Paul A. Fuhrmann

A POLYNOMIAL APPROACH TO LINEAR ALGEBRA

Springer

Paul A. Fuhrmann

A Polynomial Approach to Linear Algebra

Springer

Paul A. Fuhrmann
Department of Mathematics
Ben-Gurion University of the Negev
Beer Sheva
Israel

Editorial Board
(North America):

S. Axler
Department of
Mathematics
Michigan State University
East Lansing, MI 48824
USA

F.W. Gehring
Department of
Mathematics
University of Michigan
Ann Arbor, MI 48109
USA

P.R. Halmos
Department of
Mathematics
Santa Clara University
Santa Clara, CA 95053
USA

Mathematics Subject Classification (1991): 15-02, 15A04, 15A63, 93Axx

Library of Congress Cataloging-in-Publication Data
Fuhrmann, Paul Abraham.
A polynomial approach to linear algebra/P.A. Fuhrmann.
p. cm. – (Universitext)
Includes bibliographical references and index.
ISBN 0-387-94643-8 (softcover: alk. paper)
1. Algebras, Linear. I. Title.
QA184.F8 1996
512′.5–dc20 95-49237

Printed on acid-free paper.

© 1996 Springer-Verlag New York, Inc.
All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer-Verlag New York, Inc., 175 Fifth Avenue, New York, NY 10010, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.
The use of general descriptive names, trade names, trademarks, etc., in this publication, even if the former are not especially identified, is not to be taken as a sign that such names, as understood by the Trade Marks and Merchandise Marks Act, may accordingly be used freely by anyone.

Production managed by Francine McNeill; manufacturing supervised by Jacqui Ashri.
Photocomposed copy prepared using Springer's svsing.sty macro.
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 0-387-94643-8 Springer-Verlag New York Berlin Heidelberg SPIN 10490948

Universitext

Editorial Board
(North America):

S. Axler
F.W. Gehring
P.R. Halmos

Springer
New York
Berlin
Heidelberg
Barcelona
Budapest
Hong Kong
London
Milan
Paris
Santa Clara
Singapore
Tokyo

Universitext

Editors (North America): S. Axler, F.W. Gehring, and P.R. Halmos

Aksoy/Khamsi: Nonstandard Methods in Fixed Point Theory
Aupetit: A Primer on Spectral Theory
Booss/Bleecker: Topology and Analysis
Borkar: Probability Theory: An Advanced Course
Carleson/Gamelin: Complex Dynamics
Cecil: Lie Sphere Geometry: With Applications to Submanifolds
Chae: Lebesgue Integration (2nd ed.)
Charlap: Bieberbach Groups and Flat Manifolds
Chern: Complex Manifolds Without Potential Theory
Cohn: A Classical Invitation to Algebraic Numbers and Class Fields
Curtis: Abstract Linear Algebra
Curtis: Matrix Groups
DiBenedetto: Degenerate Parabolic Equations
Dimca: Singularities and Topology of Hypersurfaces
Edwards: A Formal Background to Mathematics I a/b
Edwards: A Formal Background to Mathematics II a/b
Foulds: Graph Theory Applications
Fuhrmann: A Polynomial Approach to Linear Algebra
Gardiner: A First Course in Group Theory
Gårding/Tambour: Algebra for Computer Science
Goldblatt: Orthogonality and Spacetime Geometry
Hahn: Quadratic Algebras, Clifford Algebras, and Arithmetic Witt Groups
Holmgren: A First Course in Discrete Dynamical Systems
Howe/Tan: Non-Abelian Harmonic Analysis: Applications of $SL(2, R)$
Howes: Modern Analysis and Topology
Humi/Miller: Second Course in Ordinary Differential Equations
Hurwitz/Kritikos: Lectures on Number Theory
Jennings: Modern Geometry with Applications
Jones/Morris/Pearson: Abstract Algebra and Famous Impossibilities
Kannan/Krueger: Advanced Real Analysis
Kelly/Matthews: The Non-Euclidean Hyperbolic Plane
Kostrikin: Introduction to Algebra
Luecking/Rubel: Complex Analysis: A Functional Analysis Approach
MacLane/Moerdijk: Sheaves in Geometry and Logic
Marcus: Number Fields
McCarthy: Introduction to Arithmetical Functions
Meyer: Essential Mathematics for Applied Fields
Mines/Richman/Ruitenburg: A Course in Constructive Algebra
Moise: Introductory Problems Course in Analysis and Topology
Morris: Introduction to Game Theory
Porter/Woods: Extensions and Absolutes of Hausdorff Spaces
Ramsay/Richtmyer: Introduction to Hyperbolic Geometry
Reisel: Elementary Theory of Metric Spaces
Rickart: Natural Function Algebras
Rotman: Galois Theory

(continued after index)

