DOLCIANI MATHEMATICAL EXPOSITIONS #44

MAA GUIDES #6

A GUIDE TO ADVANCED LINEAR ALGEBRA

Steven H. Weintraub

MATHEMATICAL ASSOCIATION OF AMERICA

A Guide to Advanced Linear Algebra

Library of Congress Catalog Card Number 2011923993

Print Edition ISBN 978-0-88385-351-1

Electronic Edition ISBN 978-0-88385-967-4

Printed in the United States of America

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

The Dolciani Mathematical Expositions
NUMBER FORTY-FOUR

MAA Guides # 6

A Guide to Advanced Linear Algebra

Steven H. Weintraub
Lehigh University

Published and Distributed by
The Mathematical Association of America

The DOLCIANI MATHEMATICAL EXPOSITIONS series of the Mathematical Association of America was established through a generous gift to the Association from Mary P. Dolciani, Professor of Mathematics at Hunter College of the City University of New York. In making the gift, Professor Dolciani, herself an exceptionally talented and successful expositor of mathematics, had the purpose of furthering the ideal of excellence in mathematical exposition.

The Association, for its part, was delighted to accept the gracious gesture initiating the revolving fund for this series from one who has served the Association with distinction, both as a member of the Committee on Publications and as a member of the Board of Governors. It was with genuine pleasure that the Board chose to name the series in her honor.

The books in the series are selected for their lucid expository style and stimulating mathematical content. Typically, they contain an ample supply of exercises, many with accompanying solutions. They are intended to be sufficiently elementary for the undergraduate and even the mathematically inclined high-school student to understand and enjoy, but also to be interesting and sometimes challenging to the more advanced mathematician.

1. *Mathematical Gems,* Ross Honsberger
2. *Mathematical Gems II,* Ross Honsberger
3. *Mathematical Morsels,* Ross Honsberger
4. *Mathematical Plums,* Ross Honsberger (ed.)
5. *Great Moments in Mathematics* (*Before 1650*), Howard Eves
6. *Maxima and Minima without Calculus,* Ivan Niven
7. *Great Moments in Mathematics* (*After 1650*), Howard Eves
8. *Map Coloring, Polyhedra, and the Four-Color Problem,* David Barnette
9. *Mathematical Gems III,* Ross Honsberger
10. *More Mathematical Morsels,* Ross Honsberger
11. *Old and New Unsolved Problems in Plane Geometry and Number Theory,* Victor Klee and Stan Wagon
12. *Problems for Mathematicians, Young and Old,* Paul R. Halmos
13. *Excursions in Calculus: An Interplay of the Continuous and the Discrete,* Robert M. Young
14. *The Wohascum County Problem Book,* George T. Gilbert, Mark Krusemeyer, and Loren C. Larson
15. *Lion Hunting and Other Mathematical Pursuits: A Collection of Mathematics, Verse, and Stories by Ralph P. Boas, Jr.,* edited by Gerald L. Alexanderson and Dale H. Mugler
16. *Linear Algebra Problem Book,* Paul R. Halmos
17. *From Erdős to Kiev: Problems of Olympiad Caliber,* Ross Honsberger
18. *Which Way Did the Bicycle Go? ... and Other Intriguing Mathematical Mysteries,* Joseph D. E. Konhauser, Dan Velleman, and Stan Wagon

19. *In Pólya's Footsteps: Miscellaneous Problems and Essays,* Ross Honsberger
20. *Diophantus and Diophantine Equations,* I. G. Bashmakova (Updated by Joseph Silverman and translated by Abe Shenitzer)
21. *Logic as Algebra,* Paul Halmos and Steven Givant
22. *Euler: The Master of Us All,* William Dunham
23. *The Beginnings and Evolution of Algebra,* I. G. Bashmakova and G. S. Smirnova (Translated by Abe Shenitzer)
24. *Mathematical Chestnuts from Around the World,* Ross Honsberger
25. *Counting on Frameworks: Mathematics to Aid the Design of Rigid Structures,* Jack E. Graver
26. *Mathematical Diamonds,* Ross Honsberger
27. *Proofs that Really Count: The Art of Combinatorial Proof,* Arthur T. Benjamin and Jennifer J. Quinn
28. *Mathematical Delights,* Ross Honsberger
29. *Conics,* Keith Kendig
30. *Hesiod's Anvil: falling and spinning through heaven and earth,* Andrew J. Simoson
31. *A Garden of Integrals,* Frank E. Burk
32. *A Guide to Complex Variables* (MAA Guides #1), Steven G. Krantz
33. *Sink or Float? Thought Problems in Math and Physics*, Keith Kendig
34. *Biscuits of Number Theory*, Arthur T. Benjamin and Ezra Brown
35. *Uncommon Mathematical Excursions: Polynomia and Related Realms*, Dan Kalman
36. *When Less is More: Visualizing Basic Inequalities*, Claudi Alsina and Roger B. Nelsen
37. *A Guide to Advanced Real Analysis* (MAA Guides #2), Gerald B. Folland
38. *A Guide to Real Variables* (MAA Guides #3), Steven G. Krantz
39. *Voltaire's Riddle: Micromégas and the measure of all things*, Andrew J. Simoson
40. *A Guide to Topology*, (MAA Guides #4), Steven G. Krantz
41. *A Guide to Elementary Number Theory*, (MAA Guides #5), Underwood Dudley
42. *Charming Proofs: A Journey into Elegant Mathematics*, Claudi Alsina and Roger B. Nelsen
43. *Mathematics and Sports*, edited by Joseph A. Gallian
44. *A Guide to Advanced Linear Algebra*, (MAA Guides #6), Steven H. Weintraub

MAA Service Center
P.O. Box 91112
Washington, DC 20090-1112
1-800-331-1MAA FAX: 1-301-206-9789

Preface

Linear algebra is a beautiful and mature field of mathematics, and mathematicians have developed highly effective methods for solving its problems. It is a subject well worth studying for its own sake.

More than that, linear algebra occupies a central place in modern mathematics. Students in algebra studying Galois theory, students in analysis studying function spaces, students in topology studying homology and cohomology, or for that matter students in just about any area of mathematics, studying just about anything, need to have a sound knowledge of linear algebra.

We have written a book that we hope will be broadly useful. The core of linear algebra is essential to every mathematician, and we not only treat this core, but add material that is essential to mathematicians in specific fields, even if not all of it is essential to everybody.

This is a book for advanced students. We presume you are already familiar with elementary linear algebra, and that you know how to multiply matrices, solve linear systems, etc. We do not treat elementary material here, though in places we return to elementary material from a more advanced standpoint to show you what it really means. However, we do not presume you are already a mature mathematician, and in places we explain what (we feel) is the "right" way to understand the material. The author feels that one of the main duties of a teacher is to provide a viewpoint on the subject, and we take pains to do that here.

One thing that you should learn about linear algebra now, if you have not already done so, is the following: *Linear algebra is about vector spaces and linear transformations, not about matrices*. This is very much the approach of this book, as you will see upon reading it.

We treat both the finite and infinite dimensional cases in this book, and point out the differences between them, but the bulk of our attention is devoted to the finite dimensional case. There are two reasons: First, the strongest results are available here, and second, this is the case most widely used in mathematics. (Of course, matrices are available only in the finite dimensional case, but, even here, we almost always argue in terms of linear transformations rather than matrices.)

We regard linear algebra as part of algebra, and that guides our approach. But we have followed a middle ground. One of the principal goals of this book is to derive canonical forms for linear transformations on finite dimensional vector spaces, i.e., rational and Jordan canonical forms. The quickest and perhaps most enlightening approach is to derive them as corollaries of the basic structure theorems for modules over a principal ideal domain (PID). Doing so would require a good deal of background, which would limit the utility of this book. Thus our main line of approach does not use these, though we indicate this approach in an appendix. Instead we adopt a more direct argument.

We have written a book that we feel is a thorough, though intentionally not encyclopedic, treatment of linear algebra, one that contains material that is both important and deservedly "well known". In a few places we have succumbed to temptation and included material that is not quite so well known, but that in our opinion should be.

We hope that you will be enlightened not only by the specific material in the book but by its style of argument–we hope it will help you learn to "think like a mathematician". We also hope this book will serve as a valuable reference throughout your mathematical career.

Here is a rough outline of the text. We begin, in Chapter 1, by introducing the basic notions of linear algebra, vector spaces and linear transformations, and establish some of their most important properties. In Chapter 2 we introduce coordinates for vectors and matrices for linear transformations. In the first half of Chapter 3 we establish the basic properties of determinants, and in the last half of that chapter we give some of their applications. Chapters 4 and 5 are devoted to the analysis of the structure of a single linear transformation from a finite dimensional vector space to itself. In particular, in these chapters, we develop eigenvalues, eigenvectors, and generalized eigenvectors, and derive rational and Jordan canonical forms. In Chapter 6 we introduce additional structure on a vector space, that of a (bilinear, sesquilinear, or quadratic) form, and analyze these forms. In Chapter 7 we specialize the situation of Chapter 6 to that of a positive definite inner product on a real or complex vector space, and in particular derive the spectral theorem. In Chapter 8 we provide an introduction to Lie groups, which are central objects in mathematics and are a meeting place for algebra, analysis, and topology. (For this chapter we require the additional background knowledge of the inverse function theorem.) In Appendix A we review basic properties of polynomials and polynomial rings that we use, and in Appendix B we rederive some of our results on canonical forms of a linear transformation from the structure theorems for modules over a PID.

We have provided complete proofs of just about all the results in this book, except that we have often omitted proofs that are routine without comment.

As we have remarked above, we have tried to write a book that will be widely applicable. This book is written in an algebraic spirit, so the student of algebra will find items of interest and particular applications, too numerous to mention here, throughout the book. The student of analysis will appreciate the fact that we not only consider finite dimensional vector spaces, but also infinite dimensional ones, and will also appreciate our material on inner product spaces and our particular examples of function spaces. The student of algebraic topology will appreciate our dimension-counting arguments and our careful attention to duality, and the student of differential topology will appreciate our material on orientations of vector spaces and our introduction to Lie groups.

No book can treat everything. With the exception of a short section on Hilbert matrices, we do not treat computational issues at all. They do not fit in with our theoretical approach. Students in numerical analysis, for example, will need to look elsewhere for this material.

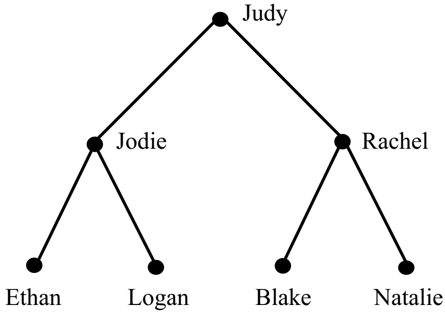
To close this preface, we establish some notational conventions. We will denote both sets (usually but not always sets of vectors) and linear transformations by script letters $\mathcal{A}, \mathcal{B}, \ldots, \mathcal{Z}$. We will tend to use script letters near the front of the alphabet for sets and script letters near the end of the alphabet for linear transformations. $\mathcal{T}$ will always denote a linear transformation and $\mathcal{I}$ will always denote the identity linear transformation. Some particular linear transformations will have particular notations, often in boldface. Capital letters will denote either vector spaces or matrices. We will tend to denote vector spaces by capital letters near the end of the alphabet, and V will always denote a vector space. Also, I will almost always denote the identity matrix. $\mathbb{E}$ and $\mathbb{F}$ will denote arbitrary fields and $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ will denote the fields of rational, real, and complex numbers respectively. $\mathbb{Z}$ will denote the ring of integers. We will use $\mathcal{A} \subseteq \mathcal{B}$ to mean that $\mathcal{A}$ is a subset of $\mathcal{B}$ and $\mathcal{A} \subset \mathcal{B}$ to mean that $\mathcal{A}$ is a proper subset of $\mathcal{B}$. $A = (a_{ij})$ will mean that A is the matrix whose entry in the (i, j) position is a_{ij}. $A = [v_1 \mid v_2 \mid \cdots \mid v_n]$ will mean that A is the matrix whose ith column is v_i. We will denote the transpose of the matrix A by ${}^tA$ (not by A^t). Finally, we will write $\mathcal{B} = \{v_i\}$ as shorthand for $\mathcal{B} = \{v_i\}_{i \in I}$ where I is an indexing set, and $\sum c_i v_i$ will mean $\sum_{i \in I} c_i v_i$.

We follow a conventional numbering scheme with, for example, Remark 1.3.12 denoting the 12th numbered item in Section 1.3 of Chapter 1. We use $\square$ to denote the end of proofs. Theorems, etc., are set in italics, so the end of italics denotes the end of their statements. But definitions, etc., are set in ordinary type, so there is ordinarily nothing to denote the end of their statements. We use $\diamond$ for that.

Steven H. Weintraub
Bethlehem, PA, USA
January 2010

Contents

To the binary tree:



CHAPTER 1

VECTOR SPACES AND LINEAR TRANSFORMATIONS

In this chapter we introduce the objects we will be studying and investigate some of their basic properties.

1.1 BASIC DEFINITIONS AND EXAMPLES

DEFINITION 1.1.1. A vector space V over a field $\mathbb{F}$ is a set V with a pair of operations $(u, v) \mapsto u + v$ for $u, v \in V$ and $(c, u) \mapsto cu$ for $c \in \mathbb{F}$, $v \in V$ satisfying the following axioms:

(1) $u + v \in V$ for any $u, v \in V$.

(2) $u + v = v + u$ for any $u, v \in V$.

(3) $u + (v + w) = (u + v) + w$ for any $u, v, w \in V$.

(4) There is a $0 \in V$ such that $0 + v = v + 0 = v$ for any $v \in V$.

(5) For any $v \in V$ there is a $-v \in V$ such that $v + (-v) = (-v) + v = 0$.

(6) $cv \in V$ for any $c \in \mathbb{F}$, $v \in V$.

(7) $c(u + v) = cu + cv$ for any $c \in \mathbb{F}$, $u, v \in V$.

(8) $(c + d)u = cu + du$ for any $c, d \in \mathbb{F}$, $u \in V$.

(9) $c(du) = (cd)u$ for any $c, d \in \mathbb{F}$, $u \in V$.

(10) $1u = u$ for any $u \in V$.

$\diamond$

REMARK 1.1.2. The elements of $\mathbb{F}$ are called *scalars* and the elements of V are called *vectors*. The operation $(u, v) \mapsto u + v$ is called *vector addition* and the operation $(c, u) \mapsto cu$ is called *scalar multiplication*. $\diamond$

REMARK 1.1.3. Properties (1) through (5) of Definition 1.1.1 state that V forms an abelian group under the operation of vector addition. $\diamond$

Lemma 1.1.4. *(1)* $0 \in V$ *is unique.*

(2) $0v = 0$ *for any* $v \in V$.

(3) $(-1)v = -v$ *for any* $v \in V$.

DEFINITION 1.1.5. Let V be a vector space. W is a *subspace* of V if $W \subseteq V$ and W is a vector space with the same operations of vector addition and scalar multiplication as V. $\diamond$

The following result gives an easy way of testing whether a subset W of V is a subspace of V.

Lemma 1.1.6. *Let* $W \subseteq V$. *Then* W *is a subspace of* V *if and only if it satisfies the equivalent sets of conditions (0), (1), and (2), or (0′), (1), and (2):*

(0) W *is nonempty.*

(0′) $0 \in W$.

(1) If $w_1, w_2 \in W$ *then* $w_1 + w_2 \in W$.

(2) If $w \in W$ *and* $c \in \mathbb{F}$, *then* $cw \in W$.

EXAMPLE 1.1.7. (1) The archetypal example of a vector space is $\mathbb{F}^n$, for a positive integer n, the space of column vectors

$$\mathbb{F}^n = \left\{ \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \middle| \ a_i \in \mathbb{F} \right\}.$$

We also have the spaces "little $\mathbb{F}^\infty$" and "big $\mathbb{F}^\infty$" which we denote by $\mathbb{F}^\infty$ and $\mathbb{F}^{\infty\infty}$ respectively (this is nonstandard notation) that are defined by

$$\mathbb{F}^\infty = \left\{ \begin{bmatrix} a_1 \\ a_2 \\ \vdots \end{bmatrix} \middle| \ a_i \in \mathbb{F}, \text{ only finitely many nonzero} \right\},$$

$$\mathbb{F}^{\infty\infty} = \left\{ \begin{bmatrix} a_1 \\ a_2 \\ \vdots \end{bmatrix} \middle| \ a_i \in \mathbb{F} \right\}.$$

$\mathbb{F}^\infty$ is a subspace of $\mathbb{F}^{\infty\infty}$.

Let e_i denote the vector in $\mathbb{F}^n$, $\mathbb{F}^\infty$, or $\mathbb{F}^{\infty\infty}$ (which we are considering should be clear from the context) with a 1 in position i and 0 everywhere else. A formal definition appears in Example 1.2.18(1).

(2) We have the vector spaces ${}^r\mathbb{F}^n$, ${}^r\mathbb{F}^\infty$, and ${}^r\mathbb{F}^{\infty\infty}$ defined analogously to $\mathbb{F}^n$, $\mathbb{F}^\infty$, and $\mathbb{F}^{\infty\infty}$ but using row vectors rather than column vectors.

(3) $\mathrm{M}_{m,n}(\mathbb{F}) = \{m\text{-by-}n \text{ matrices with entries in } \mathbb{F}\}$. We abbreviate $\mathrm{M}_{m,m}(\mathbb{F})$ by $\mathrm{M}_m(\mathbb{F})$.

(4) $P(\mathbb{F}) = \{\text{polynomials } p(x) \text{ with coefficients in } \mathbb{F}\}$. For a nonnegative integer n, $P_n(\mathbb{F}) = \{\text{polynomials } p(x) \text{ of degree at most } n \text{ with coefficients in } \mathbb{F}\}$. Although the degree of the 0 polynomial is undefined, we adopt the convention that $0 \in P_n(\mathbb{F})$ for every n. Observe that $P_n(\mathbb{F})$ is a subspace of $P(\mathbb{F})$, and that $P_m(\mathbb{F})$ is a subspace of $P_n(\mathbb{F})$ whenever $m \leq n$. (We also use the notation $\mathbb{F}[x]$ for $P(\mathbb{F})$. We use $P(\mathbb{F})$ when we want to consider polynomials as elements of a vector space while we use $\mathbb{F}[x]$ when we want to consider their properties as polynomials.)

