Graduate Texts in Mathematics

144

Noncommutative Algebra

Springer-Verlag

Benson Farb
R. Keith Dennis

Noncommutative Algebra

With 13 Illustrations

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

Benson Farb
Department of Mathematics
Princeton University
Fine Hall, Washington Road
Princeton, NJ 08544
USA

R. Keith Dennis
Department of Mathematics
White Hall
Cornell University
Ithaca, NY 14853
USA

Mathematics Subjects Classifications (1991): 16-01, 13A20, 20Cxx

Library of Congress Cataloging-in-Publication Data
Farb, Benson.
Noncommutative algebra / Benson Farb, R. Keith Dennis.
p. cm. -- (Graduate texts in mathematics ; 144)
Includes bibliographical references and index.
ISBN 0-387-94057-X.
1. Noncommutative algebras. I. Dennis, R.K. (R. Keith), 1944-
II. Title. III. Series
QA251.4.F37 1993
512'.24--dc20 93-17487

Printed on acid-free paper.

Production managed by Jim Harbison; manufacturing supervised by Vincent Scelta.
Photocomposed pages prepared from the authors' LaTeX file.
Printed and bound by R.R. Donnelley & Sons, Harrisonburg, Virginia.
Printed in the United States of America.

9 8 7 6 5 4 3 2 1

ISBN 0-387-94057-X Springer-Verlag New York Berlin Heidelberg
ISBN 3-540-94057-X Springer-Verlag Berlin Heidelberg New York

Preface

About This Book

This book is meant to be used by beginning graduate students. It covers basic material needed by any student of algebra, and is essential to those specializing in ring theory, homological algebra, representation theory and K-theory, among others. It will also be of interest to students of algebraic topology, functional analysis, differential geometry and number theory.

Our approach is more homological than ring-theoretic, as this leads the student more quickly to many important areas of mathematics. This approach is also, we believe, cleaner and easier to understand. However, the more classical, ring-theoretic approach, as well as modern extensions, are also presented via several exercises and sections in Chapter Five. We have tried not to leave any gaps on the paths to proving the main theorems - at most we ask the reader to fill in details for some of the sideline results; indeed this can be a fruitful way of solidifying one's understanding.

The exercises in this book are meant to provide concrete examples to concepts introduced in the text, to introduce related material, and to point the way to further areas of study. Our philosophy is that the best way to learn is to do; accordingly, the reader should try to work most of the exercises (or should at least read through all of the exercises). It should be noted, however, that most of the "standard" material is contained in the text proper. The problems vary in difficulty from routine computation to proofs of well-known theorems. For the more difficult problems, extensive hints are (almost always) provided.

The core of the book (Chapters Zero through Four) contains material which is appropriate for a one semester graduate course, and in fact there should be enough time left to do a few of the selected topics. Another option is to use this book as a starting point for a more specialized course on representation theory, ring theory, or the Brauer group. This book is also suitable for self study.

Chapter Zero covers some of the background material which will be used throughout the book. We cover this material quickly, but provide references which contain further elaboration of the details. This chapter should never actually be read straight through; the reader should perhaps skim it quickly before beginning with the real meat of the book, and refer back to Chapter Zero as needed.

Chapter One covers the basics of semisimple modules and rings, including the Wedderburn Structure Theorem. Many equivalent definitions of semisimplicity are given, so that the reader will have a varied supply of tools and viewpoints with which to study such rings. The chapter ends with a structure theorem for simple artinian rings, and some applications are given, although the most important applications of this material come in the selected topics later in the book, most notably in the representation theory of finite groups. Exercises include a guided tour through the well-known theorem of Maschke concerning semisimplicity of group rings, as well as a section on projective and injective modules and their connection with semisimplicity.

Chapter Two is an exposition of the theory of the Jacobson radical. The philosophy behind the radical is explored, as well as its connection with semisimplicity and other areas of algebra. Here we follow the above style, and provide several equivalent definitions of the Jacobson radical, since one can see a creature more clearly by viewing it from a variety of vantage points. The chapter concludes with a discussion of Nakayama's Lemma and its many applications. Exercises include the concepts of nilpotence and nilradical, local rings, and the radical of a module.

