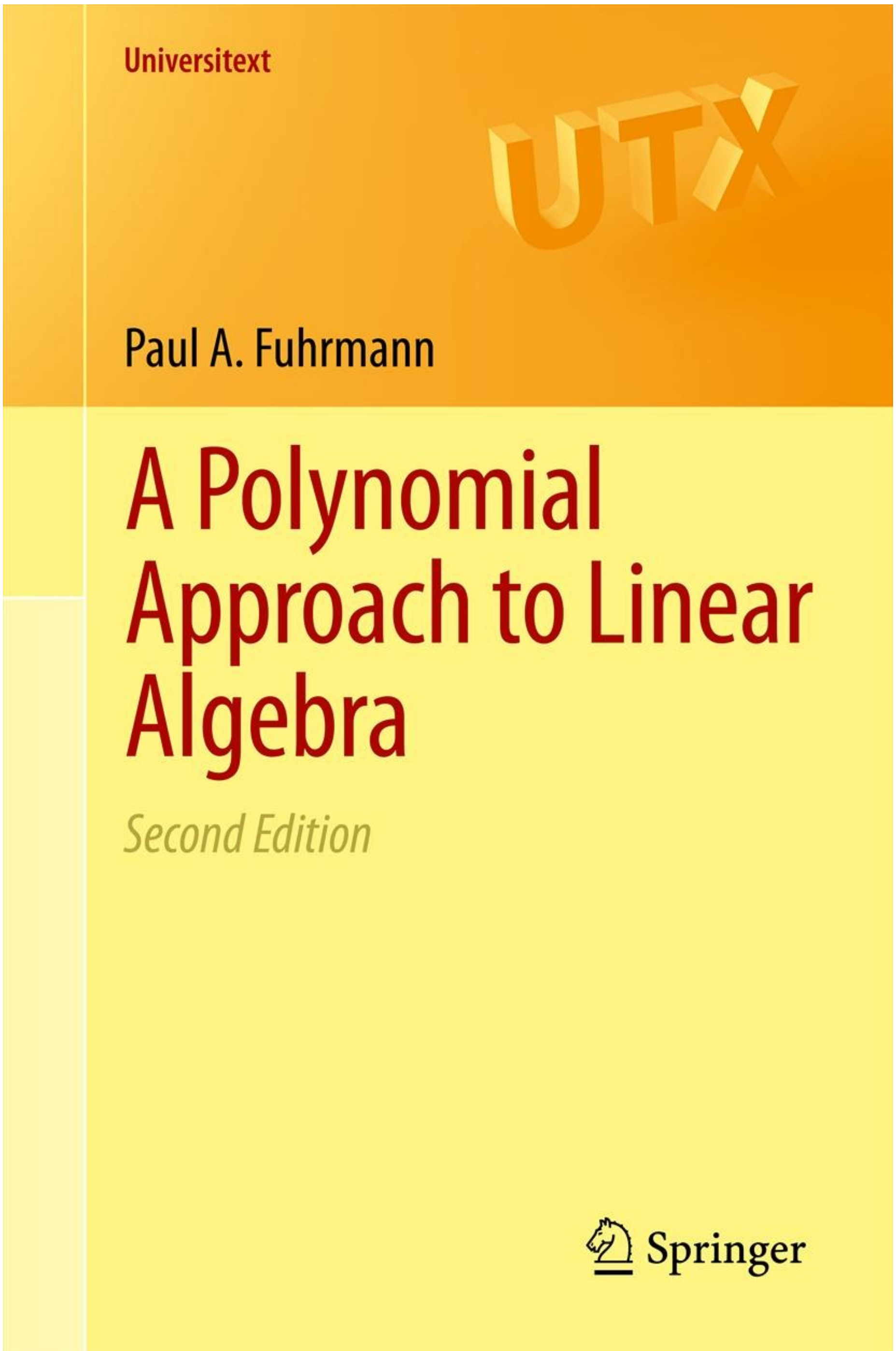
Universitext

Paul A. Fuhrmann

A Polynomial Approach to Linear Algebra

Second Edition

Springer


Universitext
UTX
Paul A. Fuhrmann
A Polynomial Approach to Linear Algebra
Second Edition
Springer

Paul A. Fuhrmann, Universitext, *A Polynomial Approach to Linear Algebra*, 2, DOI: 10.1007/978-1-4614-0338-8, © Springer Science+Business Media, LLC 2012

Universitext

Universitext is a series of textbooks that presents material from a wide variety of mathematical disciplines at master's level and beyond. The books, often well class-tested by their author, may have an informal, personal even experimental approach to their subject matter. Some of the most successful and established books in the series have evolved through several editions, always following the evolution of teaching curricula, to very polished texts.

