Linear Algebra Over Commutative Rings

Bernard R. McDonald

Linear Algebra Over Commutative Rings

Bernard R. McDonald
Division of Mathematical Sciences
National Science Foundation
Washington, D.C.

MARCEL DEKKER, INC. New York and Basel

LIBRARY OF CONGRESS CATALOGING IN PUBLICATION DATA

McDonald, Bernard R.
Linear algebra over commutative rings.

(Pure and applied mathematics ; 87)
Bibliography: p.
Includes index.
1. Commutative rings. 2. Algebras, Linear.
I. Title. II. Series: Monographs and textbooks in pure and applied mathematics ; v. 87.
QA251.3.M373 1984 512'.4 84-19935
ISBN 0-8247-7122-2

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Current printing (last digit):
10 9 8 7 6 5 4 3 2 1

PRINTED IN THE UNITED STATES OF AMERICA

Preface

This monograph arose from lectures at the University of Oklahoma on topics related to linear algebra over commutative rings. Our desire was to provide both an introduction and a survey of matrix theory over commutative rings. Many results and folklore in this subject are known to experts; however, these results are not easily discovered by the beginner or a scholar with only a temporary curiosity.

The scalars in the matrices under consideration are generally assumed to be from a commutative ring. Noncommutative scalar rings are treated only when no additional theory is needed to handle that setting. It was also hoped that this manuscript might serve as an introduction to algebraic K-theory and might serve as a starting point, for example, to the works of H. Bass.

The contents of the manuscript are arranged in a traditional format. The first chapter is devoted to matrix theory over a commutative ring. Chapter II summarizes standard results on free modules. In Chapter III, we examine the endomorphism rings of finitely generated free and projective modules, and, in Chapter IV, the structure theory of a projective module. In Chapter V the theory of a single endomorphism is discussed. The aims of each chapter are described in more detail below.

Chapter I summarizes the folklore and theory of matrix calculations over commutative rings. As in all of the chapters, there are extensive exercise sets. Some exercises are trivial or calculational; others are selected from various research papers and either examine the theory for particular choices of commutative rings or summarize additional useful information. Polynomial theory over a commutative ring plays a significant role in matrix theory and linear algebra. Thus, this topic is also discussed in Chapter I. Topics in Chapter I include the following: determinantal identities and ideals; discussion of similarity; discussion of the general linear group, its normal subgroups, its automorphisms, generators, and its stable limit; a survey of the solution of linear equations over a commutative ring and the related ideas of matrix rank.

In Chapter II we discuss the theory of a free module of finite dimension over a commutative ring. These topics are of interest in their own right and serve to provide the theory of projective modules under localization. Among other topics this chapter examines the following: the Fundamental Theorem of Projective Geometry and the projective plane—the introductory theory of projective modules and the theory of equivalence transformations—Fitting's theorem, and Fitting equivalence.

Chapter III describes the endomorphism ring of a finitely generated free and projective module. We begin with an analysis of a free module and its endomorphism ring of matrices and examine the relationships between the module theory over the scalar commutative ring and the module theory over the matrix ring. In the next section, using the "free" theory as motivation, we develop the standard duality theory of a finitely generated projective module discussing generators, projectives, and Morita theory. In Section D the Three-Cornered Galois Theory of Baer is described for a projective module. The concluding sections of this chapter describe the radical and automorphisms of an endomorphism ring of a finitely generated projective module. The appendix to this chapter discusses invertible submodules of matrix rings and the theory of equivalence.

Chapter IV concerns the theory of localization, finitely generated modules, Fitting ideals, and the structure theory of a finitely generated projective module. Included in this chapter is a proof of Serre's theorem using the matrix approach of Suslin and results on stably free projective modules.

The final chapter, Chapter V, is a study of the theory of a single endomorphism of both a free and a projective module. For a projective module this includes a discussion of the trace, determinant, characteristic polynomial, determinant-trace polynomial, and comments on similarity. This chapter also contains an introduction to the K-theory of projective modules and the K-theory of their endomorphism rings. The chapter concludes with (1) an elegant theorem of Bass relating the exterior and symmetric algebras and (2) a discussion of the Koszul complex.