Chapter Three develops the theory of central simple algebras. After a discussion of extension of scalars and semisimplicity (with applications to central simple algebras), the extremely important Skolem-Noether and Double-Centralizer Theorems are proven. The power of these theorems and methods is illustrated by two famous, classical theorems : the Wedderburn Theorem on finite division rings and the Frobenius Theorem on the classification of central division algebras over $\mathbf{R}$. The exercises include many applications of the Skolem-Noether and Double-Centralizer Theorems, as well as a thorough outline of a proof of the well-known Jacobson-Noether Theorem.

Chapter Four is an introduction to the Brauer group. The Brauer group and relative Brauer group are defined and shown to be groups, and as many examples as possible are given. The general study of $Br(k)$ is reduced to that of studying $Br(K/k)$ for galois extensions K/k. This allows a more thorough, concrete study of the Brauer group via factor sets and crossed product algebras. Group cohomology is introduced, and an explicit connection with factor sets is given, culminating in a proof that $Br(K/k)$ is isomorphic to $H^2(Gal(K/k), K^*)$. A complete proof of this extremely important theorem seems to have escaped much of the literature; most authors show only that the above two groups correspond *as sets*. There are exceptions, such as Herstein's classic *Noncommutative Rings*, where an extremely involved computational proof involving idempotents is given. We give a clean, elegant, and easy to understand proof due to Chase. This is the first time this proof appears in an English textbook. The chapter ends with applications of this homological characterization of the Brauer group, including the fact that $Br(K/k)$ is torsion, and a primary decomposition theorem for central division algebras is given.

Chapter Five introduces the notion of primitive ring, generalizing that of simple ring. The theory of primitive rings is developed along lines parallel to that of simple rings, culminating in Jacobson's Density Theorem, which is the analogue for primitive rings of the Structure Theorem for Simple Artinian Rings. Jacobson's Theorem is used to give another proof of the Structure Theorem for Simple Artinian Rings; indeed this is the classical approach to the subject. The Structure Theorem for Primitive Rings is then proved, and several applications of the above theorems are given in the exercises.

Chapter Six provides a quick introduction to the representation theory of finite groups, with a proof of Burnside's famous $p^a q^b$ theorem as the final goal. The connection between representations of a group and the structure of its group ring is discussed, and then the Wedderburn theory is brought to bear. Characters are introduced and their properties are studied. The Orthogonality Relations for characters are proved, as is their consequence that the number of absolutely irreducible representations of a finite group divide the order of the group. A nice criterion of Burnside for when a group is not simple is shown, and finally all of the above ingredients are brought together to produce a proof of Burnside's theorem.

Chapter Seven is an introduction to the global dimension of a ring. We take the elementary point of view set down by Kaplansky, hence we use projective resoultions and prove Schanuel's Lemma in order to define projective dimension of a module. Global dimension of a ring is defined and its basic properties are studied, all with an eye toward computation. The chapter concludes with a proof of the Hilbert Syzygy Theorem, which computes the global dimension of polynomial rings over fields.

Chapter Eight gives an introduction to the Brauer group of a commutative ring. Azumaya algebras are introduced as generalizations of central simple algebras over a field, and an equivalence relation on Azumaya algebras is introduced which generalizes that in the field case. It is shown that endomorphism algebras over faithfully projective modules are Azumaya. The Brauer group of a commutative ring is defined and shown to be an abelian group under the tensor product. $Br()$ is shown to be a functor from the category of commutative rings and ring homomorphisms to the category of abelian groups and group homomorphisms. Several examples and relations between Brauer groups are then discussed.

The book ends with a list of supplementary problems. These problems are divided into small sections which may be thought of as "mini-projects" for the reader. Some of these sections explore further topics which have already been discussed in the text, while others are concerned with related material and applications.

About Other Books

Any introduction to noncommutative algebra would most surely lean heavily on I.N. Herstein's classic *Noncommutative Rings*; we are no exception. Herstein's book has helped train several generations of algebraists, including the older author of this book. The reader may want to look at this book for a more classic, ring-theoretic view of things.