(5) $\mathbb{F}$ is itself an $\mathbb{F}$-vector space. If $\mathbb{E}$ is any field containing $\mathbb{F}$ as a subfield (in which case we say $\mathbb{E}$ is an extension field of $\mathbb{F}$), $\mathbb{E}$ is an $\mathbb{F}$-vector space. For example, $\mathbb{C}$ is an $\mathbb{R}$-vector space.

(6) If $\mathcal{A}$ is a set, $\{\text{functions } f : \mathcal{A} \to \mathbb{F}\}$ is a vector space. We denote it by $\mathbb{F}^{\mathcal{A}}$.

(7) $C^0(\mathbb{R})$, the space of continuous functions $f : \mathbb{R} \to \mathbb{R}$, is a vector space. For any $k > 0$, $C^k(\mathbb{R}) = \{\text{functions } f : \mathbb{R} \to \mathbb{R} \mid f, f', \ldots, f^{(k)} \text{ are all continuous}\}$ is a vector space. Also, $C^\infty(\mathbb{R}) = \{\text{functions } f : \mathbb{R} \to \mathbb{R} \mid f \text{ has continuous derivatives of all orders}\}$ is a vector space. $\diamond$

Not only do we want to consider vector spaces, we want to consider the appropriate sort of functions between them, given by the following definition.

DEFINITION 1.1.8. Let V and W be vector spaces. A function $\mathcal{T} : V \to W$ is a *linear transformation* if for all $v, v_1, v_2 \in V$ and all $c \in \mathbb{F}$:

(1) $\mathcal{T}(cv) = c\mathcal{T}(v)$.

(2) $\mathcal{T}(v_1 + v_2) = \mathcal{T}(v_1) + \mathcal{T}(v_2)$. $\diamond$

Lemma 1.1.9. *Let $\mathcal{T} : V \to W$ be a linear transformation. Then $\mathcal{T}(0) = 0$.*

DEFINITION 1.1.10. Let V be a vector space. The *identity* linear transformation $\mathcal{I} : V \to V$ is the linear transformation defined by

$$\mathcal{I}(v) = v \quad \text{for every } v \in V. \qquad \diamond$$

Here is one of the most important ways of constructing linear transformations.

EXAMPLE 1.1.11. Let A be an m-by-n matrix with entries in $\mathbb{F}$, $A \in \mathrm{M}_{m,n}(\mathbb{F})$. Then $\mathcal{T}_A : \mathbb{F}^n \to \mathbb{F}^m$ defined by

$$\mathcal{T}_A(v) = Av$$

is a linear transformation. $\diamond$

Lemma 1.1.12. *(1) Let A and B be m-by-n matrices. Then $A = B$ if and only if $\mathcal{T}_A = \mathcal{T}_B$.*

(2) Every linear transformation $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^m$ is $\mathcal{T}_A$ for some unique m-by-n matrix A.

Proof. (1) Clearly if $A = B$, then $\mathcal{T}_A = \mathcal{T}_B$. Conversely, suppose $\mathcal{T}_A = \mathcal{T}_B$. Then $\mathcal{T}_A(v) = \mathcal{T}_B(v)$ for every $v \in \mathbb{F}^n$. In particular, if $v = e_i$, then $\mathcal{T}_A(e_i) = \mathcal{T}_B(e_i)$, i.e., $Ae_i = Be_i$. But Ae_i is just the ith column of A, and Be_i is just the ith column of B. Since this is true for every i, $A = B$.

(2) $\mathcal{T} = \mathcal{T}_A$ for

$$A = \left[\mathcal{T}(e_1) \mid \mathcal{T}(e_2) \mid \cdots \mid \mathcal{T}(e_n)\right]. \qquad \square$$

DEFINITION 1.1.13. The n-by-n *identity matrix* I is the matrix defined by the equation

$$\mathcal{I} = \mathcal{T}_I. \qquad \diamond$$

It is easy to check that this gives the usual definition of the identity matrix.

We now use Lemma 1.1.12 to *define* matrix operations.

DEFINITION 1.1.14. (1) Let A be an m-by-n matrix and c be a scalar. Then $D = cA$ is the matrix defined by $\mathcal{T}_D = c\mathcal{T}_A$.

(2) Let A and B be m-by-n matrices. Then $E = A + B$ is the matrix defined by $\mathcal{T}_E = \mathcal{T}_A + \mathcal{T}_B$. $\diamond$

It is easy to check that these give the usual definitions of the scalar multiple cA and the matrix sum $A + B$.

Theorem 1.1.15. *Let U, V, and W be vector spaces. Let $\mathcal{T} : U \to V$ and $\mathcal{S} : V \to W$ be linear transformations. Then the composition $\mathcal{S} \circ \mathcal{T} : U \to W$, defined by $(\mathcal{S} \circ \mathcal{T})(u) = \mathcal{S}(\mathcal{T}(u))$, is a linear transformation.*

Proof.

$$\begin{aligned}(\mathcal{S} \circ \mathcal{T})(cu) &= \mathcal{S}(\mathcal{T}(cu)) = \mathcal{S}(c\mathcal{T}(u)) \\ &= c\mathcal{S}(\mathcal{T}(u)) = c(\mathcal{S} \circ \mathcal{T})(u)\end{aligned}$$

and

$$\begin{aligned}(\mathcal{S} \circ \mathcal{T})(u_1 + u_2) &= \mathcal{S}(\mathcal{T}(u_1 + u_2)) = \mathcal{S}(\mathcal{T}(u_1) + \mathcal{T}(u_2)) \\ &= \mathcal{S}(\mathcal{T}(u_1)) + \mathcal{S}(\mathcal{T}(u_2)) \\ &= (\mathcal{S} \circ \mathcal{T})(u_1) + (\mathcal{S} \circ \mathcal{T})(u_2).\end{aligned}$$ □

We now use Theorem 1.1.15 to *define* matrix multiplication.

DEFINITION 1.1.16. Let A be an m-by-n matrix and B be an n-by-p matrix. Then $D = AB$ is the m-by-p matrix defined by $\mathcal{T}_D = \mathcal{T}_A \circ \mathcal{T}_B$. ◇

It is routine to check that this gives the usual definition of matrix multiplication.

Theorem 1.1.17. *Matrix multiplication is associative, i.e., if A is an m-by-n matrix, B is an n-by-p matrix, and C is a p-by-q matrix, then $A(BC) = (AB)C$.*

Proof. Let $D = A(BC)$ and $E = (AB)C$. Then D is the unique matrix defined by $\mathcal{T}_D = \mathcal{T}_A \circ \mathcal{T}_{BC} = \mathcal{T}_A \circ (\mathcal{T}_B \circ \mathcal{T}_C)$, while E is the unique matrix defined by $\mathcal{T}_E = \mathcal{T}_{AB} \circ \mathcal{T}_C = (\mathcal{T}_A \circ \mathcal{T}_B) \circ \mathcal{T}_C$. But composition of functions is associative, $\mathcal{T}_A \circ (\mathcal{T}_B \circ \mathcal{T}_C) = (\mathcal{T}_A \circ \mathcal{T}_B) \circ \mathcal{T}_C$, so $D = E$, i.e., $A(BC) = (AB)C$. □

Lemma 1.1.18. *Let $\mathcal{T} : V \to W$ be a linear transformation. Then $\mathcal{T}$ is invertible (as a linear transformation) if and only if $\mathcal{T}$ is* 1-1 *and onto.*

Proof. $\mathcal{T}$ is invertible as a function if and only if $\mathcal{T}$ is 1-1 and onto. It is then easy to check that in this case the function $\mathcal{T}^{-1} : W \to V$ is a linear transformation. □

DEFINITION 1.1.19. An invertible linear transformation $\mathcal{T} : V \to W$ is called an *isomorphism*. Two vector spaces V and W are *isomorphic* if there is an isomorphism $\mathcal{T} : V \to W$. ◇

REMARK 1.1.20. It is easy to check that being isomorphic is an equivalence relation among vector spaces. $\diamond$

Although the historical development of calculus preceded the historical development of linear algebra, with hindsight we can see that calculus "works" because of the three parts of the following example.

EXAMPLE 1.1.21. Let $V = C^{\infty}(\mathbb{R})$, the vector spaces of real valued infinitely differentiable functions on the real line $\mathbb{R}$.

(1) For a real number a, let $\mathbf{E}_a : V \to \mathbb{R}$ be evaluation at a, i.e., $\mathbf{E}_a(f(x)) = f(a)$. Then $\mathbf{E}_a$ is a linear transformation. We also have the linear transformation $\widetilde{\mathbf{E}}_a : V \to V$, where $\widetilde{\mathbf{E}}_a(f(x))$ is the constant function whose value is $f(a)$.

(2) Let $\mathbf{D} : V \to V$ be differentiation, i.e., $\mathbf{D}(f(x)) = f'(x)$. Then $\mathbf{D}$ is a linear transformation.

(3) For a real number a, let $\mathbf{I}_a : V \to V$ be definite integration starting at $t = a$, i.e., $\mathbf{I}_a(f)(x) = \int_a^x f(t)\,dt$. Then $\mathbf{I}_a$ is a linear transformation. We also have the linear transformation $\mathbf{E}_b \circ \mathbf{I}_a$, with $(\mathbf{E}_b \circ \mathbf{I}_a)(f(x)) = \int_a^b f(x)\,dx$. $\diamond$

Theorem 1.1.22. *(1)* $\mathbf{D} \circ \mathbf{I}_a = \mathcal{I}$.

(2) $\mathbf{I}_a \circ \mathbf{D} = \mathcal{I} - \widetilde{\mathbf{E}}_a$.

Proof. This is the Fundamental Theorem of Calculus. $\square$

EXAMPLE 1.1.23. (1) Let $V = {}^r\mathbb{F}^{\infty\infty}$. We define $\mathbf{L} : V \to V$ (*left shift*) and $\mathbf{R} : V \to V$ (*right shift*) by

$$\mathbf{L}\big([a_1, a_2, a_3, \dots]\big) = [a_2, a_3, a_4, \dots],$$
$$\mathbf{R}\big([a_1, a_2, a_3, \dots]\big) = [0, a_1, a_2, \dots].$$

Note that $\mathbf{L}$ and $\mathbf{R}$ restrict to linear transformations (which we denote by the same letters) from ${}^r\mathbb{F}^{\infty}$ to ${}^r\mathbb{F}^{\infty}$. (We could equally well consider up-shift and down-shift on $\mathbb{F}^{\infty\infty}$ or $\mathbb{F}^{\infty}$, but it is traditional to consider left-shift and right-shift.)

(2) Let $\mathbb{E}$ be an extension field of $\mathbb{F}$. Then for $\alpha \in \mathbb{E}$, we have the linear transformation given by multiplication by α, i.e., $\mathcal{T}(\beta) = \alpha\beta$ for every $\beta \in \mathbb{E}$.

(3) Let $\mathcal{A}$ and $\mathcal{B}$ be sets. We have the vector spaces $\mathbb{F}^{\mathcal{A}} = \{f : \mathcal{A} \to \mathbb{F}\}$ and $\mathbb{F}^{\mathcal{B}} = \{g : \mathcal{B} \to \mathbb{F}\}$. Let $\varphi : \mathcal{A} \to \mathcal{B}$ be a function. Then

$\varphi^* : \mathbb{F}^{\mathcal{B}} \to \mathbb{F}^{\mathcal{A}}$ is the linear transformation defined by $\varphi^*(g) = g \circ \varphi$, i.e., $\varphi^*(g) : \mathcal{A} \to \mathbb{F}$ is the function defined by

$$\varphi^*(g)(a) = g\big(\varphi(a)\big) \quad \text{for } a \in \mathcal{A}.$$

Note that φ^* "goes the other way" than φ. That is, φ is *covariant*, i.e., pushes points forward, while φ^* is *contravariant*, i.e., pulls functions back. Also, the pull-back is given by composition. This is a situation that recurs throughout mathematics. $\diamond$

Here are two of the most important ways in which subspaces arise.

DEFINITION 1.1.24. Let $\mathcal{T} : V \to W$ be a linear transformation. Then the *kernel* of $\mathcal{T}$ is

$$\operatorname{Ker}(\mathcal{T}) = \{v \in V \mid \mathcal{T}(v) = 0\}$$

and the *image* of $\mathcal{T}$ is

$$\operatorname{Im}(\mathcal{T}) = \{w \in W \mid w = \mathcal{T}(v) \text{ for some } v \in V\}. \qquad \diamond$$

Lemma 1.1.25. *In the situation of Definition 1.1.24,* $\operatorname{Ker}(\mathcal{T})$ *is a subspace of* V *and* $\operatorname{Im}(\mathcal{T})$ *is a subspace of* W.

Proof. It is easy to check that the conditions in Lemma 1.1.6 are satisfied. $\square$

REMARK 1.1.26. If $\mathcal{T} = \mathcal{T}_A$, $\operatorname{Ker}(\mathcal{T})$ is often called the *nullspace* of A and $\operatorname{Im}(\mathcal{T})$ is often called the *column space* of A. $\diamond$

We introduce one more vector space.

DEFINITION 1.1.27. Let V and W be vector spaces. Then $\operatorname{Hom}_{\mathbb{F}}(V, W)$, the space of $\mathbb{F}$-*homomorphisms* from V to W, is

$$\operatorname{Hom}_{\mathbb{F}}(V, W) = \{\text{linear transformations } \mathcal{T} : V \to W\}.$$

If $W = V$, we set $\operatorname{End}_{\mathbb{F}}(V) = \operatorname{Hom}_{\mathbb{F}}(V, V)$, the space of $\mathbb{F}$-*endomorphisms* of V. $\diamond$

Lemma 1.1.28. *For any* $\mathbb{F}$*-vector spaces* V *and* W, $\operatorname{Hom}_{\mathbb{F}}(V, W)$ *is a vector space.*

Proof. It is routine to check that the conditions in Definition 1.1.1 are satisfied. $\square$

We also have the subset, which is definitely not a subspace, of $\mathrm{End}_{\mathbb{F}}(V)$ consisting of invertible linear transformations.

DEFINITION 1.1.29. (1) Let V be a vector space. The *general linear group* $\mathrm{GL}(V)$ is

$$\mathrm{GL}(V) = \{\text{invertible linear transformations } \mathcal{T} : V \to V\}.$$

(2) The *general linear group* $\mathrm{GL}_n(\mathbb{F})$ is

$$\mathrm{GL}_n(\mathbb{F}) = \{\text{invertible } n\text{-by-}n \text{ matrices with entries in } \mathbb{F}\}. \qquad \diamond$$

Theorem 1.1.30. *Let $V = \mathbb{F}^n$ and $W = \mathbb{F}^m$. Then $\mathrm{Hom}_{\mathbb{F}}(V, W)$ is isomorphic to $\mathrm{M}_{m,n}(\mathbb{F})$. In particular, $\mathrm{End}_{\mathbb{F}}(V)$ is isomorphic to $\mathrm{M}_n(\mathbb{F})$. Also, $\mathrm{GL}(V)$ is isomorphic to $\mathrm{GL}_n(\mathbb{F})$.*

Proof. By Lemma 1.1.12, any $\mathcal{T} \in \mathrm{Hom}_{\mathbb{F}}(V, W)$ is $\mathcal{T} = \mathcal{T}_A$ for a unique $A \in \mathrm{M}_{m,n}(\mathbb{F})$. Then the linear transformation $\mathcal{T}_A \mapsto A$ gives an isomorphism from $\mathrm{Hom}_{\mathbb{F}}(V, W)$ to $\mathrm{M}_{m,n}(\mathbb{F})$. This restricts to a group isomorphism from $\mathrm{GL}_n(\mathbb{F})$ to $\mathrm{GL}(V)$. □

REMARK 1.1.31. In the next section we define the dimension of a vector space and in the next chapter we will see that Theorem 1.1.30 remains true when V and W are allowed to be any vector spaces of dimensions n and m respectively. ◇

1.2 BASIS AND DIMENSION

In this section we develop the very important notion of a basis of a vector space. A basis $\mathcal{B}$ of the vector space V has two properties: $\mathcal{B}$ is linearly independent and $\mathcal{B}$ spans V. We begin by developing each of these two notions, which are important in their own right. We shall prove that any two bases of V have the same number of elements, which enables us to define the dimension of V as the number of elements in any basis of V.

DEFINITION 1.2.1. Let $\mathcal{B} = \{v_i\}$ be a subset of V. A vector $v \in V$ is a *linear combination* of the vectors in $\mathcal{B}$ if there is a set of scalars $\{c_i\}$, only finitely many of which are nonzero, such that

$$v = \sum c_i v_i. \qquad \diamond$$

REMARK 1.2.2. If we choose all $c_i = 0$ then we obtain

$$0 = \sum c_i v_i.$$

This is the *trivial* linear combination of the vectors in $\mathcal{B}$. Any other linear combination is *nontrivial*. $\diamond$

REMARK 1.2.3. In case $\mathcal{B} = \{\ \}$, the only linear combination we have is the empty linear combination, whose value we consider to be $0 \in V$ and which we consider to be a trivial linear combination. $\diamond$

DEFINITION 1.2.4. Let $\mathcal{B} = \{v_i\}$ be a subset of V. Then $\mathcal{B}$ is *linearly independent* if the only linear combination of elements of V that is equal to 0 is the trivial linear combination, i.e., if $0 = \sum c_i v_i$ implies $c_i = 0$ for every i. $\diamond$

DEFINITION 1.2.5. Let $\mathcal{B} = \{v_i\}$ be a subset of V. Then $\operatorname{Span}(\mathcal{B})$ is the subspace of V consisting of all linear combinations of elements of $\mathcal{B}$,

$$\operatorname{Span}(\mathcal{B}) = \left\{ \sum c_i v_i \mid c_i \in \mathbb{F} \right\}.$$

If $\operatorname{Span}(\mathcal{B}) = V$ then $\mathcal{B}$ is a *spanning set* for V (or equivalently, $\mathcal{B}$ spans V). $\diamond$

REMARK 1.2.6. Strictly speaking, we should have defined $\operatorname{Span}(\mathcal{B})$ to be a subset of V, but it is easy to verify that it is a subspace. $\diamond$

Lemma 1.2.7. *Let $\mathcal{B}$ be a subset of a vector space V. The following are equivalent:*

(1) $\mathcal{B}$ is linearly independent and spans V.

