Graduate Texts in
Mathematics

136

Algebra An Approach via Module Theory

Springer-Verlag

William A. Adkins
Steven H. Weintraub

Algebra

An Approach via Module Theory

Springer-Verlag

William A. Adkins
Steven H. Weintraub
Department of Mathematics
Louisiana State University
Baton Rouge, LA 70803
USA

Mathematics Subject Classifications: 12-01, 13-01, 15-01, 16-01, 20-01

Library of Congress Cataloging-in-Publication Data
Adkins, William A.
Algebra: an approach via module theory/William A. Adkins, Steven H. Weintraub.
p. cm. — (Graduate texts in mathematics; 136)
Includes bibliographical references and indexes.
ISBN 0-387-97839-9. — ISBN 3-540-97839-9
1. Algebra. 2. Modules (Algebra) I. Weintraub, Steven H. II. Title. III. Series.
QA154.A33 1992
512'.4—dc20 92-11951

Printed on acid-free paper.

Production managed by Francine Sikorski; manufacturing supervised by Jacqui Ashri.
Photocomposed copy prepared using TeX.
Printed and bound by R.R. Donnelley and Sons, Harrisonburg, VA.
Printed in the United States of America.

9 8 7 6 5 4 3 2 1

ISBN 0-387-97839-9 Springer-Verlag New York Berlin Heidelberg
ISBN 3-540-97839-9 Springer-Verlag Berlin Heidelberg New York

Graduate Texts in Mathematics 136

Graduate Texts in Mathematics

1 TAKEUTI/ZARING. Introduction to Axiomatic Set Theory. 2nd ed.
2 OXTOBY. Measure and Category. 2nd ed.
3 SCHAEFFER. Topological Vector Spaces.
4 HILTON/STAMMBACH. A Course in Homological Algebra.
5 MAC LANE. Categories for the Working Mathematician.
6 HUGHES/PIPER. Projective Planes.
7 SERRE. A Course in Arithmetic.
8 TAKEUTI/ZARING. Axiometic Set Theory.
9 HUMPHREYS. Introduction to Lie Algebras and Representation Theory.
10 COHEN. A Course in Simple Homotopy Theory.
11 CONWAY. Functions of One Complex Variable. 2nd ed.
12 BEALS. Advanced Mathematical Analysis.
13 ANDERSON/FULLER. Rings and Categories of Modules. 2nd ed.
14 GOLUBITSKY/GUILEMIN. Stable Mappings and Their Singularities.
15 BERBERIAN. Lectures in Functional Analysis and Operator Theory.
16 WINTER. The Structure of Fields.
17 ROSENBLATT. Random Processes. 2nd ed.
18 HALMOS. Measure Theory.
19 HALMOS. A Hilbert Space Problem Book. 2nd ed., revised.
20 HUSEMOLLER. Fibre Bundles. 2nd ed.
21 HUMPHREYS. Linear Algebraic Groups.
22 BARNES/MACK. An Algebraic Introduction to Mathematical Logic.
23 GREUB. Linear Algebra. 4th ed.
24 HOLMES. Geometric Functional Analysis and Its Applications.
25 HEWITT/STROMBERG. Real and Abstract Analysis.
26 MANES. Algebraic Theories.
27 KELLEY. General Topology.
28 ZARISKI/SAMUEL. Commutative Algebra. Vol. I.
29 ZARISKI/SAMUEL. Commutative Algebra. Vol. II.
30 JACOBSON. Lectures in Abstract Algebra I. Basic Concepts.
31 JACOBSON. Lectures in Abstract Algebra II. Linear Algebra.
32 JACOBSON. Lectures in Abstract Algebra III. Theory of Fields and Galois Theory.
33 HIRSCH. Differential Topology.
34 SPITZER. Principles of Random Walk. 2nd ed.
35 WERMER. Banach Algebras and Several Complex Variables. 2nd ed.
36 KELLEY/NAMIOKA et al. Linear Topological Spaces.
37 MONK. Mathematical Logic.
38 GRAUERT/FRITZSCHE. Several Complex Variables.
39 ARVESON. An Invitation to C^* -Algebras.
40 KEMENY/SNELL/KNAPP. Denumerable Markov Chains. 2nd ed.
41 APOSTOL. Modular Functions and Dirichlet Series in Number Theory. 2nd ed.
42 SERRE. Linear Representations of Finite Groups.
43 GILLMAN/JERISON. Rings of Continuous Functions.
44 KENDIG. Elementary Algebraic Geometry.
45 LOÈVE. Probability Theory I. 4th ed.
46 LOÈVE. Probability Theory II. 4th ed.
47 MOISE. Geometric Topology in Dimentions 2 and 3.