The books *Ring Theory* by Rowen and *Associative Rings* by Pierce cover similar material to ours, but each is more exhautive and at a higher level. Hence these texts would be suitable for reading after completing Chapters One through Four of this book; indeed they take one to the forefront of modern research in Ring Theory.

Other books which would be appropriate to read as either a companion or a continuation of this book are included in the references.

Acknowledgments

Many people have made important contributions to this project. Some parts of this book are based on notes from courses given over the years by Professors K. Brown and R.K. Dennis at Cornell University. Professor D. Webb read the manuscript thoroughly and made numerous useful comments. He worked most of the problems in the book and came up with many new exercises. It is not difficult to see the influence of Brown and Webb on this book - any insightful commentary or particularly clear exposition is most probably due to them. Thanks are also due to Professor G. Bergman, B. Grosso, Professor S. Hermiller, Professor T.Y. Lam and Professor R. Laubenbacher, all of whom read the various parts of the manuscript and made many useful comments and corrections. Thanks to Paul Brown for doing most of the diagrams, and to Professor John Stallings for his computer support. We would also like to thank Professors M. Stillman and S. Sen for using this book as part of their graduate algebra courses at Cornell, and we thank their students for comments and corrections. Several exercises, as well as the clever and enlightening new proof that $Br(K/k)$ is isomorphic to $H^2(G, K^*)$, are due to Professor S. Chase, to whom we wish to express our gratitude.

Benson Farb was supported by a National Science Foundation Graduate Fellowship during the time this work took place. R.Keith Dennis would like to thank S. Gersten, who first taught him algebra, and Benson Farb would like to thank R.Keith Dennis, who first taught him algebra. A special thanks goes from B. Farb to Craig Merow, who first showed him the beauty of mathematics, and pointed out the fact that it is possible to spend one's life thinking about such things. Finally, B. Farb would like to thank R.Keith Dennis for his positive reaction to the idea of this project, and especially for the kindness and hospitality he has shown him over the last few years.

A Word About Conventions

On occasion we will use the words "category" and "functorial", as they are the proper words to use. We do not, however, formally define these terms in this book, and the reader who doesn't know the definitions may look them up or continue reading without any loss.

When making references to other papers or books, we will write out the full name of the text instead of making a reference to the bibliography at the back of the book. We do this so that the reader may know which book we are refering to without having to look it up in the back. In addition, the complete information on each reference is contained in the bibliography.

Contents

0

Background Material

This chapter contains some of the background material that will be used throughout this book. The goal of this chapter is to fill in certain small gaps for the reader who already has some familiarity with this background material. This should also indicate how much we assume the reader already knows, and should serve to fix some notation and conventions. Accordingly, explanations will be kept to a minimum; the reader may consult the references given at the end of the book for a thorough introduction to the material. This chapter also contains several exercises, for use both by instructors and readers wishing to make sure they understand the basics. The reader may want to begin by glancing casually through this chapter, leaving a thorough reading of a section for when it is needed.

Rings: Some Basics

We begin with a rapid review of the definitions and basic properties of rings.

A ring R is a set with two binary operations, called addition and multiplication, such that

(1) R is an abelian group under addition.

(2) Multiplication is associative; i.e., $(xy)z = x(yz)$ for all $x, y, z \in R$.

(3) There exists an element $1 \in R$ with $1x = x1 = x$ for all $x \in R$.

(4) The distributive laws hold in $R : x(y + z) = xy + xz$ and $(y + z)x = yx + zx$ for all $x, y, z \in R$.

The element $1 \in R$ is called the **identity**, or **unit element** of the ring R. We will always denote the unit element for addition by 0, and the unit element for multiplication by 1. R is a **commutative ring** if $xy = yx$ for all $x, y \in R$. We shall *not* assume that our rings are commutative unless otherwise specified.

Examples:

1. **Z**, the integers, with the usual addition and multiplication, with 0 and 1 as additive and multiplicative unit elements.