(2) $\mathcal{B}$ is a maximal linearly independent subset of V.

(3) $\mathcal{B}$ is a minimal spanning set for V.

Proof (Outline). Suppose $\mathcal{B}$ is linearly independent and spans V. If $\mathcal{B} \subset \mathcal{B}'$, choose $v \in \mathcal{B}'$, $v \notin \mathcal{B}$. Since $\mathcal{B}$ spans V, v is a linear combination of elements of $\mathcal{B}$, and so $\mathcal{B}'$ is not linearly independent. Hence $\mathcal{B}$ is a maximal linearly independent subset of V. If $\mathcal{B}' \subset \mathcal{B}$, choose $v \in \mathcal{B}$, $v \notin \mathcal{B}'$. Since $\mathcal{B}$ is linearly independent, v is not in the subspace spanned by $\mathcal{B}'$, and hence $\mathcal{B}$ is a minimal spanning set for V.

Suppose that $\mathcal{B}$ is a maximal linearly independent subset of V. If $\mathcal{B}$ does not span V, choose any vector $v \in V$ that is not in the subspace spanned by $\mathcal{B}$. Then $\mathcal{B}' = \mathcal{B} \cup \{v\}$ would be linearly independent, contradicting maximality.

Suppose that $\mathcal{B}$ is a minimal spanning set for V. If $\mathcal{B}$ is not linearly independent, choose $v \in \mathcal{B}$ that is a linear combination of the other elements of $\mathcal{B}$. Then $\mathcal{B}' = \mathcal{B} - \{v\}$ would span V, contradicting minimality. $\square$

DEFINITION 1.2.8. A subset $\mathcal{B}$ of V satisfying the equivalent conditions of Lemma 1.2.7 is a *basis* of V. $\diamond$

Theorem 1.2.9. *Let V be a vector space and let $\mathcal{A}$ and $\mathcal{C}$ be subsets of V with $\mathcal{A} \subseteq \mathcal{C}$, $\mathcal{A}$ linearly independent, and $\mathcal{C}$ spanning V. Then there is a basis $\mathcal{B}$ of V with $\mathcal{A} \subseteq \mathcal{B} \subseteq \mathcal{C}$.*

Proof. This proof is an application of Zorn's Lemma. Let

$$\mathcal{Z} = \{\mathcal{B}' \mid \mathcal{A} \subseteq \mathcal{B}' \subseteq \mathcal{C},\ \mathcal{B}' \text{ linearly independent}\},$$

partially ordered by inclusion. $\mathcal{Z}$ is nonempty as $\mathcal{A} \in \mathcal{Z}$. Any chain (i.e., linearly ordered subset) of $\mathcal{Z}$ has a maximal element, its union. Then, by Zorn's Lemma, $\mathcal{Z}$ has a maximal element $\mathcal{B}$. We claim that $\mathcal{B}$ is a basis for V.

Certainly $\mathcal{B}$ is linearly independent, so we need only show that it spans V. Suppose not. Then there would be some $v \in \mathcal{C}$ not in the span of $\mathcal{B}$ (since if every $v \in \mathcal{C}$ were in the span of $\mathcal{B}$, then $\mathcal{B}$ would span V, because $\mathcal{C}$ spans V), and $\mathcal{B}^+ = \mathcal{B} \cup \{v\}$ would then be a linearly independent subset of $\mathcal{C}$ with $\mathcal{B} \subset \mathcal{B}^+$, contradicting maximality. $\square$

Corollary 1.2.10. *(1) Let $\mathcal{A}$ be any linearly independent subset of V. Then there is a basis $\mathcal{B}$ of V with $\mathcal{A} \subseteq \mathcal{B}$.*

(2) Let $\mathcal{C}$ be any spanning set for V. Then there is a basis $\mathcal{B}$ of V with $\mathcal{B} \subseteq \mathcal{C}$.

(3) Every vector space V has a basis $\mathcal{B}$.

Proof. (1) Apply Theorem 1.2.9 with $\mathcal{C} = V$.

(2) Apply Theorem 1.2.9 with $\mathcal{A} = \{\,\}$.

(3) Apply Theorem 1.2.9 with $\mathcal{A} = \{\,\}$ and $\mathcal{C} = V$. $\square$

We now show that the dimension of a vector space is well-defined. We first prove the following familiar result from elementary linear algebra, one that is useful and important in its own right.

Lemma 1.2.11. *A homogeneous system of m equations in n unknowns with $m < n$ has a nontrivial solution.*

Proof (Outline). We proceed by induction on m. Let the unknowns be $x_1, \ldots, x_n$. If $m = 0$, set $x_1 = 1, x_2 = \cdots = x_n = 0$.

Suppose the theorem is true for m and consider a system of $m + 1$ equations in $n > m + 1$ unknowns. If none of the equations involve x_1, the system has the solution $x_1 = 1$, $x_2 = \cdots = x_n = 0$. Otherwise, pick an equation involving x_1 (i.e., with the coefficient of x_1 nonzero) and subtract appropriate multiples of it from the other equations so that none of them involve x_1. Then the other equations in the transformed system are a system of $n - 1 > m$ equations in the variables $x_2, \ldots, x_n$. By induction it has a nontrivial solution for $x_2, \ldots, x_n$. Then solve the remaining equation for x_1. □

Lemma 1.2.12. *Let $\mathcal{B} = \{v_1, \ldots, v_m\}$ span V. Any subset $\mathcal{C}$ of V containing more than m vectors is linearly dependent.*

Proof. Let $\mathcal{C} = \{w_1, \ldots, w_n\}$ with $n > m$. (If $\mathcal{C}$ is infinite consider a finite subset containing $n > m$ elements.) For each $i = 1, \ldots, n$

$$w_i = \sum_{j=1}^{m} a_{ji} v_j.$$

We show that

$$0 = \sum_{i=1}^{m} c_i w_i$$

has a nontrivial solution (i.e., a solution with not all $c_i = 0$). We have

$$0 = \sum_{i=1}^{m} c_i w_i = \sum_{i=1}^{m} c_i \left(\sum_{j=1}^{n} a_{ji} v_j \right) = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_{ji} c_i \right) v_j$$

and this will be true if

$$0 = \sum_{i=1}^{n} a_{ji} c_i \quad \text{for each } j = 1, \ldots, m.$$

This is a system of m equations in the n unknowns $c_1, \ldots, c_n$ and so has a nontrivial solution by Lemma 1.2.11. □

In the following, we do not distinguish between cardinalities of infinite sets.

Theorem 1.2.13. *Let V be a vector space. Then any two bases of V have the same number of elements.*

Proof. Let V have bases $\mathcal{B}$ and $\mathcal{C}$. If both $\mathcal{B}$ and $\mathcal{C}$ are infinite, we are done. Assume not. Let $\mathcal{B}$ have m elements and $\mathcal{C}$ have n elements. Since $\mathcal{B}$ and $\mathcal{C}$ are bases, both $\mathcal{B}$ and $\mathcal{C}$ span V and both $\mathcal{B}$ and $\mathcal{C}$ are linearly independent. Applying Lemma 1.2.12 we see that $m \leq n$. Interchanging $\mathcal{B}$ and $\mathcal{C}$ we see that $n \leq m$. Hence $m = n$. □

Given this theorem we may make the following very important definition.

DEFINITION 1.2.14. Let V be a vector space. The *dimension* of V, $\dim(V)$, is the number of vectors in any basis of V, $\dim(V) \in \{0, 1, 2, \ldots\} \cup \{\infty\}$. ◇

REMARK 1.2.15. The vector space $V = \{0\}$ has basis $\{\ \}$ and hence dimension 0. ◇

While we will be considering both finite-dimensional and infinite-dimensional vector spaces, we adopt the convention that when we write "Let V be an n-dimensional vector space" or "Let V be a vector space of dimension n" we always mean that V is finite-dimensional, so that n is a nonnegative integer.

Theorem 1.2.16. *Let V be a vector space of dimension n. Let $\mathcal{C}$ be a subset of V consisting of m elements.*

(1) If $m > n$ then $\mathcal{C}$ is not linearly independent (and hence is not a basis of V).

(2) If $m < n$ then $\mathcal{C}$ does not span V (and hence is not a basis of V).

(3) If $m = n$ the following are equivalent:

(a) $\mathcal{C}$ is a basis of V.
(b) $\mathcal{C}$ spans V.
(c) $\mathcal{C}$ is linearly independent.

Proof. Let $\mathcal{B}$ be a basis of V, consisting necessarily of n elements.

(1) $\mathcal{B}$ spans V so, applying Lemma 1.2.12, if $\mathcal{C}$ has $m > n$ elements then $\mathcal{C}$ is not linearly independent.

(2) Suppose $\mathcal{C}$ spans V. Then, applying Lemma 1.2.12, $\mathcal{B}$ has $n > m$ elements so cannot be linearly independent, contradicting $\mathcal{B}$ being a basis of V.

(3) By definition, (a) is equivalent to (b) and (c), so (a) implies (b) and (a) implies (c). Suppose (b) is true. By Corollary 1.2.10, $\mathcal{C}$ has a subset of $\mathcal{C}'$ of $m \leq n$ elements that is a basis of V. By Theorem 1.2.13, $m = n$, so $\mathcal{C}' = \mathcal{C}$. Suppose (c) is true. By Corollary 1.2.10, $\mathcal{C}$ has a superset of $\mathcal{C}'$ of $m \geq n$ elements that is a basis of V. By Theorem 1.2.13, $m = n$, so $\mathcal{C}' = \mathcal{C}$. □

REMARK 1.2.17. A good mathematical theory is one that reduces hard problems to easy problems. Linear algebra is such a theory, as it reduces many problems to counting. Theorem 1.2.16 is a typical example. Suppose we want to know whether a set $\mathcal{C}$ is a basis of an n-dimensional vector space V. We count the number of elements of $\mathcal{C}$, say m. If we get the "wrong" number, i.e., if $m \neq n$, then we know $\mathcal{C}$ is not a basis of V. If we get the "right" number, i.e., if $m = n$, then $\mathcal{C}$ may or may not be a basis of V. While there are normally two conditions to check, that $\mathcal{C}$ is linearly independent and that $\mathcal{C}$ spans V, it suffices to check either one of the conditions. If that one is satisfied, the other one is automatic. ◇

EXAMPLE 1.2.18. (1) $\mathbb{F}^n$ has basis $\mathcal{E}_n$, the *standard basis*, given by $\mathcal{E}_n = \{e_{1,n}, e_{2,n}, \ldots, e_{n,n}\}$ where $e_{i,n}$ is the vector in $\mathbb{F}^n$ whose ith entry is 1 and all of whose other entries are 0.

$\mathbb{F}^\infty$ has basis $\mathcal{E}_\infty = \{e_{1,\infty}, e_{2,\infty}, \ldots\}$ defined analogously. We will often write $\mathcal{E}$ for $\mathcal{E}_n$ and e_i for $e_{i,n}$ when n is understood. Thus $\mathbb{F}^n$ has dimension n and $\mathbb{F}^\infty$ is infinite-dimensional.

(2) $\mathbb{F}^\infty$ is a proper subspace of $\mathbb{F}^{\infty\infty}$. By Corollary 1.2.10, $\mathbb{F}^{\infty\infty}$ has a basis, but it is impossible to write one down in a constructive way.

(3) The vector space of polynomials of degree at most n with coefficients in $\mathbb{F}$, $P_n(\mathbb{F}) = \{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in \mathbb{F}\}$, has basis $\{1, x, \ldots, x^n\}$ and dimension $n + 1$.

(4) The vector space of polynomials of arbitrary degree with coefficients in $\mathbb{F}$, $P(\mathbb{F}) = \{a_0 + a_1x + a_2x^2 + \cdots \mid a_i \in \mathbb{F}\}$, has basis $\{1, x, x^2, \ldots\}$ and is infinite-dimensional.

(5) Let $p_i(x)$ be any polynomial of degree i. Then $\{p_0(x), p_1(x), \ldots, p_n(x)\}$ is a basis for $P_n(\mathbb{F})$, and $\{p_0(x), p_1(x), p_2(x), \ldots\}$ is a basis for $P(\mathbb{F})$.

(6) $\mathrm{M}_{m,n}(\mathbb{F})$ has dimension mn, with basis given by the mn distinct matrices each of which has a single entry of 1 and all other entries 0.

(7) If $V = \{f : \mathcal{A} \to \mathbb{F}\}$ for some finite set $\mathcal{A} = \{a_1, \ldots, a_n\}$, then V is n-dimensional with basis $\{b_1, \ldots, b_n\}$ where b_i is the function defined by $b_i(a_j) = 1$ if $j = i$ and 0 if $j \neq i$.

(8) Let $\mathbb{E}$ be an extension of $\mathbb{F}$ and let $\alpha \in \mathbb{E}$ be *algebraic*, i.e., α is a root of a (necessarily unique) monic irreducible polynomial $f(x) \in \mathbb{F}[x]$. Let $f(x)$ have degree n. Then $\mathbb{F}(\alpha)$ defined by $\mathbb{F}(\alpha) = \{p(\alpha) \mid p(x) \in \mathbb{F}[x]\}$ is a subfield of $\mathbb{E}$ with basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ and so is an extension of $\mathbb{F}$ of degree n. $\diamond$

REMARK 1.2.19. If we consider cardinalities of infinite sets, we see that $\mathbb{F}^{\infty}$ is countably infinite-dimensional. On the other hand, $\mathbb{F}^{\infty\infty}$ is uncountably infinite-dimensional. If $\mathbb{F}$ is a countable field, this is easy to see: $\mathbb{F}^{\infty\infty}$ is uncountable. For $\mathbb{F}$ uncountable, we need a more subtle argument. We will give it here, although it presupposes results from Chapter 4. For convenience we consider ${}^{r}\mathbb{F}^{\infty\infty}$ instead, but clearly ${}^{r}\mathbb{F}^{\infty\infty}$ and $\mathbb{F}^{\infty\infty}$ are isomorphic.

Consider $\mathbf{R} : {}^{r}\mathbb{F}^{\infty\infty} \to {}^{r}\mathbb{F}^{\infty\infty}$. Observe that for any $a \in \mathbb{F}$, $\mathbf{R}$ has eigenvalue a with associated eigenvector $v_a = [1, a, a^2, a^3, \ldots]$. But eigenvectors associated to distinct eigenvalues are linearly independent. (See Lemma 4.2.5.) $\diamond$

Corollary 1.2.20. *Let W be a subspace of V. Then* $\dim(W) \leq \dim(V)$. *If* $\dim(V)$ *is finite, then* $\dim(W) = \dim(V)$ *if and only if* $W = V$.

Proof. Apply Theorem 1.2.16 with $\mathcal{C}$ a basis of W. $\square$

We have the following useful characterization of a basis.

Lemma 1.2.21. *Let V be a vector space and let $\mathcal{B} = \{v_i\}$ be a set of vectors in V. Then $\mathcal{B}$ is a basis of V if and only if every $v \in V$ can be written uniquely as $v = \sum c_i v_i$ for $c_i \in \mathbb{F}$, all but finitely many zero.*

Proof. Suppose $\mathcal{B}$ is a basis of V. Then $\mathcal{B}$ spans V, so any $v \in V$ can be written as $v = \sum c_i v_i$. We show this expression for v is unique. Suppose we have $v = \sum c_i' v_i$. Then $0 = \sum (c_i' - c_i) v_i$. But $\mathcal{B}$ is linearly independent, so $c_i' - c_i = 0$ and $c_i' = c_i$ for each i.

Conversely, suppose every $v \in V$ can be written as $v = \sum c_i v_i$ in a unique way. This clearly implies that $\mathcal{B}$ spans V. To show $\mathcal{B}$ is linearly independent, suppose $0 = \sum c_i v_i$. Certainly $0 = \sum 0 v_i$. By the uniqueness of the expression, $c_i = 0$ for each i. $\square$

This lemma will be the basis for our definition of coordinates in the next chapter. It also has immediate applications. First, an illustrative use, and then some general results.

EXAMPLE 1.2.22. (1) Let $V = P_{n-1}(\mathbb{R})$. For any real number a,

$$\mathcal{B} = \{1, x-a, (x-a)^2, \dots, (x-a)^{n-1}\}$$

is a basis of V, so any polynomial $p(x) \in V$ can be written uniquely as a linear combination of elements of $\mathcal{B}$,

$$p(x) = \sum_{c=0}^{n-1} c_i (x-a)^i .$$

Solving for the coefficients c_i we obtain the familiar Taylor expansion

$$p(x) = \sum_{i=0}^{n-1} \frac{p^{(i)}(a)}{i!} (x-a)^i .$$

(2) Let $V = P_{n-1}(\mathbb{R})$. For any set of pairwise distinct real numbers $\{a_1, \dots, a_n\}$,

$$\begin{aligned}\mathcal{B} = \{&(x-a_2)(x-a_3)\cdots(x-a_n), (x-a_1)(x-a_3)\cdots(x-a_n), \dots, \\ &(x-a_1)(x-a_n)\cdots(x-a_{n-1})\}\end{aligned}$$

is a basis of V, so any polynomial $p(x) \in V$ can be written uniquely as a linear combination of elements of $\mathcal{B}$,

$$p(x) = \sum_{i=1}^{n} c_i \big(x-a_1\big)\cdots\big(x-a_{i-1}\big)\big(x-a_{i+1}\big)\cdots\big(x-a_n\big).$$

Solving for the coefficients c_i we obtain the familiar Lagrange interpolation formula

$$\begin{aligned}p(x) = \sum_{i=1}^{n} &\frac{p\big(a_i\big)}{\big(a_i-a_1\big)\cdots\big(a_i-a_{i-1}\big)\big(a_i-a_{i+1}\big)\cdots\big(a_i-a_n\big)} \\ &\times \big(x-a_1\big)\cdots\big(x-a_{i-1}\big)\big(x-a_{i+1}\big)\cdots\big(x-a_n\big). \qquad \diamond\end{aligned}$$

So far in this section we have considered individual vector spaces. Now we consider pairs of vector spaces V and W and linear transformations between them.