Thus as research topics trickle down into graduate-level teaching, first textbooks written for new, cutting-edge courses may make their way into *Universitext* .

For further volumes: http://www.springer.com/series/223

Paul A. Fuhrmann

A Polynomial Approach to Linear Algebra

Springer

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

ISSN 0172-5939 e-ISSN 2191-6675

ISBN 978-1-4614-0337-1 e-ISBN 978-1-4614-0338-8

Springer New York Dordrecht Heidelberg London

Library of Congress Control Number: 2011941877

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

To Nilly

Preface

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

I feel that my jusification 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 standing 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 step 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, made up of engineers and applied mathematicians, which is concerned 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. While there were some significant successes in this direction, it soon became apparent, especially in 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, Beurling, Halmos, Lax, de Branges, Sz.-Nagy and Foias, provided a new approach to structure theory. It is these ideas that we have taken as our 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 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, that is, it is too much concerned with computation and not enough with structure. Functional models, especially the polynomial models, lie on an intermediate level of absraction between module theory and matrix theory.

The book includes specific chapters devoted to quadratic forms and the establishment 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 is no longer 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 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 in which stability is central. Thus the rational Hardy spaces enter, and we have analytic models and shifts. Lagrange and Hermite interpolation are replaced by Nevanlinna-Pick interpolation. Finally, coprimeness and the Bezout identity reappear, but over a different ring. I believe the study of these analogies goes a long way toward demonsrating 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 ? 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 on 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 and control theories, and some areas of stochastic processes such 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 on 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 in this project 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.

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 Ben Gurion University. If the group is a bit more advanced, one can supplement this by more material on quadratic forms. The material on qudratic 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.

Paul A. Fuhrmann

Preface to the Second Edition

Linear algebra is one of the most active areas of mathematics, and its importance is ever increasing. The reason for this is, apart from its intrinsic beauty and elegance, its usefulness to a large array of applied areas. This is a two-way road, for applications provide a great stimulus for new research directions. However, the danger of a tower-of-Babel phenomenon is ever present. The broadening of the field has to confront the possibility that, due to differences in terminology, notation, and concepts, the communication between different parts of linear algebra may break down. I strongly believe, based on my long research in the theory of linear systems, that the polynomial techniques presented in this book provide a very good common ground. In a sense, the presentation here is just a commercial for subsequent publications stressing extensions of the scalar techniques to the context of polynomial and rational matrix functions.

Moreover, in the fifteen years since the original publication of this book, my perspective on some of the topics has changed. This, at least partially, is due to the mathematical research I was doing during that period. The most significant changes are the following. Much greater emphasis is put on interpolation theory, both polynomial and rational. In particular, we also approach the commutant lifting theorem via the use of interpolation. The connection between the Chinese remainder theorem and interpolation is explained, and an analytic version of the theorem is given. New material has been added on tensor products, both of vector spaces and of modules. Because of their importance, special attention is given to the tensor products of quotient polynomial modules. In turn, this leads to a conceptual clarification of the role of Bezoutians and the Bezout map in understanding the difference between the tensor products of functional models taken with respect to the underlying field and those taken with respect to the corresponding polynomial ring. This enabled the introduction of some new material on model reduction. In particular, some connections between the polynomial Sylvester equation and model reduction techniques, related to interpolation on the one hand and projection methods on the other, are clarified. In the process of adding material, I also tried to streamline theorem statements and proofs and generally enhance the readability of the book. It is my hope that this effort was at least partially successful.

I am greatly indebted to my friends and colleagues Uwe Helmke and Abie Feintuch for reading parts of the manuscript and making useful suggestions and to Harald Wimmer for providing many useful references to the history of linear algebra. Special thanks to my beloved children, Amir, Oded, and Galit, who not only encouraged and supported me in the effort to update and improve this book, but also enlisted the help of their friends to review the manuscript. To these friends, Shlomo Hoory, Alexander Ivri, Arie Matsliah, Yossi Richter, and Patrick Worfolk, go my sincere thanks.