2. $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$; the rational numbers, real numbers, and complex numbers, respectively, with operations as in Example 1.

3. The ring $\mathbf{Z}/n\mathbf{Z}$ of integers $\bmod n$, under addition and multiplication $\bmod n$.

4. $R[x]$, the ring of polynomials with coefficients in a ring R, is a ring under addition and multiplication of polynomials, with the polynomials 0 and 1 acting as additive and multiplicative unit elements, respectively.

5. The ring $\mathcal{M}_n(R)$ of $n \times n$ matrices with entries in a ring R , under addition and multiplication of matrices, and with the $n \times n$ identity matrix as identity element.

6. The ring $End(M)$ of endomorphisms of an abelian group M, under addition and composition of endomorphisms (recall that an endomorphism of M is a homomorphism from M to itself).

7. The ring of continuous real-valued functions on an interval $[a, b]$, under addition and multiplication of functions.

The rings in examples 1,2,3, and 7 are commutative; the rings in examples 4,5 and 6 are generally not ($R[x]$ is commutative if and only if R is commutative). We shall encounter many more examples of rings, many of which will not be commutative.

A **ring homomorphism** is a mapping f from a ring R to a ring S such that

(1) $f(x+y) = f(x) + f(y)$; i.e., f is a homomorphism of abelian groups.

(2) $f(xy) = f(x)f(y)$.

(3) $f(1) = 1$.

In short, f preserves addition, multiplication, and the identity element. For those more familiar with groups than with rings, note that (3) does not follow from (1) and (2). For example, the homomorphism $f : \mathbf{R} \to \mathbf{R} \times \mathbf{R}$ given by $f(x) = (x, 0)$ satisfies (1) and (2), but not (3).

The composition of ring homomorphisms is again a ring homomorphism. An **endomorphism** of a ring is a (ring) homomorphism of the ring into itself. An **isomorphism** of rings is a ring homomorphism $f : R \longrightarrow S$ which is one-to-one and onto; in this case, R and S are said to be **isomorphic** as rings. If $f : R \longrightarrow S$ and $g : S \longrightarrow R$ are ring homomorphisms such that $f \circ g$ and $g \circ f$ are the identity homomorphisms of S and R, respectively, then both f and g are ring isomorphisms.

A subset S of a ring R is called a **subring** if S is closed under addition and multiplication and contains the same identity element as R. A subset

I of a ring R is called a **left ideal** of R if I is a subgroup of the additive group of R and if $ri \in I$ for all $r \in R, i \in I$; the notions of right ideal and two-sided ideal are similarly defined. We shall always assume, unless otherwise specified, that all ideals are left ideals. An ideal I is said to be a **maximal ideal** of the ring R if $I \neq R$ and if $I \subseteq J \subseteq R$ for some ideal J, then $J = I$ or $J = R$.

For a two-sided I, the quotient group R/I inherits a natural ring structure given by $(r+I)(s+I) = rs + I$. This ring is called the **quotient ring** of R by I. Note that there is a one-to-one, order-preserving correspondence between ideals of R/I and ideals of R containing I.

A **zero-divisor** in a ring R is an element $r \in R$ for which $rs = 0$ for some $s \neq 0$. An element $r \in R$ is called a **unit** of R, and is said to be **invertible**, if $rs = sr = 1$ for some $s \in R$. Note that the set of invertible elements of a ring R forms a group under multiplication, called the **group of units** of R. A ring such that $1 \neq 0$, and such that every nonzero element is invertible, is called a **division ring**. A commutative division ring is called a **field**.

Let F be a field and let n be the smallest integer for which $1 + \cdots + 1 = n \cdot 1 = 0$. We call n the **characteristic** of F, denoted $char(F)$, and we let $char(F) = 0$ if no such (finite) n exists. It is easy to show that the characteristic of any field is either 0 or prime. For example, $\mathbf{Q}$, $\mathbf{R}$ and $\mathbf{C}$ are fields of characteristic 0. $\mathbf{F}_q$, the field with $q = p^n$ (p prime) elements, is a field of characteristic p.