As noted above, this monograph arose from lectures given at the University of Oklahoma over several years on topics related to the linear algebra of commutative rings. The writing of the monograph began during the summer of 1979 while I was a guest of the Department of Mathematics of Queen's University at Kingston, Ontario. I am very appreciative to Anthony Geramita for inviting me to Queen's and for arranging a comfortable and peaceful setting to begin this work. The bulk of the manuscript was written in 1980-81 while I was a participant in the "Year of Algebra" sponsored by the Department of Mathematics of the University of California, Santa Barbara. Julius Zelmanowitz was instrumental in arranging both this special year in algebra and my visit, and I am deeply indebted to him. While at Santa Barbara I enjoyed many enlightening conversations with Edward Formanek. The initial version of the manuscript was typed by Ms. Trish Abolins at the University of Oklahoma. The final version was edited and prepared by the editorial staff of Marcel Dekker, Inc. Chuck Weibel, Robert Guralnick, Alex Hahn, Bill Waterhouse, and Andy Magid offered advice, results, and suggestions that were incorporated into the text and much appreciated. Oklahoma graduate students Mike Svec, Jeanna Moore, and Bessie Kirkwood helped with the reading and the proofing of the manuscript. To all of the above I owe thanks .

Despite repeated proofing, I am certain that errors remain in this manuscript. For these errors I apologize, with the hope that they are minor, and I ask that the reader inform me both of discovered errors, results that should have been included, and recent research results.*

Bernard R. McDonald

*National Science Foundation Disclaimer . . . "Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author and do not necessarily reflect the views of the National Science Foundation."

Contents

Chapter I
Matrix Theory Over Commutative Rings

A. THE POLYNOMIAL RING

The purpose of this chapter is to summarize many of the basic results in the theory of matrices over a commutative ring. The linear theory of a projective module over a commutative ring, via localization arguments, is often reduced to the theory of a free module and ultimately to matrix calculations. Some of these calculations are folklore, some are easy extensions of analogous calculations over a field, some have been scattered through the literature, and some [e.g., Suslin's results on the normality of $E_n(R)$ in $GL_n(R)$] are recent and nontrivial. This chapter also serves to introduce some of the notation we will employ throughout the monograph.

Since matrix theory and linear algebra are intimately associated with polynomial theory, this section assembles the elementary polynomial theory we will need. Most texts on commutative algebra or introductory graduate algebra provide good introductions to the theory of the polynomial ring over a commutative ring. We also recommend the survey article by Robert Gilmer [G29].

Let R be a commutative ring and X be an indeterminate over R. The polynomial ring R[X] and the ring of formal power series R[[X]] are fundamental to the study of commutative rings. The importance of polynomials is based on the *substitution morphism:*

Suppose that σ: $R \to S$ is a ring morphism and $\sigma(r)\lambda = \lambda\sigma(r)$ for some fixed λ in S and all r in R. Then there is a unique ring morphism

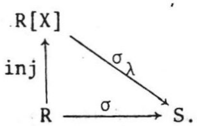
$$\sigma_\lambda: \ R[X] \to S$$

such that

(a) $\sigma_\lambda(r) = \sigma(r)$ for all r in R.

(b) $\sigma_\lambda(X) = \lambda$.

Precisely, σ_λ: $R[X] \to S$ is given by $\sigma_\lambda(\Sigma\, a_i X^i) = \Sigma\, \sigma(a_i)\lambda^i$ and makes the following diagram commutative:



Further, the substitution morphism characterizes R[X] up to ring isomorphism.

We now examine several cases of the substitution morphism. First, suppose that S = R and σ = identity. Then, if $f = \Sigma\, a_i X^i$, $\sigma_\lambda(f)$ is denoted by $f(\lambda)$. The kernel of σ_λ, $\ker(\sigma_\lambda)$, is an ideal in R[X] called the ***ideal of relations*** satisfied by λ. In order to examine elements in the ideal of relations of λ, recall that if f in R[X] is a monic polynomial (indeed, the leading coefficient need only be a unit) and g is in R[X], then (*division algorithm*) there exist unique q and r in R[X] with $g = qf + r$ where $r = 0$ or $\deg(r) < \deg(f)$.

It is easily seen that the division algorithm and the substitution morphism are related by (*Remainder Theorem*)

$$g = (X - \lambda)q + r$$

where $r = \sigma_\lambda(g) = g(\lambda)$. This gives immediately the *Factor Theorem*; i.e., the following are equivalent:

(a) g is in the ideal of relations satisfied by λ; i.e., $g(\lambda) = 0$.