Lemma 1.2.23. *(1) A linear transformation $\mathcal{T} : V \to W$ is specified by its values on any basis of V.*

(2) If $\{v_i\}$ is a basis of V and $\{w_i\}$ is an arbitrary set of vectors in W, then there is a unique linear transformation $\mathcal{T} : V \to W$ with $\mathcal{T}(v_i) = w_i$ for each i.

Proof. (1) Let $\mathcal{B} = \{v_1, v_2, \ldots\}$ be a basis of V and suppose that $\mathcal{T} : V \to W$ and $\mathcal{T}' : V \to W$ are two linear transformations that agree on each v_i. Let $v \in V$ be arbitrary. We may write $v = \sum c_i v_i$, and then

$$\begin{aligned} \mathcal{T}(v) &= \mathcal{T}\Big(\sum c_i v_i\Big) = \sum c_i \mathcal{T}\big(v_i\big) = \sum c_i \mathcal{T}'\big(v_i\big) \\ &= \mathcal{T}'\Big(\sum c_i v_i\Big) = \mathcal{T}'(v). \end{aligned}$$

(2) Let $\{w_1, w_2, \ldots\}$ be an arbitrary set of vectors in W, and define $\mathcal{T}$ as follows: For any $v \in V$, write $v = \sum c_i v_i$ and let

$$\mathcal{T}(v) = \sum c_i \mathcal{T}(v_i) = \sum c_i w_i.$$

Since the expression for v is unique, this gives a well-defined function $\mathcal{T} : V \to W$ with $\mathcal{T}(v_i) = w_i$ for each i. It is routine to check that $\mathcal{T}$ is a linear transformation. Then $\mathcal{T}$ is unique by part (1). □

Lemma 1.2.24. *Let $\mathcal{T} : V \to W$ be a linear transformation and let $\mathcal{B} = \{v_1, v_2, \ldots\}$ be a basis of V. Let $\mathcal{C} = \{w_1, w_2, \ldots\} = \{\mathcal{T}(v_1), \mathcal{T}(v_2), \ldots\}$. Then $\mathcal{T}$ is an isomorphism if and only if $\mathcal{C}$ is a basis of W.*

Proof. First suppose $\mathcal{T}$ is an isomorphism.

To show $\mathcal{C}$ spans W, let $w \in W$ be arbitrary. Since $\mathcal{T}$ is an epimorphism, $w = \mathcal{T}(v)$ for some v. As $\mathcal{B}$ is a basis of V, it spans V, so we may write $v = \sum c_i v_i$ for some $\{c_i\}$. Then

$$w = \mathcal{T}(v) = \mathcal{T}(\sum c_i v_i) = \sum c_i \mathcal{T}(v_i) = \sum c_i w_i.$$

To show $\mathcal{C}$ is linearly independent, suppose $\sum c_i w_i = 0$. Then

$$0 = \sum c_i w_i = \sum c_i \mathcal{T}\big(v_i\big) = \mathcal{T}\Big(\sum c_i v_i\Big) = \mathcal{T}(v) \text{ where } v = \sum c_i v_i.$$

Since $\mathcal{T}$ is a monomorphism, we must have $v = 0$. Thus $0 = \sum c_i v_i$. As $\mathcal{B}$ is a basis of V, it is linearly independent, so $c_i = 0$ for all i.

Conversely, suppose $\mathcal{C}$ is a basis of W. By Lemma 1.2.23(2), we may define a linear transformation $\mathcal{S} : W \to V$ by $\mathcal{S}(w_i) = v_i$. Then $\mathcal{S}\mathcal{T}(v_i) = v_i$ for each i so, by Lemma 1.2.23(1), $\mathcal{S}\mathcal{T}$ is the identity on V. Similarly $\mathcal{T}\mathcal{S}$ is the identity on W so $\mathcal{S}$ and $\mathcal{T}$ are inverse isomorphisms. □

1.3 Dimension counting and applications

We have mentioned in Remark 1.2.17 that linear algebra enables us to reduce many problems to counting. We gave examples of this in counting elements of sets of vectors in the last section. We begin this section by deriving a basic dimension-counting theorem for linear transformations, Theorem 1.3.1. The usefulness of this result cannot be overemphasized. We present one of its important applications in Corollary 1.3.2, and we give a typical example of its use in Example 1.3.10. It is used throughout linear algebra.

Here is the basic result about dimension counting.

Theorem 1.3.1. *Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to W$ be a linear transformation. Then*

$$\dim\big(\operatorname{Ker}(\mathcal{T})\big) + \dim\big(\operatorname{Im}(\mathcal{T})\big) = \dim(V).$$

Proof. Let $k = \dim(\operatorname{Ker}(\mathcal{T}))$ and $n = \dim(V)$. Let $\{v_1, \ldots, v_k\}$ be a basis of $\operatorname{Ker}(\mathcal{T})$. By Corollary 1.2.10, $\{v_1, \ldots, v_k\}$ extends to a basis $\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$ of V. We claim that $\mathcal{B} = \{\mathcal{T}(v_{k+1}), \ldots, \mathcal{T}(v_n)\}$ is a basis of $\operatorname{Im}(\mathcal{T})$.

First let us see that $\mathcal{B}$ spans $\operatorname{Im}(\mathcal{T})$. If $w \in \operatorname{Im}(\mathcal{T})$, then $w = \mathcal{T}(v)$ for some $v \in V$. Let $v = \sum c_i v_i$. Then

$$\begin{aligned}\mathcal{T}(v) &= \sum c_i \mathcal{T}\big(v_i\big) = \sum_{i=1}^{k} c_i \mathcal{T}\big(v_i\big) + \sum_{i=k+1}^{n} c_i \mathcal{T}\big(v_i\big) \\ &= \sum_{i=k+1}^{n} c_i \mathcal{T}\big(v_i\big)\end{aligned}$$

as $\mathcal{T}(v_i) = \cdots = \mathcal{T}(v_k) = 0$ since $v_1, \ldots, v_k \in \operatorname{Ker}(\mathcal{T})$.

Second, let us see that $\mathcal{B}$ is linearly independent. Suppose that

$$\sum_{i=k+1}^{n} c_i \mathcal{T}\big(v_i\big) = 0.$$

Then

$$\mathcal{T}\left(\sum_{i=k+1}^{n} c_i v_i\right) = 0,$$

so

$$\sum_{i=k+1}^{n} c_i v_i \in \operatorname{Ker}(\mathcal{T}),$$

and hence for some $c_1, \ldots, c_k$, we have

$$\sum_{i=k+1}^{n} c_i v_i = \sum_{i=1}^{k} c_i v_i .$$

Then

$$\sum_{i=1}^{k} (-c_i) v_i + \sum_{i=k+1}^{n} c_i v_i = 0,$$

so by the linear independence of $\{v_1, \ldots, v_n\}$, $c_i = 0$ for each i.

Thus $\dim(\operatorname{Im}(\mathcal{T})) = n - k$ and indeed $k + (n - k) = n$. □

Corollary 1.3.2. *Let $\mathcal{T} : V \to W$ be a linear transformation between vector spaces of the same finite dimension n. The following are equivalent:*

(1) $\mathcal{T}$ is an isomorphism.

(2) $\mathcal{T}$ is an epimorphism.

(3) $\mathcal{T}$ is a monomorphism.

Proof. Clearly (1) implies (2) and (3).

Suppose (2) is true. Then, by Theorem 1.3.1,

$$\begin{aligned} \dim\left(\operatorname{Ker}(\mathcal{T})\right) &= \dim(V) - \dim\left(\operatorname{Im}(\mathcal{T})\right) \\ &= \dim(W) - \dim\left(\operatorname{Im}(\mathcal{T})\right) = n - n = 0, \end{aligned}$$

so $\operatorname{Ker}(\mathcal{T}) = \{0\}$ and $\mathcal{T}$ is a monomorphism, yielding (3) and hence (1).

Suppose (3) is true. Then, by Theorem 1.3.1,

$$\begin{aligned} \dim\left(\operatorname{Im}(\mathcal{T})\right) &= \dim(V) - \dim\left(\operatorname{Ker}(\mathcal{T})\right) \\ &= \dim(W) - \dim\left(\operatorname{Ker}(\mathcal{T})\right) = n - 0 = 0, \end{aligned}$$

so $\operatorname{Im}(\mathcal{T}) = W$ and $\mathcal{T}$ is an epimorphism, yielding (2) and hence (1). □

Corollary 1.3.3. *Let A be an n-by-n matrix. The following are equivalent:*

(1) A is invertible.

(2) *There is an n-by-n matrix B with $AB = I$.*

(3) *There is an n-by-n matrix B with $BA = I$.*

In this situation, $B = A^{-1}$.

Proof. Apply Corollary 1.3.2 to the linear transformation $\mathcal{T}_A$. If A is invertible and $AB = I$, then $B = IB = A^{-1}(AB) = A^{-1}I = A^{-1}$, and similarly if $BA = I$. $\square$

EXAMPLE 1.3.4. Corollary 1.3.2 is false in the infinite-dimensional case:

(1) Let $V = {}^r\mathbb{F}^{\infty\infty}$ and consider left shift $\mathbf{L}$ and right shift $\mathbf{R}$. $\mathbf{L}$ is an epimorphism but not a monomorphism, while $\mathbf{R}$ is a monomorphism but not an epimorphism. We see that $\mathbf{L} \circ \mathbf{R} = \mathcal{I}$ (so $\mathbf{R}$ is a right inverse for $\mathbf{L}$ and $\mathbf{L}$ is a left inverse for $\mathbf{R}$) but $\mathbf{R} \circ \mathbf{L} \neq \mathcal{I}$ (and neither $\mathbf{L}$ nor $\mathbf{R}$ is invertible).

(2) Let $V = C^\infty(\mathbb{R})$. Then $\mathbf{D} : V \to V$ and $\mathbf{I}_a : V \to V$ are linear transformations that are not invertible, but $\mathbf{D} \circ \mathbf{I}_a$ is the identity. $\diamond$

REMARK 1.3.5. We are not in general considering cardinalities of infinite sets. But we remark that two vector spaces V and W are isomorphic if and only if they have bases of the same cardinality, as we see from Lemma 1.2.23 and Lemma 1.2.24. $\diamond$

Corollary 1.3.6. *Let V be a vector space of dimension m and let W be a vector space of dimension n.*

(1) *If $m < n$ then no linear transformation $\mathcal{T} : V \to W$ can be an epimorphism.*

(2) *If $m > n$ then no linear transformation $\mathcal{T} : V \to W$ can be a monomorphism.*

(3) *V and W are isomorphic if and only if $m = n$. In particular, every n-dimensional vector space V is isomorphic to $\mathbb{F}^n$.*

Proof. (1) In this case, $\dim(\mathrm{Im}(\mathcal{T})) \leq m < n$ so $\mathcal{T}$ is not an epimorphism.

(2) In this case, $\dim(\mathrm{Ker}(\mathcal{T})) \geq m - n > 0$ so $\mathcal{T}$ is not a monomorphism.

(3) Parts (1) and (2) show that if $m \neq n$, then V and W are not isomorphic. If $m = n$, choose a basis $\{v_1, \ldots, v_m\}$ of V and a basis $\{w_1, \ldots, w_m\}$ of W. By Lemma 1.2.23, there is a unique linear transformation $\mathcal{T}$ determined by $\mathcal{T}(v_i) = w_i$ for each i, and by Lemma 1.2.24 $\mathcal{T}$ is an isomorphism. $\square$

Corollary 1.3.7. *Let A be an n-by-n matrix. The following are equivalent:*

(1) A is invertible.

(1′) The equation $Ax = b$ has a unique solution for every $b \in \mathbb{F}^n$.

(2) The equation $Ax = b$ has a solution for every $b \in \mathbb{F}^n$.

(3) The equation $Ax = 0$ has only the trivial solution $x = 0$.

Proof. This is simply a translation of Corollary 1.3.2 into matrix language.

We emphasize that this one-sentence proof is the "right" proof of the equivalence of these properties. For the reader who would like to see a more computational proof, we shall prove directly that (1) and (1′) are equivalent. Before doing so we also observe that their equivalence does not involve dimension counting. It is their equivalence with properties (2) and (3) that does. It is possible to prove this equivalence without using dimension counting, and this is often done in elementary texts, but that is most certainly the "wrong" proof as it is a manipulative proof that obscures the ideas.

(1) ⇒(1′): Suppose A is invertible. Let $x_0 = A^{-1}b$. Then $Ax_0 = A(A^{-1}b) = b$ so x_0 is the solution of $Ax = b$. If x_1 any other solution, then $Ax_1 = b$, $A^{-1}(Ax_1) = A^{-1}b$, $x_1 = A^{-1}b = x_0$, so x_0 is the unique solution.

(1′) ⇒(1): Let b_i be a solution of $Ax = e_i$ for $i = 1, \ldots, n$, which exists by hypothesis. Let $B = [b_1 \mid b_2 \mid \cdots \mid b_n]$. Then $AB = [e_1 \mid e_2 \mid \cdots \mid e_n] = I$. We show that $BA = I$ as well. (That comes from Corollary 1.3.3, but we are trying to prove it without using Theorem 1.3.1.) Let $f_i = Ae_i$, $i = 1, \ldots, n$. Then $Ax = f_i$ evidently has the solution $x_0 = e_i$. It also has the solution $x_1 = BAe_i$ as

$$A\big(BAe_i\big) = (AB)\big(Ae_i\big) = I\big(Ae_i\big) = Ae_i = f_i.$$

By hypothesis, $Ax = f_i$ has a unique solution, so $BAe_i = e_i$ for each i, giving $BA = [e_1|e_2|\cdots|e_n] = I$. □

As another application of Theorem 1.3.1, we prove the following familiar theorem from elementary linear algebra.

Theorem 1.3.8. *Let A be an m-by-n matrix. Then the row rank of A and the column rank of A are equal.*

Proof. For a matrix C, the image of the linear transformation $\mathcal{T}_C$ is simply the column space of C.

Let B be a matrix in (reduced) row echelon form. The nonzero rows of B are a basis for the row space of B. Each of these rows has a "leading" entry of 1, and it is easy to check that the columns of B containing those leading 1's are a basis for the column space of B. Thus if B is in (reduced) row echelon form, its row rank and column rank are equal.

Thus if B has column rank k, then $\dim(\operatorname{Im}(\mathcal{T}_B)) = k$ and hence by Theorem 1.3.1 $\dim(\operatorname{Ker}(\mathcal{T}_B)) = n - k$.

Our original matrix A is row-equivalent to a (unique) matrix B in (reduced) row echelon form, so A and B may be obtained from each other by a sequence of row operations. Row operations do not change the row space of a matrix, so if B has row rank k, then A has row rank k as well. Row operations change the column space of A, so we can not use the column space directly. However, they do not change $\operatorname{Ker}(\mathcal{T}_A)$. (That is why we usually do them, to solve $Ax = 0$.) Thus $\operatorname{Ker}(\mathcal{T}_B) = \operatorname{Ker}(\mathcal{T}_A)$ and so $\dim(\operatorname{Ker}(\mathcal{T}_A)) = n - k$. Then by Theorem 1.3.1 again, $\dim(\operatorname{Im}(\mathcal{T}_A)) = k$, i.e., A has column rank k, the same as its row rank, and we are done. □

REMARK 1.3.9. This proof is a correct proof, but is the "wrong" proof, as it shows the equality without showing why it is true. We will see the "right" proof in Theorem 2.4.7 below. That proof is considerably more complicated, so we have presented this easy proof. ◇

EXAMPLE 1.3.10. Let $V = P_{n-1}(\mathbb{R})$ for fixed n. Let $a_1, \dots, a_k$ be distinct real numbers and let $e_1, \dots, e_k$ be non-negative integers with $(e_1 + 1) + \cdots + (e_k + 1) = n$. Define $\mathcal{T} : V \to \mathbb{R}^n$ by

$$\mathcal{T}\big(f(x)\big) = \begin{bmatrix} f(a_1) \\ \vdots \\ f^{(e_1)}(a_1) \\ \vdots \\ f(a_k) \\ \vdots \\ f^{(e_k)}(a_k) \end{bmatrix}.$$

If $f(x) \in \operatorname{Ker}(\mathcal{T})$, then $f^{(i)}(a_i) = 0$ for $i = 0, \dots, e_i$, so $f(x)$ is divisible by $(x - a_i)^{e_i+1}$ for each i. Thus $f(x)$ divisible by $(x - a_1)^{e_1+1} \cdots (x - a_k)^{e_k+1}$, a polynomial of degree n. Since $f(x)$ has degree at most $n-1$, we conclude $f(x)$ is the 0 polynomial. Thus $\operatorname{Ker}(\mathcal{T}) = \{0\}$. Since $\dim V = n$ we conclude from Corollary 1.3.2 that $\mathcal{T}$ is an isomorphism. Thus for any

n real numbers $b_1^0, \ldots, b_1^{e_1}, \ldots, b_k^0, \ldots, b_k^{e_k}$ there is a unique polynomial $f(x)$ of degree at most $n-1$ with $f^{(j)}(a_i) = b_i^j$ for $j = 0, \ldots, e_i$ and for $i = 1, \ldots, k$. (This example generalizes Example 1.2.22(1), where $k = 1$, and Example 1.2.22(2), where $e_i = 0$ for each i.) $\Diamond$

Let us now see that the numerical relation in Theorem 1.3.1 is the only restriction on the kernel and image of a linear transformation.

Theorem 1.3.11. *Let V and W be vector spaces with* $\dim V = n$. *Let V_1 be a k-dimensional subspace of V and let W_1 be an $(n-k)$-dimensional subspace of W. Then there is a linear transformation $\mathcal{T} : V \to W$ with* $\operatorname{Ker}(\mathcal{T}) = V_1$ *and* $\operatorname{Im}(\mathcal{T}) = V_2$.