此为试读，需要完整PDF请访问：www.ertongbook.com

Universitext *(continued)*

Rubel/Colliander: Entire and Meromorphic Functions
Sagan: Space-Filling Curves
Samelson: Notes on Lie Algebras
Schiff: Normal Families
Shapiro: Composition Operators and Classical Function Theory
Smith: Power Series From a Computational Point of View
Smoryński: Self-Reference and Modal Logic
Stillwell: Geometry of Surfaces
Stroock: An Introduction to the Theory of Large Deviations
Sunder: An Invitation to von Neumann Algebras
Tondeur: Foliations on Riemannian Manifolds

To Nilly

Preface

Linear algebra is a well-entrenched mathematical subject that is taught in virtually every undergraduate program in both the sciences and engineering. Over the years, many texts have been written on linear algebra; therefore, it is up to the author to justify the presentation of another book in this area to the public.

I feel that my justification for the writing of this book is based on a different choice of material and a different approach to the classical core of linear algebra. The main innovation in it is the emphasis placed on functional models and polynomial algebra as the best vehicle for the analysis of linear transformations and quadratic forms. In pursuing this innovation, a long-lasting trend in mathematics is being reversed. Modern algebra went from the specific to the general, abstracting the underlying unifying concepts and structures. The epitome of this trend was represented by the Bourbaki school. No doubt this was an important part in the development of modern mathematics, but it had its faults, too. It led to several generations of students who could not compute, nor could they give interesting examples of theorems they proved. Even worse, it increased the gap between pure mathematics and the general user of mathematics. It is the last group, which is made up of engineers and applied mathematicians, that is interested not only in understanding a problem, but also in its computational aspects. A very similar development occurred in functional analysis and operator theory. Initially, the axiomatization of Banach and Hilbert spaces led to a search for general methods and results. Although there were some significant successes in these directions, it soon became apparent, especially when trying to understand the structure of bounded operators, that one has to be much more specific. In particular, the introduction of functional models, through the work of Livsic, De Branges, Sz.-Nagy, and Foias, provided a new approach to structure theory. It is these ideas that I have taken as my motivation in the writing of this book.

In the present book, at least where the structure theory is concerned, we look at a special class of shift operators. These are defined by using polynomial modular arithmetic. The interesting fact about this class is its property of universality, in the sense that every cyclic operator is similar to a shift and every linear operator on a finite-dimensional vector space is similar to a direct sum of shifts. Thus, the shifts are the building blocks of an arbitrary linear operator.

Basically, the approach taken in this book is a variation on the study of a linear transformation via the study of the module structure induced by it over the ring of polynomials. While module theory provides great elegance, it is also difficult to grasp by students. Furthermore, it seems too far removed from computation. Matrix theory seems to be at the other extreme; it is concerned too much with computation and not enough with structure. Functional models, especially the polynomial models, lie on an intermediate level of abstraction between module theory and matrix theory.

The book includes specific chapters devoted to quadratic forms and the establishments of algebraic stability criteria. The emphasis is shared between the general theory and the specific examples, which are in this case the study of the Hankel and Bezout forms. This general area, via the work of Hermite, is one of the roots of the theory of Hilbert spaces. I feel that it is most illuminating to see the Euclidean algorithm and the associated Bezout identity not as isolated results, but as an extremely effective tool in the development of fast inversion algorithms for structured matrices.

Another innovation in this book is the inclusion of basic system-theoretic ideas. It is my conviction that it no longer is possible to separate in a natural way the study of linear algebra from the study of linear systems. The two topics have benefited greatly from cross-fertilization. In particular, the theory of finite-dimensional linear systems seems to provide an unending flow of problems, ideas, and concepts that are quickly assimilated in linear algebra. Realization theory is as much a part of linear algebra as is the long familiar companion matrix.

The inclusion of a whole chapter on Hankel norm approximation theory, or AAK theory as it is commonly known, is also a new addition as far as linear algebra books are concerned. This part requires very little mathematical knowledge not covered in the book, but a certain mathematical maturity is assumed. I believe that it is very much within the grasp of a well-motivated undergraduate. In this part, several results from early chapters are reconstructed in a context where stability is central. Thus, the rational Hardy spaces enter, and we have analytic models and shifts. Lagrange and Hermite interpolations are replaced by the Nevanlinna–Pick interpolation. Finally, coprimeness and the Bezout identity reappear, but over a different ring. I believe that the study of these analogies goes a long way toward demonstrating to the student the underlying unity of mathematics.