continued after index

William A. Adkins Steven H. Weintraub

Algebra

An Approach via Module Theory

Springer-Verlag
New York Berlin Heidelberg London Paris
Tokyo Hong Kong Barcelona Budapest

Preface

This book is designed as a text for a first-year graduate algebra course. As necessary background we would consider a good undergraduate linear algebra course. An undergraduate abstract algebra course, while helpful, is not necessary (and so an adventurous undergraduate might learn some algebra from this book).

Perhaps the principal distinguishing feature of this book is its point of view. Many textbooks tend to be encyclopedic. We have tried to write one that is thematic, with a consistent point of view. The theme, as indicated by our title, is that of modules (though our intention has not been to write a textbook purely on module theory). We begin with some group and ring theory, to set the stage, and then, in the heart of the book, develop module theory. Having developed it, we present some of its applications: canonical forms for linear transformations, bilinear forms, and group representations.

Why modules? The answer is that they are a basic unifying concept in mathematics. The reader is probably already familiar with the basic role that vector spaces play in mathematics, and modules are a generalization of vector spaces. (To be precise, modules are to rings as vector spaces are to fields.) In particular, both abelian groups and vector spaces with a linear transformation are examples of modules, and we stress the analogy between the two—the basic structure theorems in each of these areas are special cases of the structure theorem of finitely generated modules over a principal ideal domain (PID). As well, our last chapter is devoted to the representation theory of a group G over a field $\mathbf{F}$, this being an important and beautiful topic, and we approach it from the point of view of such a representation being an $\mathbf{F}(G)$-module. On the one hand, this approach makes it very clear what is going on, and on the other hand, this application shows the power of the general theory we develop.

We have heard the joke that the typical theorem in mathematics states that something you do not understand is equal to something else you cannot compute. In that sense we have tried to make this book atypical. It has been our philosophy while writing this book to provide proofs with a

maximum of insight and a minimum of computation, in order to promote understanding. However, since in practice it is necessary to be able to compute as well, we have included extensive material on computations. (For example, in our entire development in Chapter 4 of canonical forms for linear transformations we only have to compute one determinant, that of a companion matrix. But then Chapter 5 is almost entirely dedicated to computational methods for modules over a PID, showing how to find canonical forms and characteristic polynomials. As a second example, we derive the basic results about complex representations of finite groups in Section 8.3, without mentioning the word *character*, but then devote Section 8.4 to characters and how to use them.)

Here is a more detailed listing of the contents of the book, with emphasis on its novel features:

Chapter 1 is an introduction to (or review of) group theory, including a discussion of semidirect products.

Chapter 2 is an introduction to ring theory, covering a variety of standard topics.

In Chapter 3 we develop basic module theory. This chapter culminates in the structure theorem for finitely generated modules over a PID. (We then specialize to obtain the basic structure theorem for finitely generated Abelian groups.) We feel that our proof of this theorem is a particularly insightful one. (Note that in considering free modules we do not assume the corresponding results for vector spaces to be already known.) Noteworthy along the way is our introduction and use of the language of homological algebra and our discussion of free and projective modules.