Proof. Let $\mathcal{B}_1 = \{v_1, \ldots, v_k\}$ be a basis of V_1 and extend $\mathcal{B}_1$ to $\mathcal{B} = \{v_1, \ldots, v_n\}$, a basis of V. Let $\mathcal{C}_1 = \{w_{k+1}, \ldots, w_n\}$ be a basis of W_1. Define $\mathcal{T} : V \to W$ by $\mathcal{T}(v_i) = 0$ for $i = 1, \ldots, k$ and $\mathcal{T}(v_i) = w_i$ for $i = k+1, \ldots, n$. $\square$

REMARK 1.3.12. In this section we have stressed the importance and utility of counting arguments. Here is a further application:

A philosopher, an engineer, a physicist, and a mathematician are sitting at a sidewalk cafe having coffee. On the opposite side of the street there is an empty building. They see two people go into the building. A while later they see three come out.

The philosopher concludes "There must have been someone in the building to start with."

The engineer concludes "We must have miscounted."

The physicist concludes "There must be a rear entrance."

The mathematician concludes "If another person goes in, the building will be empty." $\Diamond$

1.4 SUBSPACES AND DIRECT SUM DECOMPOSITIONS

We now generalize the notion of spanning sets, linearly independent sets, and bases. We introduce the notions of V being a sum of subspaces $W_1, \ldots,$ W_k, of the subspaces $W_1, \ldots, W_k$ being independent, and of V being the direct sum of the subspaces $W_1, \ldots, W_k$. In the special case where each $W_1, \ldots, W_k$ consists of the multiples of a single nonzero vector v_i, let $\mathcal{B} = \{v_1, \ldots, v_k\}$. Then V is the sum of $W_1, \ldots, W_k$ if and only if $\mathcal{B}$ spans

V; the subspaces $W_1, \ldots, W_k$ are independent if and only if $\mathcal{B}$ is linearly independent; and V is the direct sum of $W_1, \ldots, W_k$ if and only if $\mathcal{B}$ is a basis of V. Thus our work here generalizes part of our work in Section 1.2, but this generalization will be essential for future developments. In most cases we omit the proofs as they are very similar to the ones we have given.

DEFINITION 1.4.1. Let V be a vector space and let $\{W_1, \ldots, W_k\}$ be a set of subspaces of V. Then V is the *sum* $V = W_1 + \cdots + W_k$ if every $v \in V$ can be written as $v = w_1 + \ldots + w_k$ where $w_i \in W_i$. $\diamond$

DEFINITION 1.4.2. Let V be a vector space and let $\{W_1, \ldots, W_k\}$ be a set of subspaces of V. This set of spaces is *independent* if $0 = w_1 + \cdots + w_k$ with $w_i \in W_i$ implies $w_i = 0$ for each i. $\diamond$

DEFINITION 1.4.3. Let V be a vector space and let $\{W_1, \ldots, W_k\}$ be a set of subspaces of V. Then V is the direct sum $V = W_1 \oplus \cdots \oplus W_k$ if

(1) $V = W_1 + \cdots + W_k$, and

(2) $\{W_1, \ldots, W_k\}$ is independent. $\diamond$

We have the following equivalent criterion.

Lemma 1.4.4. *Let $\{W_1, \ldots, W_k\}$ be a set of subspaces of V. This set of subspaces is independent if and only if $W_i \cap (W_1 + \cdots + W_{i-1} + W_{i+1} + \cdots + W_k) = \{0\}$ for each i.*

If we only have two subspaces $\{W_1, W_2\}$ this condition simply states $W_1 \cap W_2 = \{0\}$. If we have more than two subspaces, it is stronger than the condition $W_i \cap W_j = \{0\}$ for $i \neq j$, and it is the stronger condition we need for independence, not the weaker one.

Lemma 1.4.5. *Let V be a vector space and let $\{W_1, \ldots, W_k\}$ be a set of subspaces of V. Then V is the direct sum $V = W_1 \oplus \cdots \oplus W_k$ if and only if $v \in V$ can be written as $v = w_1 + \cdots + w_k$ with $w_i \in W_i$, for each i, in a unique way.*

Lemma 1.4.6. *Let V be a vector space and let $\{W_1, \ldots, W_k\}$ be a set of subspaces of V. Let $\mathcal{B}_i$ be a basis of W_i, for each i, and let $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_k$. Then*

(1) $\mathcal{B}$ spans V if and only if $V = W_1 + \cdots + W_k$.

(2) $\mathcal{B}$ is linearly independent if and only if $\{W_1, \ldots, W_k\}$ is independent.

(3) $\mathcal{B}$ is a basis for V if and only if $V = W_1 \oplus \cdots \oplus W_k$.

Corollary 1.4.7. *Let V be a finite-dimensional vector space and let $\{W_1, \ldots, W_k\}$ be a set of subspaces with $V = W_1 \oplus \cdots \oplus W_k$. Then* $\dim(V) = \dim(W_1) + \cdots + \dim(W_k)$.

Corollary 1.4.8. *Let V be a vector space of dimension n and let $\{W_1, \ldots, W_k\}$ be a set of subspaces. Let $n_i = \dim(W_i)$.*

(1) If $n_1 + \cdots + n_k > n$ then $\{W_1, \ldots, W_k\}$ is not independent.

(2) If $n_1 + \cdots + n_k < n$ then $V \neq W_1 + \cdots + W_k$.

(3) If $n_1 + \cdots + n_k = n$ the following are equivalent:

(a) $V = W_1 \oplus \cdots \oplus W_k$.
(b) $V = W_1 + \cdots + W_k$
(c) $\{W_1, \ldots, W_k\}$ is independent.

DEFINITION 1.4.9. Let V be a vector space and let W_1 be a subspace of V. Then W_2 is a *complement* of W_1 if $V = W_1 \oplus W_2$. ◇

Lemma 1.4.10. *Let V be a vector space and let W_1 be a subspace of V. Then W_1 has a complement W_2.*

Proof. Let $\mathcal{B}_1$ be a basis of W_1. Then $\mathcal{B}_1$ is linearly independent, so by Corollary 1.2.10 there is a basis $\mathcal{B}$ of V containing $\mathcal{B}_1$. Let $\mathcal{B}_2 = \mathcal{B} - \mathcal{B}_1$. Then $\mathcal{B}_2$ is a subset of V, so is linearly independent. Let W_2 be the span of $\mathcal{B}_2$. Then $\mathcal{B}_2$ is a linearly independent spanning set for W_2, i.e., a basis for W_2, and so by Lemma 1.4.6 $V = W_1 \oplus W_2$, and hence W_2 is a complement of W_1. □

REMARK 1.4.11. Except when $W_1 = \{0\}$ (where $W_2 = V$) or $W_1 = V$ (where $W_1 = \{0\}$), the subspace W_2 is *never* unique. We can always choose a different way of extending $\mathcal{B}_1$ to a basis of V, in order to obtain a different W_2. Thus W_2 is *a*, not *the*, complement of W_1. ◇

1.5 AFFINE SUBSPACES AND QUOTIENT SPACES

For the reader familiar with these notions, we can summarize much of what we are about to do in this section in a paragraph: Let W be a subspace of V. Then W is a subgroup of V, regarded as an additive group. An affine subspace of V parallel to W is simply a coset of W in V, and the quotient space V/W is simply the group quotient V/W, which also has a vector space structure.

But we will not presume this familiarity, and instead proceed "from scratch".

We begin with a generalization of the notion of a subspace of a vector space.

DEFINITION 1.5.1. Let V be a vector space. A subset X of V is an *affine subspace* if for some element x_0 of X,

$$U = \{x' - x_0 \mid x' \in X\}$$

is a subspace of V. In this situation X is *parallel* to U. ◇

The definition makes the element x_0 of X look distinguished, but that is not the case.

Lemma 1.5.2. *Let X be affine subspace of V parallel to the subspace U. Then for any element x of X,*

$$U = \{x' - x \mid x' \in X\}.$$

REMARK 1.5.3. An affine subspace X of V is a subspace of V if and only if $0 \in X$. ◇

An alternative way of looking at affine subspaces is given by the following result.

Proposition 1.5.4. *A subset X of V is an affine subspace of V parallel to the subspace U of V if and only if for some, and hence for every, element x of X,*

$$X = x + U = \{x + u \mid u \in U\}.$$

There is a natural definition of the dimension of an affine subspace.

DEFINITION 1.5.5. Let X be affine subspace of V parallel to the subspace U. Then the *dimension* of X is $\dim(X) = \dim(U)$. ◇

Proposition 1.5.6. *Let X be an affine subspace of V parallel to the subspace U of V. Let x_0 be an element of X and let $\{u_1, u_2, \ldots\}$ be a basis of U. Then any element x of X may be written uniquely as*

$$x = x_0 + \sum c_i u_i$$

for some scalars $\{c_1, c_2, \ldots\}$.

The most important way in which affine subspaces arise is as follows.

Theorem 1.5.7. *Let $\mathcal{T} : V \to W$ be a linear transformation and let $w_0 \in W$ be an arbitrary element of W. If $\mathcal{T}^{-1}(w_0)$ is nonempty, then $\mathcal{T}^{-1}(w_0)$ is an affine subspace of V parallel to* $\operatorname{Ker}(\mathcal{T})$.

Proof. Choose $v_0 \in V$ with $\mathcal{T}(v_0) = w_0$. If $v \in \mathcal{T}^{-1}(w_0)$ is arbitrary, then $v = v_0 + (v - v_0) = v_0 + u$ and $\mathcal{T}(u) = \mathcal{T}(v - v_0) = \mathcal{T}(v) - \mathcal{T}(v_0) = w_0 - w_0 = 0$, so $u \in \operatorname{Ker}(\mathcal{T})$. Conversely, if $u \in \operatorname{Ker}(\mathcal{T})$ and $v = v_0 + u$, then $\mathcal{T}(v) = \mathcal{T}(v_0 + u) = \mathcal{T}(v_0) + \mathcal{T}(u) = w_0 + 0 = w_0$. Thus we see that

$$\mathcal{T}^{-1}(w_0) = v_0 + \operatorname{Ker}(\mathcal{T})$$

and the theorem then follows from Proposition 1.5.4. □

REMARK 1.5.8. The condition in Definition 1.5.1 is stronger than the condition that $U = \{x_2 - x_1 \mid x_1, x_2 \in U\}$. (We must fix x_1 and let x_2 vary, or vice versa, but we cannot let both vary.) For example, if V is any vector space and $X = V - \{0\}$, then $V = \{x_2 - x_1 \mid x_1, x_2 \in X\}$, but X is never an affine subspace of V, except in the case that V is a 1-dimensional vector space over the field with 2 elements. ◇

Let V be a vector space and W a subspace. We now define the important notion of the quotient vector space V/W, and investigate some of its properties.

DEFINITION 1.5.9. Let V be a vector space and let W be a subspace of V. Let $\sim$ be the equivalence relation on V given by $v_1 \sim v_2$ if $v_1 - v_2 \in W$. Denote the equivalence class of $v \in V$ under this relation by $[v]$. Then the *quotient* V/W is the vector space

$$V/W = \{\text{equivalence classes } [v] \mid v \in V\}$$

with addition given by $[v_1] + [v_2] = [v_1 + v_2]$ and scalar multiplication given by $c[v] = [cv]$. ◇

REMARK 1.5.10. We leave it to the reader to check that these operations give V/W the structure of a vector space. ◇

Here is an alternative definition of V/W.

Lemma 1.5.11. *The quotient space V/W of Definition 1.5.9 is given by*

$$V/W = \{\textit{affine subspaces of } V \textit{ parallel to } W\}.$$

Proof. As in Proposition 1.5.4, we can check that for $v_0 \in V$, the equivalence class $[v_0]$ of v_0 is given by

$$\big[v_0\big] = \big\{v \in V \mid v \sim v_0\big\} = \big\{v \in V \mid v - v_0 \in W\big\} = v_0 + W,$$

which is an affine subspace parallel to W, and every affine subspace arises in this way from a unique equivalence class. □

There is a natural linear transformation from V to V/W.

DEFINITION 1.5.12. Let W be a subspace of V. The *canonical projection* $\pi : V \to V/W$ is the linear transformation given by $\pi(v) = [v] = v + W$. ◇

We have the following important construction and results. They improve on the purely numerical information provided by Theorem 1.3.1.

Theorem 1.5.13. *Let $\mathcal{T} : V \to X$ be a linear transformation. Then $\overline{\mathcal{T}} : V/\operatorname{Ker}(\mathcal{T}) \to X$ given by $\overline{\mathcal{T}}(v + \operatorname{Ker}(\mathcal{T})) = \mathcal{T}(v)$ (i.e., by $\overline{\mathcal{T}}(\pi(v)) = \mathcal{T}(v)$) is a well-defined linear transformation, and $\overline{\mathcal{T}}$ gives an isomorphism from $V/\operatorname{Ker}(\mathcal{T})$ to $\operatorname{Im}(\mathcal{T}) \subseteq X$.*

Proof. If $v_1 + \operatorname{Ker}(\mathcal{T}) = v_2 + \operatorname{Ker}(\mathcal{T})$, then $v_1 = v_2 + w$ for some $w \in \operatorname{Ker}(\mathcal{T})$, so $\mathcal{T}(v_1) = \mathcal{T}(v_2 + w) = \mathcal{T}(v_2) + \mathcal{T}(w) = \mathcal{T}(v_2) + 0 = \mathcal{T}(v_2)$, and $\overline{\mathcal{T}}$ is well-defined. It is then easy to check that it is a linear transformation, that it is 1-1, and that its image is $\operatorname{Im}(\mathcal{T})$, completing the proof. □

Let us now see how to find a basis for a quotient vector space.

Theorem 1.5.14. *Let V be a vector space and W_1 a subspace. Let $\mathcal{B}_1 = \{w_1, w_2, \ldots\}$ be a basis for W_1 and extend $\mathcal{B}_1$ to a basis $\mathcal{B}$ of V. Let $\mathcal{B}_2 = \mathcal{B} - \mathcal{B}_1 = \{z_1, z_2, \ldots\}$. Let W_2 be the subspace of V spanned by $\mathcal{B}_2$, so that W_2 is a complement W_1 in V with basis $\mathcal{B}_2$. Then the linear transformation $\mathcal{P} : W_2 \to V/W_1$ defined by $\mathcal{P}(z_i) = [z_i]$ is an isomorphism. In particular, $\overline{\mathcal{B}}_2 = \{[z_1], [z_2], \ldots\}$ is a basis for V/W_1.*

Proof. It is easy to check that $\mathcal{P}$ is a linear transformation. We show that $\{[z_1], [z_2], \ldots\}$ is a basis for V/W_1. Then, since $\mathcal{P}$ is a linear transformation taking a basis of one vector space to a basis of another, $\mathcal{P}$ is an isomorphism.

First let us see that $\overline{\mathcal{B}}_2$ spans V/W_1. Consider an equivalence class $[v]$ in V/W_1. Since $\mathcal{B}$ is a basis of V, we may write $v = \sum c_i w_i + \sum d_j z_j$

for some $\{c_i\}$ and $\{d_j\}$. Then $v - \sum d_j z_j = \sum c_i w_i \in W_1$, so $v \sim \sum d_j z_j$ and hence $[v] = [\sum d_j z_j] = \sum d_j [z_j]$.

Next let us see that $\overline{\mathcal{B}}_2$ is linearly independent. Suppose $\sum d_j [z_j] = [\sum d_j z_j] = 0$. Then $\sum d_j z_j \in W_1$, so $\sum d_j z_j = \sum c_i w_i$ for some $\{c_i\}$. But then $\sum(-c_i)w_i + \sum d_j z_j = 0$, an equation in V. But $\{w_1, w_2, \ldots, z_1, z_2, \ldots\} = \mathcal{B}$ is a basis of V, and hence linearly independent, so ($c_1 = c_2 = \cdots = 0$ and) $d_1 = d_2 = \cdots = 0$. □

REMARK 1.5.15. We cannot emphasize strongly enough the difference between a complement W_2 of the subspace W_1 and the quotient V/W_1. The quotient V/W_1 is canonically associated to W_1, whereas a complement is not. As we observed, W_1 almost never has a unique complement. Theorem 1.5.14 shows that any of these complements is isomorphic to the quotient V/W_1. We are in a situation here where every quotient object V/W_1 is isomorphic to a subobject W_2. This is not always the case in algebra, though it is here, and this fact simplifies arguments, as long as we remember that what we have is an isomorphism between W_2 and V/W_1, *not* an identification of W_2 with V/W_1. Indeed, it would be a *bad mistake* to identify V/W_1 with a complement W_2 of W_1. ◇

Often when considering a subspace W of a vector space V, what is important is not its dimension, but rather its codimension, which is defined as follows.

DEFINITION 1.5.16. Let W be a subspace of V. Then the *codimension* of W in V is

$$\operatorname{codim}_V W = \dim V/W. \qquad \diamond$$

Lemma 1.5.17. *Let W_1 be a subspace of V. Let W_2 be any complement of W_1 in V. Then* $\operatorname{codim}_V W_1 = \dim W_2$.

Proof. By Theorem 1.5.14, V/W_1 and W_2 are isomorphic. □

Corollary 1.5.18. *Let V be a vector space of dimension n and let W be a subspace of V of dimension k. Then* $\dim V/W = \operatorname{codim}_V W = n - k$.

Proof. Immediate from Theorem 1.5.14 and Lemma 1.5.17. □

Here is one important way in which quotient spaces arise.

DEFINITION 1.5.19. Let $\mathcal{T} : V \to W$ be a linear transformation. Then the *cokernel* of $\mathcal{T}$ is the quotient space

$$\operatorname{Coker}(\mathcal{T}) = W/\operatorname{Im}(\mathcal{T}). \qquad \diamond$$

Corollary 1.5.20. *Let V be an n-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. Then* $\dim(\operatorname{Ker}(\mathcal{T})) = \dim(\operatorname{Coker}(\mathcal{T}))$.

Proof. By Theorem 1.3.1, Corollary 1.5.18, and Definition 1.5.19,

$$\begin{aligned}\dim\left(\operatorname{Ker}(\mathcal{T})\right) &= \dim(V) - \dim\left(\operatorname{Im}(\mathcal{T})\right) = \dim\left(V/\operatorname{Im}(\mathcal{T})\right)\\ &= \dim\left(\operatorname{Coker}(\mathcal{T})\right). \qquad \square\end{aligned}$$

We have shown that any linearly independent set in a vector space V extends to a basis of V. We outline another proof of this, using quotient spaces. This proof is not any easier, but its basic idea is one we will be using later.