Paul A. Fuhrmann

Contents

Paul A. Fuhrmann, Universitext, *A Polynomial Approach to Linear Algebra*, DOI: 10.1007/978-1-4614-0338-8_1, © Springer Science+Business Media, LLC 2012

1. Algebraic Preliminaries

Paul A. Fuhrmann[1]

(1) Ben-Gurion University of the Negev, Beer Sheva, Israel

Abstract
This book emphasizes the use of polynomials, and more generally, rational functions, as the vehicle for the development of linear algebra and linear system theory. This is a powerful and elegant idea, and the development of linear theory is leaning more toward the conceptual than toward the technical. However, this approach has its own weakness. The stumbling block is that before learning linear algebra, one has to know the basics of algebra. Thus groups, rings, fields, and modules have to be introduced. This we proceed to do, accompanied by some examples that are relevant to the content of the rest of the book.

1.1 Introduction

This book emphasizes the use of polynomials, and more generally, rational functions, as the vehicle for the development of linear algebra and linear system theory. This is a powerful and elegant idea, and the development of linear theory is leaning more toward the conceptual than toward the technical. However, this approach has its own weakness. The stumbling block is that before learning linear algebra, one has to know the basics of algebra. Thus groups, rings, fields, and modules have to be introduced. This we proceed to do, accompanied by some examples that are relevant to the content of the rest of the book.

1.2 Sets and 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 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. $a \simeq b \Rightarrow b \simeq a$
3. $a \simeq b$ and $b \simeq c \Rightarrow a \simeq c$

then we say 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 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 $f : A \to B$ or A{ f \atop →} B. We denote by $f(A)$ the image of the set A defined by

$f(A) = \{y \mid y \in B, \exists x \in A \text{ s.t. } y = f(x)\}$. The inverse image of a subset $M \subset B$ is defined by $f^{-1}(M) = \{x \mid x \in A,\ f(x) \in M\}$. A map $f : A \to B$ is called **injective** or 1-to-1 if $f(x) = f(y)$ implies $x = y$. A map $f : A \to B$ is called **surjective** or onto if $f(A) = B$, i.e., for each $y \in B$ there exists an $x \in A$ such that $y = f(x)$. A map f is called **bijective** if it is both injective and surjective.

Given maps $f : A \to B$ and $g : B \to C$, we can define a map $h : A \to C$ 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{ f \atop →} B{ g \atop →} C{ h \atop →} 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, i.e.,

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

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 $f : A \to B$, we define an equivalence relation $\simeq$ 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 $A_a = \{x \mid x \in A,\ f(x) = f(a)\}$. We will denote by $A/\simeq$ the set of equivalence classes and refer to this as the quotient set by the equivalence relation.

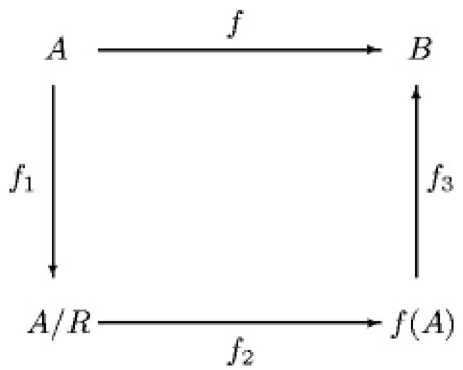
Next we define three transformations

$$A \overset{f_1}{\underset{\longrightarrow}{}} A/R \overset{f_2}{\underset{\longrightarrow}{}} f(A) \overset{f_3}{\underset{\longrightarrow}{}} B$$

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 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 can be described also via the following commutative diagram:



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

1.3 Groups

Given a set M, a **binary operation** in M 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 $a(bc) = (ab)c$ holds. 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 1.1.
A **group** is a set G with a binary operation, called multiplication, that satisfies

1. $a(bc) = (ab)c$, i.e., the associative law.

2. There exists a left identity, or unit element, $e \in G$, i.e., $ea = a$ for all $a \in G$.

3. For each $a \in G$ there exists a left inverse, denoted by a^{-1}, which satisfies $a^{-1}a = e$.

A group G is called **abelian** if the group operation is commutative, i.e., if $ab = ba$ holds for all $a, b \in G$.

In many cases, an abelian group operation will be denoted using the additive notation, i.e., $a + b$ rather than ab, as in the case of the group of integers $\mathbb{Z}$ with addition as the group operation. Other useful examples are $\mathbb{R}$, the set of all real numbers under addition, and $\mathbb{R}_+$, the set of all positive real numbers with multiplication as the group operation.

Given a nonempty set S, the set of all bijective mappings of S onto itself forms a group with the group action being composition. The elements of G are called **permutations** of S. If $S = \{1, \ldots, n\}$, then the group of permutations of S is called the **symmetric group** of degree n and denoted by S_n.

Theorem 1.2.