Let me explain the philosophy that underlies the writing of this book. In a way I share the aim of Halmos [1958] in trying to treat linear transformations on finite-dimensional vector spaces by methods of more general theories. These theories were functional analysis and operator theory in Hilbert space; this is still the case in this book. However, in the intervening years, operator theory has changed remarkably. The emphasis has moved from the study of self-adjoint and normal operators to the study of non-self-adjoint operators. The hope that a general structure theory for linear operators might be developed seems to be too naive. The methods utilizing Riesz–Dunford integrals proved to be too restrictive. On the other hand, a whole new area centering around the theory of invariant subspaces, and the construction and study of functional models, was developed. This new development had its roots not only in pure mathematics, but also in many applied areas, notably scattering, network, control theories, and some areas of stochastic processes as estimation and prediction theories.

I hope that this book will show how linear algebra is related to other, more advanced areas of mathematics. Polynomial models have their root in operator theory, especially that part of operator theory that centered around invariant subspace theory and Hardy spaces. Thus, the point of view adopted here provides a natural link with that area of mathematics, as well as those application areas I have already mentioned.

In writing this book, I chose to work almost exclusively with scalar polynomials, the one exception being the invariant factor algorithm and its application to structure theory. My choice was influenced by the desire to have the book accessible to most undergraduates. Virtually all results about scalar polynomial models have polynomial matrix generalizations, and some of the appropriate references are pointed out in the "Notes and Remarks" sections.

The exercises at the end of chapters have been chosen partly to indicate directions not covered in the book. I have refrained from including routine computational problems. This does not indicate a negative attitude toward computation. Quite to the contrary, I am a great believer in the exercise of computation, and I suggest that readers choose, and work out, their own problems. This is the best way to get a better grasp of the presented material.

I usually use the first seven chapters for a one-year course on linear algebra at the Ben-Gurion University. If the group is a bit more advanced, one can supplement this by more material on quadratic forms. The material on quadratic forms and stability can be used as a one-semester course of special topics in linear algebra. Also, the material on linear systems and Hankel norm approximations can be used as a basis for either a one-term course or a seminar.

Beer Sheva, Israel

Paul A. Fuhrmann

Contents

此为试读,需要完整PDF请访问: www.ertongbook.com

1
Preliminaries

1.1 Maps

Let S be a set. If between elements of the set a relation $a \simeq b$ is defined, so that either $a \simeq b$ holds or not, then we say that we have a **binary relation**. If a binary relation in S satisfies the following conditions:

1. $a \simeq a$ holds for all $a \in S$,

2. $a \simeq b \Leftarrow b \simeq a$,

3. $a \simeq b$ and $b \simeq c \Leftarrow a \simeq c$,

then we say that we have an **equivalence relation** in S. The three conditions are referred to as **reflexivity**, **symmetry**, and **transitivity**, respectively.

For each $a \in S$ we define its equivalence class S_a by $S_a = \{x \in S | x \simeq a\}$. Clearly, $S_a \subset S$ and $S_a \neq \emptyset$.

An equivalence relation leads to a "partition" of the set S. By a **partition** of S we mean a representation of S as the disjoint union of subsets. Since, clearly, using transitivity, either $S_a \cap S_b = \emptyset$ or $S_a = S_b$, and $S = \cup_{a \in S} S_a$, the set of equivalence classes is a partition of S.

Similarly, any partition $S = \cup_\alpha S_\alpha$ defines an equivalence relation by letting $a \simeq b$ if for some α we have $a, b \in S_\alpha$.

A rule that assigns to each member $a \in A$ a unique member $b \in B$ is called a **map** or a **function** from A into B. We will denote this by $f : A \longrightarrow B$ or $A \xrightarrow{f} B$.

We denote by $f(A)$ the image of the set A defined by $f(A) = \{y | y \in B$, there exists an $x \in A$ s.t. $y = f(x)\}$. The inverse image of a subset $M \subset B$ is defined by $f^{-1}(M) = \{x | x \in A,\ f(x) \in M\}$. A map $f : A \longrightarrow B$ is called **injective**, or 1-1, if $f(x) = f(y)$ implies $x = y$. A map $f : A \longrightarrow B$ is called **surjective**, or onto, if $f(A) = B$, for example, for each $y \in B$ there exists an $x \in A$ such that $y = f(x)$.

Given maps $f : A \longrightarrow B$ and $g : B \longrightarrow C$, we can define a map $h : A \longrightarrow C$ by letting $h(x) = g(f(x))$. We call this map h the **composition** or **product** of the maps f and g. This will be denoted by $h = g \circ f$. Given three maps $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$, we compute

$$h \circ (g \circ f)(x) = h(g(f(x)))$$

and

$$(h \circ g) \circ f(x) = h(g(f(x))).$$

So the product of maps is associative, that is,

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Due to the associative law of composition, we can write $h \circ g \circ f$ and, more generally, $f_n \circ \cdots \circ f_1$, unambiguously.

Given a map $f : A \longrightarrow B$, we define an equivalence relation R in A by letting

$$x_1 \simeq x_2 \Leftrightarrow f(x_1) = f(x_2).$$

Thus the equivalence class of a is given by $A_a = \{x | x \in A,\ f(x) = f(a)\}$. We will denote by A/R the set of equivalence classes and refer to this as the quotient set by the equivalence relation.