We begin Chapter 4 with a treatment of basic topics in linear algebra. In principle, this should be a review, but we are careful to develop as much of the theory as possible over a commutative ring (usually a PID) rather than just restricting ourselves to a field. The matrix representation for module homomorphisms is even developed for modules over noncommutative rings, since this is needed for applications to Wedderburn's theorem in Chapter 7. This chapter culminates in the derivation of canonical forms (the rational canonical form, the (generalized) Jordan canonical form) for linear transformations. Here is one place where the module theory shows its worth. By regarding a vector space V over a field F, with a linear transformation T, as an $F[X]$-module (with X acting by T), these canonical forms are immediate consequences of the structure theorem for finitely generated torsion modules over a PID. We also derive the important special case of the real Jordan canonical form, and end the chapter by deriving the spectral theorem.

Chapter 5 is a computational chapter, showing how to obtain effectively (in so far as is possible) the canonical forms of Chapter 4 in concrete cases. Along the way, we introduce the Smith and Hermite canonical forms as well.

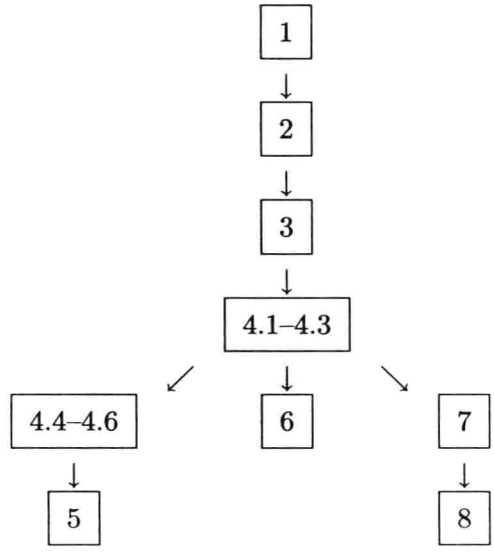
This chapter also has Dixon's proof of a criterion for similarity of matrices based solely on rank computations.

In Chapter 6 we discuss duality and investigate bilinear, sesquilinear, and quadratic forms, with the assistance of module theory, obtaining complete results in a number of important special cases. Among these are the cases of skew-symmetric forms over a PID, sesquilinear (Hermitian) forms over the complex numbers, and bilinear and quadratic forms over the real numbers, over finite fields of odd characteristic, and over the field with two elements (where the Arf invariant enters in the case of quadratic forms).

Chapter 7 has two sections. The first discusses semisimple rings and modules (deriving Wedderburn's theorem), and the second develops some multilinear algebra. Our results in both of these sections are crucial for Chapter 8.

Our final chapter, Chapter 8, is the capstone of the book, dealing with group representations mostly, though not entirely, in the semisimple case. Although perhaps not the most usual of topics in a first-year graduate course, it is a beautiful and important part of mathematics. We view a representation of a group G over a field $\mathbf{F}$ as an $\mathbf{F}(G)$-module, and so this chapter applies (or illustrates) much of the material we have developed in this book. Particularly noteworthy is our treatment of induced representations. Many authors define them more or less ad hoc, perhaps mentioning as an aside that they are tensor products. We define them as tensor products and stick to that point of view (though we provide a recognition principle not involving tensor products), so that, for example, Frobenius reciprocity merely becomes a special case of adjoint associativity of Hom and tensor product.

The interdependence of the chapters is as follows:



We should mention that there is one subject we do not treat. We do not discuss any field theory in this book. In fact, in writing this book we were careful to avoid requiring any knowledge of field theory or algebraic number theory as a prerequisite.

We use standard set theoretic notation. For the convenience of the reader, we have provided a very brief introduction to equivalence relations and Zorn's lemma in an appendix. In addition, we provide an index of notation, with a reference given of the first occurrence of the symbol.

We have used a conventional decimal numbering system. Thus a reference to Theorem 4.6.23 refers to item number 23 in Section 6 of Chapter 4, which happens to be a theorem. Within a given chapter, the chapter reference is deleted.

The symbol □ is used to denote the end of a proof; the end of proof symbol □ with a blank line is used to indicate that the proof is immediate from the preceding discussion or result.

The material presented in this book is for the most part quite standard. We have thus not attempted to provide references for most results. The bibliography at the end is a collection of standard works on algebra.