Theorem 1.5.21. *Let $\mathcal{B}_1$ be any linearly independent subset of a vector space V. Then $\mathcal{B}_1$ extends to a basis $\mathcal{B}$ of V.*

Proof. Let W be the subspace of V generated by $\mathcal{B}_1$, and let $\pi : V \to V/W$ be the canonical projection. Let $\mathcal{C} = \{x_1, x_2, \ldots\}$ be a basis of V/W and for each i let $u_i \in V$ with $\pi(u_i) = x_i$. Let $\mathcal{B}_2 = \{u_1, u_2, \ldots\}$. We leave it to the reader to check that $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ is a basis of V. $\square$

In a way, this result is complementary to Theorem 1.5.14, where we showed how to obtain a basis of V/W, starting from the right sort of basis of V. Here we showed how to obtain a basis of V, starting from a basis of W and a basis of V/W.

DEFINITION 1.5.22. Let $\mathcal{T} : V \to V$ be a linear transformation. $\mathcal{T}$ is *Fredholm* if $\operatorname{Ker}(\mathcal{T})$ and $\operatorname{Coker}(\mathcal{T})$ are both finite-dimensional, in which case the *index* of $\mathcal{T}$ is $\dim(\operatorname{Ker}(\mathcal{T})) - \dim(\operatorname{Coker}(\mathcal{T}))$. $\diamond$

EXAMPLE 1.5.23. (1) In case V is finite-dimensional, every $\mathcal{T}$ is Fredholm. Then by Corollary 1.5.20, $\dim(\operatorname{Ker}(\mathcal{T})) = \dim(\operatorname{Coker}(\mathcal{T}))$, so $\mathcal{T}$ has index 0. Thus in the finite-dimensional case, the index is completely uninteresting.

(2) In the infinite-dimensional case, the index is an important invariant, and may take on any integer value. For example, if $V = {}^r\mathbb{F}^{\infty\infty}$, $\mathbf{L} : V \to V$ is left shift and $\mathbf{R} : V \to V$ is right shift, as in Example 1.1.23(1), then $\mathbf{L}^n$ has index n and $\mathbf{R}^n$ has index $-n$.

(3) If $V = C^\infty(\mathbb{R})$, then $\mathbf{D} : V \to V$ has kernel $\{f(x) \mid f(x)$ is a constant function$\}$, of dimension 1, and is surjective, so $\mathbf{D}$ has index 1. Also, $\mathbf{I}_a : V \to V$ is injective and has image $\{f(x) \mid f(a) = 0\}$, of codimension 1, so $\mathbf{I}_a$ has index -1. $\diamond$

1.6 DUAL SPACES

We now consider the dual space of a vector space. The dual space is easy to define, but we will have to be careful, as there is plenty of opportunity for confusion.

DEFINITION 1.6.1. Let V be a vector space over a field $\mathbb{F}$. The *dual* V^* of V is

$$V^* = \mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F}) = \{\text{linear transformations } \mathcal{T} : V \to \mathbb{F}\}. \qquad \diamond$$

Lemma 1.6.2. *(1) If V is a vector space over $\mathbb{F}$, then V is isomorphic to a subspace of V^*.*

(2) If V is finite-dimensional, then V is isomorphic to V^*. In particular, in this case $\dim V = \dim V^*$.

Proof. Choose a basis $\mathcal{B}$ of V, $\mathcal{B} = \{v_1, v_2, \ldots\}$. Let $\mathcal{B}^*$ be the subset of V^* given by $\mathcal{B} = \{w_1^*, w_2^*, \ldots\}$ where v_i^* is defined by $w_i^*(v_i) = 1$ and $w_i^*(v_j) = 0$ if $j \neq i$. (This defines w_i^* by Lemma 1.2.23.) We claim that $\mathcal{B}^*$ is a linearly independent set. To see this, suppose $\sum c_j w_j^* = 0$. Then $(\sum c_j w_j^*)(v) = 0$ for every $v \in V$. Choosing $v = v_i$, we see that $c_i = 0$, for each i.

The linear transformation $\mathcal{S}_{\mathcal{B}} : V \to V^*$ defined by $\mathcal{S}_{\mathcal{B}}(v_i) = w_i^*$ takes the basis $\mathcal{B}$ of V to the independent set $\mathcal{B}^*$ of V^*, so is an injection (more precisely, an isomorphism from V to the subspace of V^* spanned by $\mathcal{B}^*$).

Suppose V is finite-dimensional and let w^* be an element of V^*. Let $w^*(v_i) = a_i$ for each i. Let $v = \sum a_i v_i$, a finite sum since V is finite-dimensional. For each i, $\mathcal{S}_{\mathcal{B}}(v)(v_i) = w^*(v_i)$. Since these two linear transformations agree on the basis $\mathcal{B}$ of V, by Lemma 1.2.23 they are equal, i.e., $\mathcal{S}_{\mathcal{B}}(v) = w^*$, and $\mathcal{S}_{\mathcal{B}}$ is a surjection. □

REMARK 1.6.3. It is important to note that there is *no* natural map from V to V^*. The linear transformation $\mathcal{S}_{\mathcal{B}}$ depends on the choice of basis $\mathcal{B}$. In particular, if V is finite-dimensional then, although V and V^* are isomorphic as abstract vector spaces, there is no natural isomorphism between them, and it would be a mistake to identify them. $\diamond$

REMARK 1.6.4. If $V = \mathbb{F}^n$ with $\mathcal{E}$ the standard basis $\{e_1, \ldots, e_n\}$, then the proof of Lemma 1.6.2 gives the standard basis $\mathcal{E}^*$ of V^*, $\mathcal{E}^* = \{e_1^*, \ldots,$

$e_n^*\}$, defined by

$$e_i^*\left(\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}\right) = a_i. \qquad \diamond$$

REMARK 1.6.5. The basis $\mathcal{B}^*$ (and hence the map $\mathcal{S}_{\mathcal{B}}$) depends on the entire basis $\mathcal{B}$. For example, let $V = \mathbb{F}^2$ and choose the standard basis $\mathcal{E}$ of V,

$$\mathcal{E} = \left\{\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right\} = \{e_1, e_2\}.$$

Then $\mathcal{E}^*$ is the basis $\{e_1^*, e_2^*\}$ of V^*, with

$$e_1^*\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = x \qquad \text{and} \qquad e_2^*\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = y.$$

If we choose the basis $\mathcal{B}$ of V given by

$$\mathcal{B} = \left\{\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \end{bmatrix}\right\} = \{v_1, v_2\},$$

then $\mathcal{B}^* = \{w_1^*, w_2^*\}$ with

$$w_1^*\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = x + y \qquad \text{and} \qquad w_2^*\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = -y.$$

Thus, even though $v_1 = e_1$, $w_1^* \neq e_1^*$. $\diamond$

EXAMPLE 1.6.6. If V is infinite-dimensional, then in general the linear transformation $\mathcal{S}_{\mathcal{B}}$ is an injection but not a surjection. Let $V = \mathbb{F}^\infty$ with basis $\mathcal{E} = \{e_1, e_2, \ldots\}$ and consider the set $\mathcal{E}^* = \{e_1^*, e_2^*, \ldots\}$. Any element w^* of the subspace V^* spanned by $\mathcal{E}^*$ has the property that $w^*(e_i) \neq 0$ for only finitely many values of i. This is not the case for a general element of V^*. In fact, V^* is isomorphic to $\mathbb{F}^{\infty\infty}$ as follows: If

$$v = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \end{bmatrix} \in \mathbb{F}^\infty \qquad \text{and} \qquad x^* = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \end{bmatrix} \in \mathbb{F}^{\infty\infty}$$

then we have the pairing $x^*(v) = \sum a_i b_i$. (This makes sense for any x^*, as only finitely many entries of v are nonzero.) Any element w^* of V^* arises in this way as we may choose

$$x^* = \begin{bmatrix} w^*(e_1) \\ w^*(e_2) \\ \vdots \end{bmatrix}.$$

Thus in this case the image of $\mathcal{S}_{\mathcal{B}}$ is $\mathbb{F}^{\infty} \subset \mathbb{F}^{\infty\infty}$. $\diamond$

REMARK 1.6.7. The preceding example leaves open the possibility that V might be isomorphic to V^* by some other isomorphism than $\mathcal{T}_B$. That is also not the case in general. We have seen in Remark 1.2.19 that $\mathbb{F}^{\infty}$ is a vector space of countably infinite dimension and $\mathbb{F}^{\infty\infty}$ is a vector space of uncountably infinite dimension. $\diamond$

REMARK 1.6.8. Just as a typical element of V is denoted by v, a typical element of V^* is often denoted by v^*. This notation carries the danger of giving the impression that there is a natural map from V to V^* given by $v \mapsto v^*$ (i.e., that the element v^* of V^* is the dual of the element v of V), and we emphasize again that that is *not* the case. There is no such natural map and that is does not make sense to speak of the dual of an element of V. Thus we do not use this notation and instead use w^* to denote an element of V^*. $\diamond$

EXAMPLE 1.6.9 (Compare Example 1.2.22). Let $V = P_{n-1}(\mathbb{R})$ for any n.

(1) For any $a \in \mathbb{R}$, V has basis $\mathcal{B} = \{p_0(x), p_1(x), \ldots, p_{n-1}(x)\}$ where $p_0(x) = 1$ and $p_k(x) = (x-a)^k/k!$ for $k = 1, \ldots, n-1$. The dual basis $\mathcal{B}^*$ is given by $\mathcal{B}^* = \{\mathbf{E}_a, \mathbf{E}_a \circ \mathbf{D}, \ldots, \mathbf{E}_a \circ \mathbf{D}^{n-1}\}$.

(2) For any distinct $a_1, \ldots, a_n \in \mathbb{R}$, V has basis $\mathcal{C} = \{q_1(x), \ldots, q_n(x)\}$ with $q_k(x) = \Pi_{j \neq k}(x - a_j)/(a_k - a_j)$. The dual basis $\mathcal{C}^*$ is given by $\mathcal{C}^* = \{\mathbf{E}_{a_1}, \ldots, \mathbf{E}_{a_n}\}$.

(3) Fix an interval $[a, b]$ and let $\mathcal{T} : V \to \mathbb{R}$ be the linear transformation

$$\mathcal{T}\big(f(x)\big) = \int_a^b f(x)\,dx.$$

Then $\mathcal{T} \in V^*$. Since $\mathcal{C}^*$ (as above) is a basis of V^*, we have $\mathcal{T} = \sum_{i=1}^n c_i \mathbf{E}_{a_i}$ for some constants $c_1, \ldots, c_n$.

In other words, we have the exact quadrature formula, valid for every $f(x) \in V$,

$$\int_a^b f(x)\,dx = \sum_{i=1}^n c_i f(a_i).$$

For simplicity, let $[a, b] = [0, 1]$, and let us for example choose equally spaced points.

For $n = 0$ choose $a_1 = 1/2$. Then $c_1 = 1$, i.e.,

$$\int_0^1 f(x)\,dx = f(1/2) \quad \text{for } f \in P_0(\mathbb{R}).$$

For $n = 1$, choose $a_1 = 0$ and $a_2 = 1$. Then $c_1 = c_2 = 1/2$, i.e.,

$$\int_0^1 f(x)\,dx = (1/2)f(0) + (1/2)f(1) \quad \text{for } f \in P_1(\mathbb{R}).$$

For $n = 2$, choose $a_1 = 0$, $a_2 = 1/2$, $a_3 = 1$. Then $c_1 = 1/6$, $c_2 = 4/6$, $c_3 = 1/6$, i.e.,

$$\int_0^1 f(x)\,dx = (1/6)f(0) + (4/6)f(1/2) + (1/6)f(1) \quad \text{for } f \in P_2(\mathbb{R}).$$

The next two expansions of this type are

$$\begin{aligned}\int_0^1 f(x)\,dx &= (1/8)f(0) + (3/8)f(1/3) + (3/8)f(2/3)\\ &\qquad + (1/8)f(1) \quad \text{for } f \in P_3(\mathbb{R}),\\ \int_0^1 f(x)\,dx &= (7/90)f(0) + (32/90)f(1/4) + (12/90)f(1/2)\\ &\qquad + (32/90)f(3/4) + (7/90)f(1) \quad \text{for } f \in P_4(\mathbb{R}).\end{aligned}$$

These formulas are the basis for commonly used approximate quadrature formulas: The first three yield the midpoint rule, the trapezoidal rule, and Simpson's rule respectively.

(4) Fix an interval $[a, b]$ and for any polynomial $g(x)$ let

$$\mathcal{T}_{g(x)} = \int_a^b f(x)g(x)\,dx.$$

Then $\mathcal{T}_{g(x)} \in V^*$. Let $\mathcal{D}^* = \{\mathcal{T}_1, \mathcal{T}_x, \ldots, \mathcal{T}_{x^{n-1}}\}$. We claim that $\mathcal{D}^*$ is linearly independent. To see this, suppose that

$$\mathcal{T} = a_0\mathcal{T}_1 + a_1\mathcal{T}_x + \cdots + a_{n-1}\mathcal{T}_{x^{n-1}} = 0.$$

Then $\mathcal{T} = \mathcal{T}_{g(x)}$ with $g(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in V$. To say that $\mathcal{T} = 0$ is to say that $\mathcal{T}(f(x)) = 0$ for every $f(x) \in V$. But if we choose $f(x) = g(x)$, we find

$$\mathcal{T}\big(f(x)\big) = \mathcal{T}_{g(x)}\big(g(x)\big) = \int_a^b g(x)^2\,dx = 0$$

which forces $g(x) = 0$, i.e., $a_0 = a_1 = \cdots = a_{n-1} = 0$, and $\mathcal{D}^*$ is linearly independent.

Since $\mathcal{D}^*$ is a linearly independent set of n elements in V^*, a vector space of dimension n, it must be a basis of V^*, so every element of V^* is $\mathcal{T}_{g(x)}$ for a unique $g(x) \in V$. In particular this is true for $\mathbf{E}_c$ for every $c \in [a, b]$. It is simply a matter of solving a linear system to find $g(x)$. For example, let $[a, b] = [0, 1]$ and let $c = 0$. We find

$$f(0) = \int_0^1 f(x)g(x)\,dx$$

$$\begin{array}{ll}
\text{for } g(x) = 1 & \text{if } f(x) \in P_0(\mathbb{R}), \\
\text{for } g(x) = 4 - 6x & \text{if } f(x) \in P_1(\mathbb{R}), \\
\text{for } g(x) = 9 - 36x + 30x^2 & \text{if } f(x) \in P_2(\mathbb{R}), \\
\text{for } g(x) = 16 - 120x + 240x^2 - 140x^3 & \text{if } f(x) \in P_3(\mathbb{R}), \\
\text{for } g(x) = 25 - 300x + 1050x^2 - 1400x^3 + 630x^4 & \text{if } f(x) \in P_4(\mathbb{R}).
\end{array}$$

Admittedly, we rarely if ever want to evaluate a function at a point by computing an integral instead, but this shows how it could be done.

We have presented (3) and (4) here so that the reader may see some interesting examples early, but they are best understood in the context of inner product spaces, which we consider in Chapter 7. ◇

To every subspace of V we can naturally associate a subspace of V^* (and vice-versa), as follows.

DEFINITION 1.6.10. Let U be a subspace of V. Then the *annihilator* $\operatorname{Ann}^*(U)$ is the subspace of V^* defined by

$$\operatorname{Ann}^*(U) = \{w^* \in V^* \mid w^*(u) = 0 \text{ for every } u \in U\}. \qquad \diamond$$

Lemma 1.6.11. *Let U be a finite-dimensional subspace of V. Then $V^*/\operatorname{Ann}^*(U)$ is isomorphic to U. Consequently,*

$$\operatorname{codim}\big(\operatorname{Ann}^*(U)\big) = \dim(U).$$

Proof. Set $X^* = \operatorname{Ann}^*(U)$ and let $\{x_1^*, x_2^*, \ldots\}$ be a basis of X^*. Let $\{u_1, \ldots, u_k\}$ be a basis for U. Let U' be a complement of U, so $V = U \oplus U'$, and let $\{u_1', u_2', \ldots\}$ be a basis of U'. Then $\{u_1, \ldots, u_k, u_1', u_2', \ldots\}$

is a basis of V. For $j = 1, \ldots, k$ define $y_j^* \in V^*$ by

$$\begin{aligned} y_j^*(u_i) &= 0 \quad \text{if } i \neq j, \\ y_j^*(u_j) &= 1, \\ y_j^*(u_m') &= 0 \quad \text{for every } m. \end{aligned}$$

We claim $\{y_1^*, \ldots, y_k^*, x_1^*, x_2^*, \ldots\}$ is a basis of V^*. First we show it is linearly independent: Suppose $\sum c_j y_j^* + \sum d_m x_m^* = 0$. Evaluating this function at u_i we see it has the value c_i, so $c_i = 0$ for $i = 1, \ldots, k$. Then $d_m = 0$ for each m as $\{x_1^*, x_2^*, \ldots\}$ is linearly independent. Next we show it spans V^*: Let $w^* \in V^*$. For $j = 1, \ldots, k$, let $c_i = w^*(u_i)$. Let $y^* = w^* - \sum c_j y_j^*$. Then $y^*(u_i) = 0$ for each i, so $y^* \in \mathrm{Ann}(U^*)$ and hence $y^* = \sum d_m x_m^*$ for some $d_1, \ldots, d_m$. Then $w^* = \sum c_j y_j^* + \sum d_m x_m^*$.