Modules: Some Basics

Let R be a ring. A **left R-module** is an abelian group M, written additively, on which R acts linearly; that is, there is a map $R \times M \longrightarrow M$, denoted by $(r, m) \longmapsto rm$ for $r \in R, m \in M$, for which

(1) $(r+s)m = rm + sm$

(2) $r(m+n) = rm + rn$

(3) $(rs)m = r(sm)$

(4) $1m = m$

for $r, s \in R$ and $m, n \in M$. Equivalently, M is an abelian group together with a ring homomorphism $\rho : R \longrightarrow End(M)$, where $End(M)$ denotes the ring of group endomorphisms of an abelian group (for those unfamiliar with this notion, see page 13). ρ is called the **structure map**, or a **representation** of the ring R. There is a corresponding notion of right module, but, unless otherwise specified, we shall assume all modules are left modules.

Examples:

1. An ideal I of a ring R is an R-module. In particular, R is an R-module.

2. Any vector space over a field k is a k-module. A module over a division ring D is sometimes called a vector space over D.

3. Any abelian group is a $\mathbf{Z}$-module.

4. The cartesian product $R^n = R \times \cdots \times R$ is an R-module in the obvious way. R^n is called the **free module of rank n**.

5. The set of $n \times n$ matrices $\mathcal{M}_n(R)$ over a ring R is an R-module under addition of matrices. The action of R on $\mathcal{M}_n(R)$ is defined, for $r \in R, B \in \mathcal{M}_n(R)$, to be $r \longmapsto rB$, where rB denotes the matrix whose i, jth entry is r times the i, jth entry of B.

Let M and N be R-modules. A mapping $f : M \longrightarrow N$ is an **R-module homomorphism** if :

(1) $f(m+n) = f(m) + f(n)$
(2) $f(rm) = rf(m)$

for all $m, n \in M, r \in R$. In this case f is also called **R-linear**. Note that the composition of two module homomorphisms is again a module homomorphism. A **(module) endomorphism** is a homomorphism of a module to itself. A module homomorphism $f : M \longrightarrow N$ which is one-to one and onto is called a **(module) isomorphism**, in which case M and N are said to be isomorphic modules.

A subset N of a module M is called a **submodule** of M, if N is an (additive) subgroup of M and if $rn \in N$ for all $r \in R, n \in N$. Thus, the R-submodules of R are precisely the (left) ideals of R. If $f : M \longrightarrow N$ is a homomorphism of R-modules, let

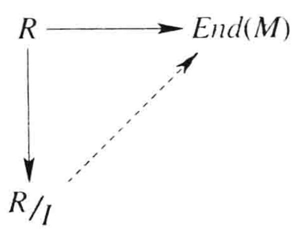
$$\begin{aligned} ker(f) &= \{m \in M : f(m) = 0\} \\ im(f) &= f(M) \end{aligned}$$

be the kernel and the image of f. It is easy to check that $ker(f)$ is a submodule of M and $im(f)$ is a submodule of N. In particular, for fixed $m \in M$, the kernel of the R-module homomorphism $\phi : R \longrightarrow M$ given by $\phi(r) = rm$, is a submodule (i.e., left ideal) of R. More explicitly, this kernel is $\{r \in R : rm = 0\}$. This ideal of R is called the **annihilator** of m, and is denoted by $ann(m)$. The intersection of the annihilators of each of the elements of M is called the **annihilator of** M, and is denoted $ann(M)$; that is

$$ann(M) = \bigcap_{m \in M} ann(m)$$

An R-module M is called **faithful** if $ann(M) = 0$. In this case the associated representation ρ is also called a **faithful representation** of R.

The abelian group M/N inherits a natural R-module structure via $r(m+N) = rm + N$. This R-module is called the **quotient module** of M by N. Note that there is a one-to-one, order preserving correspondence between submodules of M/N and submodules of M containing N. This is sometimes referred to as the Correspondence Theorem for Modules. If I is a two-sided ideal of a ring R, and if M is an R/I-module, then M is also an R-module via $R \longrightarrow R/I \longrightarrow End(M)$. Further, given an R-module M which is annihilated by I (i.e., $I \subseteq ann(m)$ for all $m \in M$), there is a unique R/I-module structure on M giving rise to the original structure on M :



Thus, there is a one-to-one correspondence between R/I-modules and R-modules annihilated by I.