Baton Rouge, Louisiana

William A. Adkins
Steven H. Weintraub

Contents

Chapter 1

Groups

In this chapter we introduce groups and prove some of the basic theorems in group theory. One of these, the structure theorem for finitely generated abelian groups, we do not prove here but instead derive it as a corollary of the more general structure theorem for finitely generated modules over a PID (see Theorem 3.7.22).

1.1 Definitions and Examples

(1.1) Definition. *A* **group** *is a set G together with a binary operation*

$$\cdot : G \times G \to G$$

satisfying the following three conditions:

(*a*) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *for all* $a, b, c \in G$. *(Associativity)*
(*b*) *There exists an element* $e \in G$ *such that* $a \cdot e = e \cdot a = a$ *for all* $a \in G$. *(Existence of an identity element)*
(*c*) *For each* $a \in G$ *there exists a* $b \in G$ *such that* $a \cdot b = b \cdot a = e$. *(Existence of an inverse for each* $a \in G$*)*

It is customary in working with binary operations to write $a \cdot b$ rather than $\cdot(a, b)$. Moreover, when the binary operation defines a group structure on a set G then it is traditional to write the group operation as ab. One exception to this convention occurs when the group G is **abelian**, i.e., if $ab = ba$ for all $a, b \in G$. If the group G is abelian then the group operation is commonly written additively, i.e., one writes $a + b$ rather than ab. This convention is not rigidly followed; for example, one does not suddenly switch to additive notation when dealing with a group that is a subset of a group written multiplicatively. However, when dealing specifically with abelian groups the additive convention is common. Also, when dealing with abelian groups the identity is commonly written $e = 0$, in conformity with

the additive notation. In this chapter, we will write e for the identity of general groups, i.e., those written multiplicatively, but when we study group representation theory in Chapter 8, we will switch to 1 as the identity for multiplicatively written groups.

To present some examples of groups we must give the set G and the operation $\cdot : G \times G \to G$ and then check that this operation satisfies (a), (b), and (c) of Definition 1.1. For most of the following examples, the fact that the operation satisfies (a), (b), and (c) follows from properties of the various number systems with which you should be quite familiar. Thus details of the verification of the axioms are generally left to the reader.

(1.2) Examples.

(1) The set $\mathbf{Z}$ of integers with the operation being ordinary addition of integers is a group with identity $e = 0$, and the inverse of $m \in \mathbf{Z}$ is $-m$. Similarly, we obtain the additive group $\mathbf{Q}$ of rational numbers, $\mathbf{R}$ of real numbers, and $\mathbf{C}$ of complex numbers.

(2) The set $\mathbf{Q}^*$ of nonzero rational numbers with the operation of ordinary multiplication is a group with identity $e = 1$, and the inverse of $a \in \mathbf{Q}^*$ is $1/a$. $\mathbf{Q}^*$ is abelian, but this is one example of an abelian group that is not normally written with additive notation. Similarly, there are the abelian groups $\mathbf{R}^*$ of nonzero real numbers and $\mathbf{C}^*$ of nonzero complex numbers.

(3) The set $\mathbf{Z}_n = \{0, 1, \ldots, n-1\}$ with the operation of addition modulo n is a group with identity 0, and the inverse of $x \in \mathbf{Z}_n$ is $n-x$. Recall that addition modulo n is defined as follows. If $x, y \in \mathbf{Z}_n$, take $x + y \in \mathbf{Z}$ and divide by n to get $x + y = qn + r$ where $0 \leq r < n$. Then define $x + y \pmod{n}$ to be r.

(4) The set U_n of complex n^{th} roots of unity, i.e., $U_n = \{\exp((2k\pi i)/n) : 0 \leq k \leq n-1\}$ with the operation of multiplication of complex numbers is a group with the identity $e = 1 = \exp(0)$, and the inverse of $\exp((2k\pi i)/n)$ is $\exp((2(n-k)\pi i)/n)$.