Let Y^* be the subspace of V^* spanned by $\{y_1^*, \ldots, y_k^*\}$. Then $V^* = X^* \oplus Y^*$ so V^*/X^* is isomorphic to Y^*. But we have an isomorphism $S : U \to Y^*$ given by $S(u_i) = y_i^*$. (If we let u_i^* be the restriction of y_i^* to U, then $\{u_1^*, \ldots, u_k^*\}$ is the dual basis to $\{u_1, \ldots, u_k\}$.) □

REMARK 1.6.12. We often think of Lemma 1.6.11 as follows: Suppose we have k linearly independent elements $u_1, \ldots, u_k$ of V, so that they generate a subspace U of V of dimension k. Then the requirements that a linear transformation from V to $\mathbb{F}$ be zero at each of $u_1, \ldots, u_k$ imposes k linearly independent conditions on the space of all such linear transformations, so the subspace of linear transformations satisfying precisely these conditions, which is $\mathrm{Ann}^*(U)$, has codimension k. ◇

To go the other way, we have the following association.

DEFINITION 1.6.13. Let U^* be a subspace of V^*. Then the *annihilator* $\mathrm{Ann}(U^*)$ is the subspace of V defined by

$$\mathrm{Ann}(U^*) = \left\{v \in V \mid w^*(v) = 0 \text{ for every } w^* \in U^*\right\}.$$

◇

REMARK 1.6.14. Observe that $\mathrm{Ann}^*(\{0\}) = V^*$ and $\mathrm{Ann}^*(V) = \{0\}$; similarly $\mathrm{Ann}(\{0\}) = V$ and $\mathrm{Ann}(V^*) = \{0\}$. ◇

If V is finite-dimensional, our pairings are inverses of each other, as we now see.

Theorem 1.6.15. *(1) For any subspace U of V,* $\mathrm{Ann}(\mathrm{Ann}^*(U)) = U$.

(2) Let V be finite-dimensional. For any subspace U^* of V^*,

$$\mathrm{Ann}^*(\mathrm{Ann}(U^*)) = U^*.$$

So far in this section we have considered vectors, i.e., objects. We now consider linear transformations, i.e., functions. We first saw pullbacks in Example 1.1.23(3), and now we see them again.

DEFINITION 1.6.16. Let $\mathcal{T} : V \to X$ be a linear transformation. Then the *dual* $\mathcal{T}^*$ of $\mathcal{T}$ is the linear transformation $\mathcal{T}^* : X^* \to V^*$ given by $\mathcal{T}^*(y^*) = y^* \circ T$, i.e., $\mathcal{T}^*(y^*) \in V^*$ is the linear transformation on V defined by

$$\big(\mathcal{T}^*\big(y^*\big)\big)(v) = \big(y^* \circ T\big)(v) = y^*\big(\mathcal{T}(v)\big), \quad \text{for } y^* \in X^*. \qquad \diamond$$

REMARK 1.6.17. (1) It is easy to check that $\mathcal{T}^*(y^*)$ is a linear transformation for any $y^* \in X^*$. But we are claiming more, that $y^* \mapsto \mathcal{T}^*(y^*)$ is a linear transformation from V^* to X^*. This follows from checking that $\mathcal{T}^*(y_1^* + y_2^*) = \mathcal{T}^*(y_1^*) + \mathcal{T}^*(y_2^*)$ and $\mathcal{T}^*(cy^*) = c\mathcal{T}^*(y^*)$.

(2) The dual $\mathcal{T}^*$ of $\mathcal{T}$ is well-defined and does not depend on a choice of basis, as it was defined directly in terms of $\mathcal{T}$. $\diamond$

Now we derive some relations between various subspaces.

Lemma 1.6.18. *Let $\mathcal{T} : V \to X$ be a linear transformation. Then* $\mathrm{Im}(\mathcal{T}^*) = \mathrm{Ann}^*(\mathrm{Ker}(\mathcal{T}))$.

Proof. Let $w^* \in V^*$ be in $\mathrm{Im}(\mathcal{T}^*)$, so $w^* = \mathcal{T}^*(y^*)$ for some $y^* \in X^*$. Then for any $u \in \mathrm{Ker}(\mathcal{T})$, $w^*(u) = (\mathcal{T}^*(y^*))(u) = y^*(\mathcal{T}(u)) = y^*(0) = 0$, so w^* is in $\mathrm{Ann}^*(\mathrm{Ker}(\mathcal{T}))$. Thus we see that $\mathrm{Im}(\mathcal{T}^*) \subseteq \mathrm{Ann}^*(\mathrm{Ker}(\mathcal{T}))$.

Let $w^* \in V^*$ be in $\mathrm{Ann}^*(\mathrm{Ker}(\mathcal{T}))$, so $w^*(u) = 0$ for every $u \in \mathrm{Ker}(\mathcal{T})$. Let V' be a complement of $\mathrm{Ker}(\mathcal{T})$, so $V = \mathrm{Ker}(\mathcal{T}) \oplus V'$. Then we may write any $v \in V$ uniquely as $v = u + v'$ with $u \in \mathrm{Ker}(\mathcal{T})$, $v' \in V'$. Then $w^*(v) = w^*(u + v') = w^*(u) + w^*(v') = w^*(v')$. Also, $\mathcal{T}(v) = \mathcal{T}(v')$, so $\mathcal{T}(V) = \mathcal{T}(V')$. Let X' be any complement of $\mathcal{T}(V')$ in X, so that $X = \mathcal{T}(V') \oplus X'$.

Since the restriction of $\mathcal{T}$ to V' is an isomorphism, we may write $x \in X$ uniquely as $x = \mathcal{T}(v') + x'$ with $v' \in V'$ and $x' \in X'$. Define $y^* \in X^*$ by

$$y^*(x) = w^*(v') \quad \text{where } x = \mathcal{T}(v') + x',\ v' \in V' \text{ and } x' \in X'.$$

(It is routine to check that y^* is a linear transformation.) Then for $v \in V$, writing $v = u + v'$, with $u \in \mathrm{Ker}(\mathcal{T})$ and $v' \in V'$, we have

$$\big(\mathcal{T}^*\big(y^*\big)\big)(v) = y^*\big(\mathcal{T}(v)\big) = y^*\big(\mathcal{T}(v')\big) = w^*(v') = w^*(v).$$

Thus $\mathcal{T}^*(y^*) = w^*$ and we see that $\mathrm{Ann}^*(\mathrm{Ker}(\mathcal{T})) \subseteq \mathrm{Im}(\mathcal{T}^*)$. $\square$

The following corollary gives a useful dimension count.

Corollary 1.6.19. *Let $\mathcal{T} : V \to X$ be a linear transformation.*
(1) If $\mathrm{Ker}(\mathcal{T})$ *is finite-dimensional, then*

$$\operatorname{codim}\left(\operatorname{Im}\left(\mathcal{T}^*\right)\right) = \dim\left(\operatorname{Coker}\left(\mathcal{T}^*\right)\right) = \dim\left(\operatorname{Ker}(\mathcal{T})\right).$$

(2) If $\mathrm{Coker}(\mathcal{T})$ *is finite-dimensional, then*

$$\dim\left(\operatorname{Ker}\left(\mathcal{T}^*\right)\right) = \dim\left(\operatorname{Coker}(\mathcal{T})\right) = \operatorname{codim}\left(\operatorname{Im}(\mathcal{T})\right).$$

Proof. (1) Let $U = \mathrm{Ker}(\mathcal{T})$. By Lemma 1.6.11,

$$\dim\left(\operatorname{Ker}\left(\mathcal{T}\right)\right) = \operatorname{codim}\left(\operatorname{Ann}^*\left(\operatorname{Ker}(\mathcal{T})\right)\right).$$

By Lemma 1.6.18,

$$\operatorname{Ann}^*\left(\operatorname{Ker}(\mathcal{T})\right) = \operatorname{Im}\left(\mathcal{T}^*\right).$$

(2) is proved using similar ideas and we omit the proof. □

Here is another useful dimension count.

Corollary 1.6.20. *Let $\mathcal{T} : V \to X$ be a linear transformation.*
(1) If $\dim(V)$ *is finite, then*

$$\dim\left(\operatorname{Im}\left(\mathcal{T}^*\right)\right) = \dim\left(\operatorname{Im}\left(\mathcal{T}\right)\right).$$

(2) If $\dim(V) = \dim(X)$ *is finite, then*

$$\dim\left(\operatorname{Ker}\left(\mathcal{T}^*\right)\right) = \dim\left(\operatorname{Ker}(\mathcal{T})\right).$$

Proof. (1) By Theorem 1.3.1 and Corollary 1.6.19,

$$\begin{aligned}\dim(V) - \dim\left(\operatorname{Im}(\mathcal{T})\right) &= \dim\left(\operatorname{Ker}(\mathcal{T})\right)\\ &= \operatorname{codim}\left(\operatorname{Im}\left(\mathcal{T}^*\right)\right) = \dim\left(V^*\right) - \dim\left(\operatorname{Im}(\mathcal{T})\right),\end{aligned}$$

and by Lemma 1.6.2, $\dim(V^*) = \dim(V)$.
(2) By Theorem 1.3.1 and Lemma 1.6.2,

$$\begin{aligned}\dim(\operatorname{Ker}\left(\mathcal{T}^*\right)) &= \dim\left(X^*\right) - \dim\left(\operatorname{Im}(\mathcal{T}^*)\right)\\ &= \dim(V) - \dim\left(\operatorname{Im}(\mathcal{T})\right) = \dim\left(\operatorname{Ker}(\mathcal{T})\right).\end{aligned}$$ □

REMARK 1.6.21. Again we caution the reader that although we have equality of dimensions, there is no natural identification of the subspaces in each part of Corollary 1.6.20. ◇

Lemma 1.6.22. *Let $\mathcal{T} : V \to X$ be a linear transformation.*

(1) $\mathcal{T}$ is injective if and only if $\mathcal{T}^*$ is surjective.

(2) $\mathcal{T}$ is surjective if and only if $\mathcal{T}^*$ is injective.

(3) $\mathcal{T}$ is an isomorphism if and only if $\mathcal{T}^*$ is an isomorphism.

Proof. (1) Suppose that $\mathcal{T}$ is injective. Let $w^* \in V^*$ be arbitrary. To show that $\mathcal{T}^*$ is surjective we must show that there is a $y^* \in X^*$ with $\mathcal{T}^*(y^*) = w^*$, i.e., $y^* \circ \mathcal{T} = w^*$.

Let $\mathcal{B} = \{v_1, v_2, \ldots\}$ be a basis of V and set $x_i = \mathcal{T}(v_i)$. $\mathcal{T}$ is injective so $\{x_1, x_2, \ldots\}$ is a linearly independent set in X. Extend this set to a basis $\mathcal{C} = \{x_1, x_2, \ldots, x_1', x_2', \ldots\}$ of X and define a linear transformation $\mathcal{U} : X \to V$ by $\mathcal{U}(x_i) = v_i$, $\mathcal{U}(x_j') = 0$. Note $\mathcal{U}\mathcal{T}(v_i) = v_i$ for each i so $\mathcal{U}\mathcal{T}$ is the identity map on V. Set $y^* = w^* \circ \mathcal{U}$. Then $\mathcal{T}^*(y^*) = y^* \circ \mathcal{T} = (w^* \circ \mathcal{U}) \circ \mathcal{T} = w^* \circ (\mathcal{U} \circ \mathcal{T}) = w^*$.

Suppose that $\mathcal{T}$ is not injective and choose $v \neq 0$ with $\mathcal{T}(v) = 0$. Then for any $y^* \in X^*$, $\mathcal{T}^*(y^*)(v) = (y^* \circ \mathcal{T})(v) = y^*(\mathcal{T}(v)) = y^*(0) = 0$. But not every element w^* of V^* has $w^*(v) = 0$. To see this, let $v_1 = v$ and extend v_1 to a basis $\mathcal{B} = \{v_1, v_2, \ldots\}$ of V. Then there is an element w^* of V^* defined by $w^*(v_1) = 0$, $w^*(v_i) = 0$ for $i \neq 1$.

(2) Suppose that $\mathcal{T}$ is surjective. Let $y^* \in X^*$. To show that $\mathcal{T}^*$ is injective we must show that if $\mathcal{T}^*(y^*) = 0$, then $y^* = 0$. Thus, suppose $\mathcal{T}^*(y^*) = 0$, i.e., that $(\mathcal{T}^*(y^*))(v) = 0$ for every $v \in V$. Then $0 = (\mathcal{T}^*(y^*))(v) = (y^* \circ \mathcal{T})(v) = y^*(\mathcal{T}(v))$ for every $v \in V$. Choose $x \in X$. Then, since $\mathcal{T}$ is surjective, there is a $v \in V$ with $x = \mathcal{T}(v)$, and so $y^*(x) = y^*(\mathcal{T}(v)) = 0$. Thus $y^*(x) = 0$ for every $x \in X$, i.e., $y^* = 0$.

Suppose that $\mathcal{T}$ is not surjective. Then $\mathrm{Im}(\mathcal{T})$ is a proper subspace of X. Let $\{x_1, x_2, \ldots\}$ be a basis for $\mathrm{Im}(\mathcal{T})$ and extend this set to a basis $\mathcal{C} = \{x_1, x_2, \ldots, x_1', x_2', \ldots\}$ of X. Define $y^* \in X^*$ by $y^*(x_i) = 0$ for all i, $y^*(x_1') = 1$, and $y^*(x_j') = 0$ for $j \neq 1$. Then $y^* \neq 0$, but $y^*(x) = 0$ for every $x \in \mathrm{Im}(\mathcal{T})$. Then

$$\big(\mathcal{T}^*\big(y^*\big)\big)(v) = \big(y^* \circ \mathcal{T}\big)(v) = y^*\big(\mathcal{T}(v)\big) = 0$$

so $\mathcal{T}^*(y^*) = 0$.

(3) This immediately follows from (1) and (2). □

Next we see how the dual behaves under composition.

Lemma 1.6.23. *Let $\mathcal{T} : V \to W$ and $\mathcal{S} : W \to X$ be linear transformations. Then $\mathcal{S} \circ \mathcal{T} : V \to X$ has dual $(\mathcal{S} \circ \mathcal{T})^* : X^* \to V^*$ given by $(\mathcal{S} \circ \mathcal{T})^* = \mathcal{T}^* \circ \mathcal{S}^*$.*

Proof. Let $y^* \in X^*$ and let $x \in X$. Then

$$\begin{aligned}\big((\mathcal{S} \circ \mathcal{T})^*(y^*)\big)(x) &= y^*\big((\mathcal{S} \circ \mathcal{T})(x)\big) = y^*\big(\mathcal{S}(\mathcal{T}(x))\big)\\ &= \big(\mathcal{S}(y^*)\big)\big(\mathcal{T}(x)\big) = \big(\mathcal{T}^*(\mathcal{S}(y^*))\big)(x)\\ &= \big((\mathcal{T}^* \circ \mathcal{S}^*)(y^*)\big)(x).\end{aligned}$$

Since this is true for every x and y^*, $(\mathcal{S} \circ \mathcal{T})^* = \mathcal{T}^* \circ \mathcal{S}^*$. □

We can now consider the dual V^{**} of V^*, known as the *double dual* of V.

An element of V^* is a linear transformation from V to $\mathbb{F}$, and so is a function from V to $\mathbb{F}$. An element of V^{**} is a linear transformation from V^* to $\mathbb{F}$, and so is a function from V^* to $\mathbb{F}$. In other words, an element of V^{**} is a function on functions. There is one natural way to get a function on functions: evaluation at a point. This is the linear transformation $\mathbf{E}_v$ ("Evaluation at v") of the next definition.

DEFINITION 1.6.24. Let $\mathbf{E}_v \in V^{**}$ be the linear transformation $\mathbf{E}_v : V^* \to \mathbb{F}$ defined by $\mathbf{E}_v(w^*) = w^*(v)$ for every $w^* \in V^*$. ◇

REMARK 1.6.25. It is easy to check that $\mathbf{E}_v$ is a linear transformation. Also, $\mathbf{E}_v$ is naturally defined. It does not depend on a choice of basis. ◇

Lemma 1.6.26. *The linear transformation $\mathcal{H} : V \to V^{**}$ given by $\mathcal{H}(v) = \mathbf{E}_v$ is an injection. If V is finite-dimensional, it is an isomorphism.*

Proof. Let v be an element of V with $\mathbf{E}_v = 0$. Now $\mathbf{E}_v$ is an element of V^{**}, the dual of V^*, so $\mathbf{E}_v = 0$ means that for every $w^* \in V^*$, $\mathbf{E}_v(w^*) = 0$. But $\mathbf{E}_v(w^*) = w^*(v)$. Thus $v \in V$ has the property that $w^*(v) = 0$ for every $w^* \in V^*$. We claim that $v = 0$. Suppose not. Let $v_1 = v$ and extend $\{v_1\}$ to a basis $\mathcal{B} = \{v_1, v_2, \ldots\}$ of V. Consider the dual basis $\mathcal{B}^* = \{w_1^*, w_2^*, \ldots\}$ of V^*. Then $w_1^*(v_1) = 1 \neq 0$.

If V is finite-dimensional, then $\mathbf{E}_v$ is an injection between vector spaces of the same dimension and hence is an isomorphism. □

REMARK 1.6.27. As is common practice, we will often write $v^{**} = \mathcal{H}(v)$ in case V is finite-dimensional. The map $v \mapsto v^{**}$ then provides a *canonical* identification of elements of V with elements of V^{**}, as there is no choice, of basis or anything else, involved. ◇

Beginning with a vector space V and a subspace U of V, we obtained from Definition 1.6.10 the subspace $\mathrm{Ann}^*(U)$ of V^*. Similarly, beginning with the subspace $\mathrm{Ann}^*(U)$ of V^* we could obtain the subspace $\mathrm{Ann}^*(\mathrm{Ann}^*(U))$ of V^{**}. This is not the construction of Definition 1.6.13, which would give us the subspace $\mathrm{Ann}(\mathrm{Ann}^*(U))$, which we saw in Theorem 1.6.15 was just U. But these two constructions are closely related.

Corollary 1.6.28. *Let V be a finite-dimensional vector space and let U be a subspace of V. Let $\mathcal{H}$ be the linear transformation of Lemma 1.6.26. Then $\mathcal{H} : U \to \mathrm{Ann}^*(\mathrm{Ann}^*(U))$ is an isomorphism.*

Since we have a natural way of identifying finite-dimensional vector spaces with their double duals, we should have a natural way of identifying linear transformations between finite-dimensional vector spaces with linear transformations between their double duals, and we do.