(b) $g = (X - \lambda)q$ for some q in $R[X]$; i.e., $X - \lambda$ is a factor of g.

As a second application of the substitution morphism, let σ: $R \to T$ be a ring morphism, let $S = T[X]$, and let $\lambda = X$. Then

$$\sigma_X(\Sigma\ a_i X^i) = \Sigma\ \sigma(a_i) X^i$$

(we are employing the same notation for both indeterminates). If $A = \ker(\sigma)$ in the second application, then clearly

$$\ker(\sigma_X) = A[X] = \{\Sigma\ a_i X^i \mid a_i \text{ in } A\}.$$

Hence, if σ is surjective, $T \simeq R/A$, σ_X is surjective, and $R[X]/\ker(\sigma_X) = R[X]/A[X]$ is isomorphic to $(R/A)[X]$.

Several facts follow from the second case:

(a) σ is injective (surjective) if and only if σ_X is injective (surjective).

(b) A is a prime ideal in R if and only if $A[X]$ is a prime ideal in $R[X]$.

(c) If m is a maximal ideal in R, then $m[X]$ is a prime (but *not* maximal) ideal in $R[X]$ and each prime ideal P of $R[X]$ which contains $m[X]$ properly is a maximal ideal.

I.A.1 EXERCISE. Let σ: $R \to S$ be a ring morphism of commutative rings. Show that σ induces a ring morphism σ_X on the formal power series rings, σ_X: $R[[X]] \to S[[X]]$ by $\sigma_X(\Sigma_0^\infty\ a_i X^i) = \Sigma_0^\infty\ \sigma(a_i) X^i$. If $A = \ker(\sigma)$, show that the kernel of σ_X

$$\ker(\sigma_X) = \{\Sigma\ a_i X^i \mid a_i \text{ in } A\}$$
$$= A[[X]].$$

Thus $R[[X]]/A[[X]] \simeq (R/A)[[X]]$. Show that

(a) σ is injective (surjective) if and only if σ_X is injective (surjective).

(b) $A[[X]]$ is a prime ideal in $R[[X]]$ if and only if A is a prime ideal in R.

(c) If m is maximal in R, then $m[[X]] + (X)$ is the unique maximal ideal of $R[[X]]$ containing $m[[X]]$. [*Hint*: $(R/m)[[X]]$ is a local ring with maximal ideal (X).]

I.A.2 EXERCISE. Let $f = a_0 + a_1X + \cdots + a_nX^n$ be in $R[X]$ and $g = b_0 + b_1X + \cdots + b_nX^n + \cdots$ be in $R[[X]]$.

(a) Show that g is a unit in $R[[X]]$ if and only if b_0 is a unit in R. Show that f is a unit in $R[X]$ if and only if a_0 is a unit in R and $a_1, \ldots, a_n$ are nilpotent. (*Hint*: Unit + nilpotent = unit.)

(b) Show that f is a zero divisor in $R[X]$ if and only if there is an $r \neq 0$ in R with $rf = 0$. See Gilmer [G29] for a discussion of the analogue for g in $R[[X]]$; e.g., if R is Noetherian, the analogous statement is valid.

(c) Show that f is nilpotent in $R[X]$ if and only if $a_0, a_1, \ldots, a_n$ are nilpotent. Show that if g is nilpotent in $R[[X]]$, then b_i is nilpotent for each i (the converse is true if R is Noetherian—see Gilmer [G29]).

(d) Let A be an ideal in R. Let f and g be in $R[X]$ with $g = b_0 + b_1X + \cdots + b_mX^m$. Suppose that fg is in $A[X]$ but g is not in $A[X]$. Show that there is an r in $(b_0, b_1, \ldots, b_m)$, but not in A, with rf in $A[X]$. Deduce (b) (for $R[X]$) from this exercise.

I.A.3 EXERCISE (Continued). If S is a commutative ring, let S* denote the group of units of S. Let σ_0: $R[X] \to R$ (resp., $R[[X]] \to R$) denote the "constant term" morphism, i.e., substitution by 0. Then σ_0 induces a surjective group morphism σ_0: $R[X]^* \to R^*$ (resp., $R[[X]]^* \to R^*$) by Exercise I.A.2.