Next we define three transformations,

$$A \xrightarrow{f_1} A/R \xrightarrow{f_2} f(A) \xrightarrow{f_3} B,$$

with the f_i defined by

$$\begin{aligned} f_1(a) &= A_a \\ f_2(A_a) &= f(a) \\ f_3(b) &= b,\ b \in f(A). \end{aligned}$$

Clearly the map f_1 is surjective, f_2 is bijective, and f_3 is injective. Moreover, we have

$$f = f_3 \circ f_2 \circ f_1.$$

This factorization of f is referred to as the **canonical factorization**. The canonical factorization also can be described via the following commutative diagram:

$$\begin{tikzcd}
A \arrow[r] \arrow[d] & B \arrow[d] \\
A/R \arrow[r] & f(A)
\end{tikzcd}$$

We note that $f_2 \circ f_1$ is surjective whereas $f_3 \circ f_2$ is injective.

1.2 Groups

Given a set M, a **binary operation** is a map from $M \times M$ into M. Thus an ordered pair (a, b) is mapped into an element of M denoted by ab.

A set M with an associative binary operation is called a **semigroup**. Thus, if $a, b \in M$, we have $ab \in M$ and the associative rule is $a(bc) = (ab)c$. Thus the product $a_1 \cdots a_n$ of elements of M is unambiguously defined.

We proceed to define the notion of a **group**, which is the cornerstone of most mathematical structures.

Definition 1.2.1 *A* **group** *is a set G with a binary operation, called multiplication, that satisfies*

1. *$a(bc) = (ab)c$, that is, the associative law.*
2. *There exists a left identity $e \in G$, that is, $ea = a$ for all $a \in G$.*
3. *For each $a \in G$ there exists a left inverse, denoted by a^{-1}, that satisfies $a^{-1}a = e$.*
4. *A group G is called* **abelian** *if the group operation is commutative, that is, if $ab = ba$ holds for all $a, b \in G$.*

Theorem 1.2.1

1. *Let G be a group and let a be an element of G. Then a left inverse a^{-1} of a is also a right inverse.*
2. *A left identity is also a right identity.*
3. *The identity element of a group is unique.*

Proof:

1. We compute

$$\begin{aligned}(a^{-1})^{-1}a^{-1}aa^{-1} &= ((a^{-1})^{-1}a^{-1})(aa^{-1}) = e(aa^{-1}) \\ &= aa^{-1} = (a^{-1})^{-1}(a^{-1}a)a^{-1} = (a^{-1})^{-1}(ea^{-1}) = (a^{-1})^{-1}a^{-1} = e.\end{aligned}$$

   So, in particular, $aa^{-1} = e$.

2. Let $a \in G$ be arbitrary and let e be a left identity. Then

$$aa^{-1}a = a(a^{-1}a) = ae = (aa^{-1})a = ea = a.$$

   Thus $ae = a$ for all a. So e is also a right identity.

3. Let e, e' be two identities in G. Then, using the fact that e is a left identity and e' a right identity, we get

$$e = ee' = e'.$$

□

In a group G, equations of the type $axb = c$ are easily solvable with the solution given by $x = a^{-1}cb^{-1}$. Also, it is easily checked that we have the following rule for inversion:

$$(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}.$$

Definition 1.2.2 *A subset H of a group G is called a* **subgroup** *of G if it is a group with the composition rule inherited from G. Thus H is a subgroup if, with $a, b \in H$, we have $ab \in H$ and $a^{-1} \in H$.*

This can be made a bit more concise.

Lemma 1.2.1 *A subset H of a group G is a subgroup if and only if, with $a, b \in H$, $ab^{-1} \in H$ also.*

Proof: If H is a subgroup, then with $a, b \in H$ it also contains b^{-1} and hence also ab^{-1}.

Conversely, if $a, b \in H$ implies $ab^{-1} \in H$, then $b^{-1} = eb^{-1} \in H$ and hence also $ab = a(b^{-1})^{-1} \in H$, $a, b \in H$. □

Given a subgroup H of a group G, we say that two elements $a, b \in G$ are **equivalent**, and we write $a \simeq b$ if $b^{-1}a \in H$. It is easily checked that this is a bona fide equivalence relation in G, that is, it is a reflexive, symmetric, and transitive relation. We denote by M_a the equivalence class of a, that is,

$$M_a = \{x | x \in G, x \simeq a\}.$$

If we denote by aH the set $\{x | ah, h \in H\}$, then $M_a = aH$. We will refer to these as **right equivalence classes** or as **right cosets. Left equivalence classes** or **left cosets** Ha are defined in a completely analogous way.

此为试读，需要完整PDF请访问：www.ertongbook.com