We shall now discuss certain operations on rings and modules which will be useful later in the text. If M is an R-module and $N \subseteq M, I \subseteq R$ are additive subgroups, then IN is defined to be the additive subgroup generated by $\{rn : r \in I, n \in N\}$; that is, $IN = \{\sum_{i=1}^{m} r_i n_i : m \in \mathbf{N}, r_i \in I, n_i \in N\}$. Note that if N is a submodule of M, then $IN \subseteq N$, and if I is a left ideal of R, then IN is a submodule. In particular, if $M = R$, then IN is a product of ideals. The following formulas hold for $I, I_1, I_2 \subseteq R$ and $N, N_1, N_2 \subseteq M$:

$$\text{Associative Law :} \quad I_1(I_2N) = (I_1I_2)N$$

Both sides are the additive subgroup generated by products r_1r_2n.

$$\text{Distributive Laws :} \quad \begin{aligned} (I_1 + I_2)N &= I_1N + I_2N \\ I(N_1 + N_2) &= IN_1 + IN_2 \end{aligned}$$

If M is an R-module and $m \in M$, then Rm is a submodule of M and is said to be the **cyclic submodule** of M generated by m.

Zorn's Lemma

Zorn's Lemma is used frequently in ring theory. Here we include one typical application.

A **partially ordered set** is a set S, together with a relation $\leq$, which satisifies

$a \leq a$	(reflexive)
$a \leq b$ and $b \leq c$ implies $a \leq c$	(transitive)
$a \leq b$ and $b \leq a$ implies $a = b$	(anti-symmetric)

for all $a, b, c \in S$. A subset $T \subseteq S$ is called a **chain** if either $a \leq b$ or $b \leq a$ for all $a, b \in T$. An **upper bound** for a chain T in S is an element $c \in S$ such that $a \leq c$ for all $a \in T$. An element $c \in S$ is called a **maximal element** of S if $a \in S$ and $c \leq a$ implies $c = a$. We now state

Lemma 0.1 (Zorn's Lemma) *Let S be a partially ordered set. If every chain T of S has an upper bound in S, then S has at least one maximal element.*

Zorn's Lemma is logically equivalent both to the Axiom of Choice and to the Well-ordering Principle. For proofs of these equivalences, see Halmos, *Naive Set Theory*. For those who worry about using the Axiom of Choice (and thus Zorn's Lemma), we shall always point out where Zorn's Lemma is used.

We conclude this section with a typical application of Zorn's Lemma.

Proposition 0.2 *Let $R \neq 0$ be a ring (with 1). Then R has a maximal left ideal.*

Proof: Let $\mathcal{S}$ be the set of proper (i.e., $\neq R$) left ideals of R, partially ordered by inclusion. If $\{I_\alpha\}$ is a chain of ideals in R, then for all α and β, either $I_\alpha \subseteq I_\beta$ or $I_\beta \subseteq I_\alpha$. It is now easy to check that $I = \bigcup_\alpha I_\alpha$ is an ideal of R, and that $1 \notin I$ since $1 \notin I_\alpha$ for any α. Thus $I \in \mathcal{S}$ and I is an upper bound for the chain. Hence $\mathcal{S}$ contains a maximal element. □

Products

Let R_1 and R_2 be rings. Then the cartesian product $R_1 \times R_2 = \{(r_1, r_2) : r_1 \in R_1, r_2 \in R_2\}$ is a ring if addition and multiplication are taken coordinatewise. The ring $R_1 \times R_2$ is called the **product** of the rings R_1 and R_2. There are natural ring homomorphisms $p_i : R_1 \times R_2 \longrightarrow R_i$ given by projection onto the ith coordinate, $i = 1, 2$. There is also a one-to-one map