(a) Let $U_1 = \ker \sigma_0$, σ_0: $R[X]^* \to R^*$. Then f is in U_1, i.e., $\sigma_0(f) = f(0) = 1$, if and only if $f = 1 + a_1X + \cdots + a_nX^n$ where $a_1, \ldots, a_n$ are nilpotent. The set of nilpotent polynomials in $R[X]$ forms the prime radical* (from

*We denote the prime or nil radical of a commutative ring S by rad(S) and the Jacobson radical by Rad(S)—see Exercise I.A.4.

Exercise I.A.4, $rad(R[X]) = Rad(R[X])$, which we denote by $rad(R[X])$. Let $N = rad(R)$. Then $rad(R[X]) = N[X]$ and f is in U_1 if and only if f is in $1 + XN[X]$. Thus $U_1 = 1 + XN[X]$ and we have an exact sequence

$$1 \to 1 + XN[X] \to R[X]^* \xrightarrow{\sigma_0} R^* \to 1$$

which splits under the natural injection $R \to R[X]$.

(b) Let $\bar{U}_1 = \ker(\sigma_0)$, σ_0: $R[[X]]^* \to R^*$. Show that if g is in $R[[X]]$, then $1 + Xg$ is invertible (see Exercise I.A.2). Thus $\bar{U}_1 = 1 + XR[[X]] = 1 + (X)$ and

$$1 \to 1 + (X) \to R[[X]]^* \xrightarrow{\sigma_0} R^* \to 1$$

is split exact with splitting morphism induced from the injection $R \to R[[X]]$. Hence from (a),

$$R[X]^* \simeq R^* \times [1 + XN[[X]]$$

and

$$R[[X]]^* \simeq R^* \times [1 + (X)].$$

I.A.4 EXERCISE. Exercise I.A.3 introduced the nil and Jacobson radicals. Recall that if R is a commutative ring, then the prime or nil radical, denoted rad(R), is the intersection of all prime ideals of R; equivalently, rad(R) is the ideal of all nilpotent elements in R. The Jacobson radical of R, Rad(R), is the intersection of all maximal ideals of R; equivalently, the ideal of all x in R such that $1 - xy$ is a unit in R for all y in R. Show that

(a) $rad(R[X]) = Rad(R[X]) = (rad(R))[X]$.

(b) $f = \Sigma_{i=0}^{\infty} b_i X^i$ in $R[[X]]$ is in $Rad(R[[X]])$ if and only if b_0 is in Rad(R).

If R is Noetherian, then (see, e.g., Gilmer [G29]) $rad(R[[X]]) = (rad(R))[[X]]$.

I.A.5 EXERCISE. The previous exercises introduced Noetherian rings. Recall that a commutative ring R is said to be *Noetherian* if every ideal of R is finitely generated.

(a) Show that the following are equivalent for a commutative ring R:

 (1) Every ideal of R is finitely generated.

 (2) Every ascending chain of ideals $A_1 \subseteq A_2 \subseteq \cdots$ of R has only a finite number of distinct terms.

(b) (Hilbert basis theorem) Show that if R is Noetherian, then R[X] is Noetherian. (Similarly for $R[X_1,\ldots,X_n]$.)

(c) Show that if R is Noetherian, then R[[X]] is Noetherian. (Similarly for $R[[X_1,\ldots,X_n]]$.)

(d) Suppose that R is a Noetherian ring and σ: $R \to S$ is a surjective ring morphism. Show that S is Noetherian. Hence if A is an ideal of R[X] (resp., R[[X]]) and R is Noetherian, then R[X]/A (resp., R[[X]]/A) is Noetherian.

(e) If R is a Noetherian ring and M is a finitely generated R-module, show that every submodule of M is finitely generated.

(f) Let R be a commutative ring and $a_1, \ldots, a_n$ be a finite set in R. Let $Z[a_1,\ldots,a_n]$ denote the subring generated by $a_1, \ldots, a_n$ in R. Show that $Z[a_1,\ldots,a_n]$ is Noetherian.

I.A.6 EXERCISE

(a) Let k be a field and f a polynomial in k[X] of degree $n \geq 0$. Show that f has at most n roots in k.

(b) Suppose that k is infinite and S is an infinite subset of k. Let f be in k[X]. Show that f(a) = 0 for all a in S implies that $f \equiv 0$; i.e., f is the zero function.

(c) Suppose that k is an infinite field and $T_1, \ldots, T_n$ are infinite subsets of k. Let f be in $k[X_1,\ldots,X_n]$. Show that if $f(t_1,\ldots,t_n) = 0$ for all t_i in T_i, $1 \leq i \leq n$, then $f \equiv 0$.