(5) Let $\mathbf{Z}_n^* = \{m : 1 \leq m < n \text{ and } m \text{ is relatively prime to } n\}$. Under the operation of multiplication modulo n, $\mathbf{Z}_n^*$ is a group with identity 1. Details of the verification are left as an exercise.

(6) If X is a set let S_X be the set of all bijective functions $f : X \to X$. Recall that a function is bijective if it is one-to-one and onto. Functional composition gives a binary operation on S_X and with this operation it becomes a group. S_X is called the group of **permutations** of X or the **symmetric group** on X. If $X = \{1, 2, \ldots, n\}$ then the symmetric group on X is usually denoted S_n and an element α of S_n can be conveniently indicated by a $2 \times n$ matrix

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix}$$

where the entry in the second row under k is the image $\alpha(k)$ of k under the function α. To conform with the conventions of functional composition, the product $\alpha\beta$ will be read from right to left, i.e., first do β and then do α. For example,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}.$$

(7) Let $\mathrm{GL}(n, \mathbf{R})$ denote the set of $n \times n$ invertible matrices with real entries. Then $\mathrm{GL}(n, \mathbf{R})$ is a group under matrix multiplication. Let $\mathrm{SL}(n, \mathbf{R}) = \{T \in \mathrm{GL}(n, \mathbf{R}) : \det T = 1\}$. Then $\mathrm{SL}(n, \mathbf{R})$ is a group under matrix multiplication. (In this example, we are assuming familiarity with basic properties of matrix multiplication and determinants. See Chapter 4 for details.) $\mathrm{GL}(n, \mathbf{R})$ (respectively, $\mathrm{SL}(n, \mathbf{R})$) is known as the **general linear group** (respectively, **special linear group**) of degree n over $\mathbf{R}$.

(8) If X is a set let $\mathcal{P}(X)$ denote the power set of X, i.e., $\mathcal{P}(X)$ is the set of all subsets of X. Define a product on $\mathcal{P}(X)$ by the formula $A \triangle B = (A \setminus B) \cup (B \setminus A)$. $A \triangle B$ is called the symmetric difference of A and B. It is a straightforward exercise to verify the associative law for the symmetric difference. Also note that $A \triangle A = \emptyset$ and $\emptyset \triangle A = A \triangle \emptyset = A$. Thus $\mathcal{P}(X)$ with the symmetric difference operation is a group with $\emptyset$ as identity and every element as its own inverse. Note that $\mathcal{P}(X)$ is an abelian group.

(9) Let $\mathcal{C}(\mathbf{R})$ be the set of continuous real-valued functions defined on $\mathbf{R}$ and let $\mathcal{D}(\mathbf{R})$ be the set of differentiable real-valued functions defined on $\mathbf{R}$. Then $\mathcal{C}(\mathbf{R})$ and $\mathcal{D}(\mathbf{R})$ are groups under the operation of function addition.

One way to explicitly describe a group with only finitely many elements is to give a table listing the multiplications. For example the group $\{1, -1\}$ has the multiplcation table

$\cdot$	1	-1
1	1	-1
-1	-1	1

whereas the following table

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

is the table of a group called the **Klein 4-group**. Note that in these tables each entry of the group appears exactly once in each row and column. Also the multiplication is read from left to right; that is, the entry at the intersection of the row headed by α and the column headed by β is the product $\alpha\beta$. Such a table is called a **Cayley diagram** of the group. They are sometimes useful for an explicit listing of the multiplication in small groups.

The following result collects some elementary properties of a group:

(1.3) Proposition. *Let G be a group.*

(1) *The identity e of G is unique.*
(2) *The inverse b of $a \in G$ is unique. We denote it by a^{-1}.*
(3) $(a^{-1})^{-1} = a$ *for all* $a \in G$ *and* $(ab)^{-1} = b^{-1}a^{-1}$ *for all* $a, b \in G$.
(4) *If* $a, b \in G$ *the equations* $ax = b$ *and* $ya = b$ *each have unique solutions in* G.
(5) *If* $a, b, c \in G$ *then* $ab = ac$ *implies that* $b = c$ *and* $ab = cb$ *implies that* $a = c$.

