IX.