(d) Let R be an infinite domain. Let f be a polynomial in $R[X_1,\ldots,X_n]$. Suppose that $f(\alpha_1,\ldots,\alpha_n) = 0$ for all sets of values $\{\alpha_1,\ldots,\alpha_n\}$ satisfying some finite number of algebraic relations.

$$g(\alpha_1,\ldots,\alpha_n) \neq 0, \quad h(\alpha_1,\ldots,\alpha_n) \neq 0, \quad \ldots .$$

Show that $f \equiv 0$. This has been called the "principle of irrelevance of algebraic inequalities" by H. Weyl ([W32], p. 4). See the discussion following Corollary I.6.

B. ELEMENTARY IDEAS

Throughout this chapter R will denote a commutative ring with identity 1. Let I and J be index sets of finite cardinality. Suppose that

$$I = \{1,2,3,\ldots,m\},$$
$$J = \{1,2,3,\ldots,n\}.$$

An $m \times n$ *matrix over* R is a map

$$\sigma\colon \quad I \times J \to R.$$

The map $\sigma\colon I \times J \to R$ is usually identified with its range of values in R arranged in the following tabular form:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{bmatrix} = [a_{ij}]$$

where $a_{ij} = \sigma(i,j)$. The element a_{ij} in the table of values above is said to have *row index* i and *column index* j and is said to *occupy the* (i,j)*-position* or be the (i,j)-th *entry* of the matrix.

Two maps $\sigma\colon \; I \times J \to R$ and $\beta\colon \; I \times J \to R$ are *equal*, $\sigma = \beta$, if $\sigma(i,j) = \beta(i,j)$ for all (i,j) in $I \times J$. Equivalently, if σ has array $[a_{ij}]$ where $\sigma(i,j) = a_{ij}$ and β has array $[b_{ij}]$ where $\beta(i,j) = b_{ij}$, then $[a_{ij}] = [b_{ij}]$ if $a_{ij} = b_{ij}$ for all (i,j) in $I \times J$.

We now suppress reference to maps $\sigma\colon \; I \times J \to R$ and use the tabular form to denote matrices. The set of all matrices over R of size $m \times n$ is denoted $(R)_{m,n}$. If $m = n$, then $(R)_{m,n}$ is abbreviated to $(R)_n$. A matrix in $(R)_{m,1}$ is called a *column* of *size, dimension*, or *length* m. A matrix in $(R)_{1,n}$ is called a *row* of *size*, etc., n.

Our first purpose is to give $(R)_{m,n}$ and $(R)_n$ algebraic operations and, consequently, an algebraic structure. The first operation, addition, is natural and is induced by both the addition in R and the standard fashion by which maps are added. If $[a_{ij}]$ and $[b_{ij}]$ are in R, then define *addition* by

$$[a_{ij}] + [b_{ij}] = [c_{ij}]$$

where $c_{ij} = a_{ij} + b_{ij}$ for each (i,j) in $I \times J$.

Clearly, $(R)_{m,n}$ under + is an Abelian group with identity $0 = [0]$ (0 in every position) where the additive inverse of $[a_{ij}]$ is $-[a_{ij}] = [-a_{ij}]$. Let r be in R. Define the *scalar product* (or *scalar multiplication*) of r and $[a_{ij}]$ by

$$r[a_{ij}] = [ra_{ij}].$$

Then $(R)_{m,n}$ under addition and scalar multiplication is an R-module.

The next operation is a product of matrices. It does not arise naturally from the consideration of maps $\sigma\colon\ I \times J \to R$. Instead, it is derived from the composition of linear maps between free modules (in Chapter II).

Let $[a_{ij}]$ be in $(R)_{m,n}$ and $[b_{jk}]$ be in $(R)_{n,p}$. Define the *product* of $[a_{ij}]$ and $[b_{jk}]$ by

$$[a_{ij}][b_{jk}] = [c_{ik}]$$

where

$$c_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk}.$$

The product above is a "convolution product." Both the richness of the theory of matrices and their inherent difficulties and mystery are an outcome of this product. It is easy to see that the product gives a map

$$(R)_{m,n} \times (R)_{n,p} \to (R)_{m,p}$$

which is R-bilinear; i.e.,