Proof. (1) Suppose e' is also an identity. Then $e' = e'e = e$.

(2) Suppose $ab = ba = e$ and $ab' = b'a = e$. Then $b = eb = (b'a)b = b'(ab) = b'e = b'$, so inverses are unique.

(3) $a(a^{-1}) = (a^{-1})a = e$, so $(a^{-1})^{-1} = a$. Also $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e$ and similarly $(b^{-1}a^{-1})(ab) = e$. Thus $(ab)^{-1} = b^{-1}a^{-1}$.

(4) $x = a^{-1}b$ solves $ax = b$ and $y = ba^{-1}$ solves $ya = b$, and any solution must be the given one as one sees by multiplication on the left or right by a^{-1}.

(5) If $ab = ac$ then $b = a^{-1}(ab) = a^{-1}(ac) = c$. □

The results in part (5) of Proposition 1.3 are known as the cancellation laws for a group.

The associative law for a group G shows that a product of the elements a, b, c of G can be written unambiguously as abc. Since the multiplication is binary, what this means is that any two ways of multiplying a, b, and c (so that the order of occurrence in the product is the given order) produces the same element of G. With three elements there are only two choices for multiplication, that is, $(ab)c$ and $a(bc)$, and the law of associativity says

that these are the same element of G. If there are n elements of G then the law of associativity combined with induction shows that we can write $a_1a_2\cdots a_n$ unambiguously, i.e., it is not necessary to include parentheses to indicate which sequence of binary multiplications occurred to arrive at an element of G involving all of the a_i. This is the content of the next proposition.

(1.4) Proposition. *Any two ways of multiplying the elements $a_1, a_2, \ldots, a_n$ in a group G in the order given (i.e., removal of all parentheses produces the juxtaposition $a_1a_2\cdots a_n$) produces the same element of G.*

Proof. If $n = 3$ the result is clear from the associative law in G.

Let $n > 3$ and consider two elements g and h obtained as products of $a_1, a_2, \ldots, a_n$ in the given order. Writing g and h in terms of the last multiplications used to obtain them gives

$$g = (a_1 \cdots a_i) \cdot (a_{i+1} \cdots a_n)$$

and

$$h = (a_1 \cdots a_j) \cdot (a_{j+1} \cdots a_n).$$

Since i and j are less than n, the induction hypothesis implies that the products $a_1 \cdots a_i$, $a_{i+1} \cdots a_n$, $a_1 \cdots a_j$, and $a_{j+1} \cdots a_n$ are unambiguously defined elements in G. Without loss of generality we may assume that $i \leq j$. If $i = j$ then $g = h$ and we are done. Thus assume that $i < j$. Then, by the induction hypothesis, parentheses can be rearranged so that

$$g = (a_1 \cdots a_i)((a_{i+1} \cdots a_j)(a_{j+1} \cdots a_n))$$

and

$$h = ((a_1 \cdots a_i)(a_{i+1} \cdots a_j))(a_{j+1} \cdots a_n).$$

Letting $A = (a_1 \cdots a_i)$, $B = (a_{i+1} \cdots a_j)$, and $C = (a_{j+1} \cdots a_n)$ the induction hypothesis implies that A, B, and C are unambiguously defined elements of G. Then

$$g = A(BC) = (AB)C = h$$

and the proposition follows by the principle of induction. □

Since products of n elements of G are unambiguous once the order has been specified, we will write $a_1a_2\cdots a_n$ for such a product, without any specification of parentheses. Note that the only property of a group used in Proposition 1.4 is the associative property. Therefore, Proposition 1.4 is valid for *any* associative binary operation. We will use this fact to be able to write unambiguous multiplications of elements of a ring in later chapters. A convenient notation for $a_1 \cdots a_n$ is $\prod_{i=1}^{n} a_i$. If $a_i = a$ for all i then $\prod_{i=1}^{n} a$ is denoted a^n and called the n^{th} power of a. Negative powers of a are defined