DEFINITION 1.6.29. Let V and X be finite-dimensional vector spaces. If $\mathcal{T} : V \to X$ is a linear transformation, its *double dual* is the linear transformation $\mathcal{T}^{**} : V^{**} \to X^{**}$ given by $\mathcal{T}^{**}(v^{**}) = (\mathcal{T}(v))^{**}$. $\diamond$

Lemma 1.6.30. *Let V and X be finite-dimensional vector spaces. Then $\mathcal{T} \mapsto \mathcal{T}^{**}$ is an isomorphism from $\mathrm{Hom}_{\mathbb{F}}(V, X) = \{$linear transformations: $V \to X\}$ to $\mathrm{Hom}_{\mathbb{F}}(V^{**}, X^{**}) = \{$linear transformations:$V^{**} \to X^{**}\}$.*

Proof. It is easy to check that $\mathcal{T} \mapsto \mathcal{T}^{**}$ is a linear transformation. Since V and V^{**} have the same dimension, as do X and X^{**}, {linear transformations: $V \to X$} and {linear transformations:$V^{**} \to X^{**}$} are vector spaces of the same dimension. Thus in order to show that $\mathcal{T} \mapsto \mathcal{T}^{**}$ is an isomorphism, it suffices to show that $\mathcal{T} \mapsto \mathcal{T}^{**}$ is an injection. Suppose $\mathcal{T}^{**} = 0$, i.e., $\mathcal{T}^{**}(v^{**}) = 0$ for every $v^{**} \in V^{**}$. Let $v \in V$ be arbitrary. Then $0 = \mathcal{T}^{**}(v^{**}) = (\mathcal{T}(v))^{**} = \mathcal{H}(\mathcal{T}(v))$. But $\mathcal{H}$ is an isomorphism by Lemma 1.6.26, so $\mathcal{T}(v) = 0$. Since this is true for every $v \in V$, $\mathcal{T} = 0$. $\square$

REMARK 1.6.31. In the infinite-dimensional case it is in general not true that V is isomorphic to V^{**}. For example, if $V = \mathbb{F}^{\infty}$ we have seen in Example 1.6.6 that V^* is isomorphic to $\mathbb{F}^{\infty\infty}$. Also, V^* is isomorphic to a subspace of V^{**}. We thus see that V has countably infinite dimension and V^{**} has uncountably infinite dimension, so they cannot be isomorphic. $\diamond$

CHAPTER 2

Coordinates

In this chapter we investigate coordinates.

It is useful to keep in mind the metaphor:

> Coordinates are a language for describing vectors and linear transformations.

In human languages we have, for example:

$$[*]_{\text{English}} = \text{star},\ [*]_{\text{French}} = \text{étoile},\ [*]_{\text{German}} = \text{Stern},$$

$$[\to]_{\text{English}} = \text{arrow},\ [\to]_{\text{French}} = \text{flèche},\ [\to]_{\text{German}} = \text{Pfeil}.$$

Coordinates share two similarities with human languages, but have one important difference.

(1) Often it is easier to work with objects, and often it is easier to work with words that describe them. Similarly, often it is easier and more enlightening to work with vectors and linear transformations directly, and often it is easier and more enlightening to work with their descriptions in terms of coordinates, i.e., with coordinate vectors and matrices.

(2) There are many different human languages and it is useful to be able to translate among them. Similarly, there are different coordinate systems and it is not only useful but indeed essential to be able to translate among them.

(3) A problem expressed in one human language is not solved by translating it into a second langauge. It is just expressed it differently. Coordinate systems are different. For many problems in linear algebra there is a preferred coordinate system, and translating the problem into that

language greatly simplifies it and helps to solve it. This is the idea behind eigenvalues, eigenvectors, and canonical forms for matrices. We save their investigation for a later chapter.

2.1 Coordinates for vectors

We begin by restating Lemma 1.2.21.

Lemma 2.1.1. *Let V be a vector space and let $\mathcal{B} = \{v_i\}$ be a set of vectors in V. Then $\mathcal{B}$ is a basis for V if and only if every $v \in V$ can be written uniquely as $v = \sum c_i v_i$ for $c_i \in \mathbb{F}$, all but finitely many zero.*

With this lemma in hand we may make the following important definition.

DEFINITION 2.1.2. Let V be an n-dimensional vector space and let $\mathcal{B} = \{v_1, \dots, v_n\}$ be a basis for V. For $v \in V$ the *coordinate vector* of v with respect to the basis $\mathcal{B}$, $[v]_{\mathcal{B}}$, is given as follows: If $v = \sum c_i v_i$, then

$$[v]_{\mathcal{B}} = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} \in \mathbb{F}^n. \qquad \diamond$$

Theorem 2.1.3. *Let V be an n-dimensional vector space and let $\mathcal{B}$ be a basis of V. Then $\mathcal{T} : V \to \mathbb{F}^n$ by $\mathcal{T}(v) = [v]_{\mathcal{B}}$ is an isomorphism.*

Proof. Let $\mathcal{B} = \{v_1, \dots, v_n\}$. Define $\mathcal{S} : \mathbb{F}^n \to V$ by

$$\mathcal{S}\left(\begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}\right) = \sum c_i v_i.$$

It is easy to check that $\mathcal{S}$ is a linear transformation, and then Lemma 2.1.1 shows that $\mathcal{S}$ is an isomorphism. Furthermore, $\mathcal{T} = \mathcal{S}^{-1}$. $\square$

EXAMPLE 2.1.4. (1) Let $V = \mathbb{F}^n$ and let $\mathcal{B} = \mathcal{E}$ be the standard basis. If $v = \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}$, then $v = \sum c_i e_i$ (where $\mathcal{E} = \{e_1, \dots, e_n\}$) and so $[v]_{\mathcal{E}} = \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}$. That is, a vector "looks like itself" in the standard basis.

(2) Let V be arbitrary and let $\mathcal{B} = \{b_1, \dots, b_n\}$ be a basis for V. Then $[b_i]_{\mathcal{B}} = e_i$.

(3) Let $V = \mathbb{R}^2$, let $\mathcal{E} = \left\{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right\} = \{e_1, e_2\}$ and let $\mathcal{B} = \left\{\begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}3\\7\end{bmatrix}\right\} = \{b_1, b_2\}$. Then $[b_1]_{\mathcal{E}} = \begin{bmatrix}1\\2\end{bmatrix}$ and $[b_2]_{\mathcal{E}} = \begin{bmatrix}3\\7\end{bmatrix}$ (as $\begin{bmatrix}1\\2\end{bmatrix} = 1\begin{bmatrix}1\\0\end{bmatrix} + 2\begin{bmatrix}0\\1\end{bmatrix}$ and $\begin{bmatrix}3\\7\end{bmatrix} = 3\begin{bmatrix}1\\0\end{bmatrix} + 7\begin{bmatrix}0\\1\end{bmatrix}$).

On the other hand, $[e_1]_{\mathcal{B}} = \begin{bmatrix}7\\-2\end{bmatrix}$ and $[e_2]_{\mathcal{B}} = \begin{bmatrix}-3\\1\end{bmatrix}$ (as $\begin{bmatrix}1\\0\end{bmatrix} = 7\begin{bmatrix}1\\2\end{bmatrix} + (-2)\begin{bmatrix}3\\7\end{bmatrix}$ and $\begin{bmatrix}0\\1\end{bmatrix} = (-3)\begin{bmatrix}1\\0\end{bmatrix} + 1\begin{bmatrix}3\\7\end{bmatrix}$).

Let $v_1 = \begin{bmatrix}17\\39\end{bmatrix}$. Then $[v_1]_{\mathcal{E}} = \begin{bmatrix}17\\39\end{bmatrix}$. Also, $[v_1]_{\mathcal{B}} = \begin{bmatrix}x_1\\x_2\end{bmatrix}$ where $v_1 = x_1b_1 + x_2b_2$, i.e., $\begin{bmatrix}17\\39\end{bmatrix} = x_1\begin{bmatrix}1\\2\end{bmatrix} + x_2\begin{bmatrix}3\\7\end{bmatrix}$. Solving, we find $x_1 = 2$, $x_2 = 5$, so $[v_1]_{\mathcal{B}} = \begin{bmatrix}2\\5\end{bmatrix}$. Similarly, let $v_2 = \begin{bmatrix}27\\62\end{bmatrix}$. Then $[v_2]_{\mathcal{E}} = \begin{bmatrix}27\\62\end{bmatrix}$. Also, $[v_2]_{\mathcal{B}} = \begin{bmatrix}y_1\\y_2\end{bmatrix}$ where $v_2 = y_1b_1 + y_2b_2$, i.e., $\begin{bmatrix}27\\62\end{bmatrix} = y_1\begin{bmatrix}1\\2\end{bmatrix} + y_2\begin{bmatrix}3\\7\end{bmatrix}$. Solving, we find $y_1 = 3$, $y_2 = 8$, so $[v_2]_{\mathcal{B}} = \begin{bmatrix}3\\8\end{bmatrix}$.

(4) Let $V = P_2(\mathbb{R})$, let $\mathcal{B}_0 = \{1, x, x^2\}$, and let $\mathcal{B}_1 = \{1, x-1, (x-1)^2\}$. Let $p(x) = 3 - 6x + 4x^2$. Then

$$\left[p(x)\right]_{\mathcal{B}_0} = \begin{bmatrix}3\\-6\\4\end{bmatrix}.$$

Also $p(x) = 1 + 2(x-1) + 4(x-1)^2$, so

$$\left[p(x)\right]_{\mathcal{B}_1} = \begin{bmatrix}1\\2\\4\end{bmatrix}. \qquad \diamond$$

2.2 MATRICES FOR LINEAR TRANSFORMATIONS

Let V and W be vector spaces of finite dimensions n and m respectively with bases $\mathcal{B} = \{v_1, \ldots, v_n\}$ and $\mathcal{C} = \{w_1, \ldots, w_m\}$ and let $\mathcal{T} : V \to W$ is a linear transformation. Then we have isomorphisms $\mathcal{S} : V \to \mathbb{F}^n$ given by $\mathcal{S}(v) = [v]_B$ and $\mathcal{U} : W \to \mathbb{F}^m$ given by $\mathcal{U}(w) = [w]_C$, and we may form the composition $\mathcal{U} \circ \mathcal{T} \circ \mathcal{S}^{-1} : \mathbb{F}^n \to \mathbb{F}^m$. Since this is a linear transformation, it is given by multiplication by a unique matrix. We are thus led to the following definition.

DEFINITION 2.2.1. Let V be an n-dimensional vector space with basis $\mathcal{B} = \{v_1, \ldots, v_n\}$ and let W be an m-dimensional vector space with basis $\mathcal{C} = \{w_1, \ldots, w_m\}$. Let $\mathcal{T} : V \to W$ be a linear transformation. The *matrix of the linear transformation* $\mathcal{T}$ *with respect to the bases* $\mathcal{B}$ *and* $\mathcal{C}$, denoted $[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}$, is the unique matrix such that

$$[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}[v]_{\mathcal{B}} = [\mathcal{T}(v)]_{\mathcal{C}} \quad \text{for every } v \in V. \qquad \diamond$$

It is easy to write down $[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}$ (at least in principle).

Lemma 2.2.2. *In the situation of Definition 2.2.1, the matrix* $[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}$ *is given by*

$$[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}} = \big[\big[\mathcal{T}(v_1)\big]_{\mathcal{C}} \mid \big[\mathcal{T}(v_2)\big]_{\mathcal{C}} \mid \cdots \mid \big[\mathcal{T}(v_n)\big]_{\mathcal{C}}\big],$$

i.e., $[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}$ *is the matrix whose* i*th column is* $[\mathcal{T}(v_i)]_{\mathcal{C}}$*, for each* i.

Proof. By Lemma 1.2.23, we need only verify the equation $[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}[v] = [\mathcal{T}(v)]_{\mathcal{C}}$ for $v = v_i$, $i = 1\ldots, n$. But $[v_i]_{\mathcal{B}} = e_i$ and $[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}e_i$ is the ith column of $[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}$, i.e., $[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}[v_i]_{\mathcal{B}} = [\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}e_i = [\mathcal{T}(v_i)]_{\mathcal{C}}$ as required. □

Theorem 2.2.3. *Let* V *be a vector space of dimension* n *and let* W *be a vector space of dimension* m *over a field* $\mathbb{F}$. *Choose bases* $\mathcal{B}$ *of* V *and* $\mathcal{C}$ *of* W. *Then the linear transformation*

$$\begin{aligned}\mathcal{S} : \{&\textit{linear transformations } \mathcal{T} : V \to W\}\\ &\to \{\textit{m-by-n matrices with entries in } \mathbb{F}\}\end{aligned}$$

given by $\mathcal{S}(\mathcal{T}) = [\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}$ *is an isomorphism.*

Corollary 2.2.4. *In the situation of Theorem 2.2.3,* $\{$*linear transformations* $\mathcal{T} : V \to W\}$ *is a vector space over* $\mathbb{F}$ *of dimension* mn.

Proof. $\{m$-by-n matrices with entries in $\mathbb{F}\}$ is a vector space of dimension mn, with basis the set of matrices $\{E_{ij}\}$, $1 \le i \le m$, $1 \le j \le n$, where E_{ij} has an entry of 1 in the (i, j) position and all other entries 0. □

Lemma 2.2.5. *Let* U*,* V*, and* W *be finite-dimensional vector spaces with bases* $\mathcal{B}$*,* $\mathcal{C}$*, and* $\mathcal{D}$ *respectively. Let* $\mathcal{T} : U \to V$ *and* $\mathcal{S} : V \to W$ *be linear transformations. Then* $\mathcal{S} \circ \mathcal{T} : U \to W$ *is a linear transformation with*

$$[\mathcal{S} \circ \mathcal{T}]_{\mathcal{D}\leftarrow\mathcal{B}} = [\mathcal{S}]_{\mathcal{D}\leftarrow\mathcal{C}}[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}.$$

Proof. For any $u \in W$,

$$\begin{aligned}
\big([\mathcal{S}]_{\mathcal{D}\leftarrow\mathcal{C}}[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}\big)[u]_{\mathcal{B}} &= [\mathcal{S}]_{\mathcal{D}\leftarrow\mathcal{C}}\big([\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}[u]_{\mathcal{B}}\big)\\
&= [\mathcal{S}]_{\mathcal{D}\leftarrow\mathcal{C}}\big([\mathcal{T}(u)]_{\mathcal{C}}\big)\\
&= \big[\mathcal{S}\big(\mathcal{T}(u)\big)\big]_{\mathcal{D}} = \big[\big(\mathcal{S}\circ\mathcal{T}\big)(u)\big]_{\mathcal{D}}.
\end{aligned}$$

But also $[\mathcal{S}\circ\mathcal{T}]_{\mathcal{D}\leftarrow\mathcal{B}}[u]_{\mathcal{B}} = [(\mathcal{S}\circ\mathcal{T})(u)]_{\mathcal{D}}$ so

$$[\mathcal{S}\circ\mathcal{T}]_{\mathcal{D}\leftarrow\mathcal{B}} = [\mathcal{S}]_{\mathcal{D}\leftarrow\mathcal{C}}[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}.$$ □

EXAMPLE 2.2.6. Let A be an m-by-n matrix and let $\mathcal{T}_A : \mathbb{F}^n \to \mathbb{F}^m$ be defined by $\mathcal{T}_A(v) = Av$. Choose the standard bases $\mathcal{E}_n$ for $\mathbb{F}^n$ and $\mathcal{E}_m$ for $\mathbb{F}^m$. Write $A = [a_1 \mid a_2 \mid \cdots \mid a_n]$, i.e., a_i is the ith column of A. Then $[\mathcal{T}_A]_{\mathcal{E}_m\leftarrow\mathcal{E}_n}$ is the matrix whose ith column is

$$\big[\mathcal{T}_A\big(e_i\big)\big]_{\mathcal{E}_m} = \big[Ae_i\big]_{\mathcal{E}_m} = \big[a_i\big]_{\mathcal{E}_m} = a_i,$$

so we see that $[\mathcal{T}_A]_{\mathcal{E}_m\leftarrow\mathcal{E}_n} = A$. That is, multiplication by a matrix "looks like itself" with respect to the standard bases. ◇

The following definition is the most important special case of Definition 2.2.1, and the case we will concentrate on.

DEFINITION 2.2.7. Let V be an n-dimensional vector space with basis $\mathcal{B} = \{v_1, \ldots, v_n\}$ and let $\mathcal{T} : V \to V$ be a linear transformation. The *matrix of the linear transformation $\mathcal{T}$ in the basis $\mathcal{B}$*, denoted $[\mathcal{T}]_{\mathcal{B}}$, is the unique matrix such that

$$[\mathcal{T}]_{\mathcal{B}}[v]_{\mathcal{B}} = [\mathcal{T}(v)]_{\mathcal{B}} \quad \text{for every } v \in V.$$ ◇

REMARK 2.2.8. Comparing Definition 2.2.7 with Definition 2.2.1, we see that we have simplified our notation in this special case: We have replaced $[\mathcal{T}]_{\mathcal{B}\leftarrow\mathcal{B}}$ by $[\mathcal{T}]_{\mathcal{B}}$.

With this simplification, the conclusion of Lemma 2.2.2 reads

$$[\mathcal{T}]_{\mathcal{B}} = \big[\big[\mathcal{T}\big(v_1\big)\big]_{\mathcal{B}} \mid \big[\mathcal{T}\big(v_2\big)\big]_{\mathcal{B}} \mid \cdots \mid \big[\mathcal{T}\big(v_n\big)\big]_{\mathcal{B}}\big].$$ ◇

We also make the following observation.

Lemma 2.2.9. *Let V be a finite-dimensional vector space and let $\mathcal{B}$ be a basis of V.*

(1) If $\mathcal{T} = \mathcal{I}$, the identity linear transformation, then $[\mathcal{T}]_{\mathcal{B}} = I$, the identity matrix.

(2) $\mathcal{T} : V \to V$ is an isomorphism if and only if $[\mathcal{T}]_{\mathcal{B}}$ is an invertible matrix, in which case $[\mathcal{T}^{-1}]_{\mathcal{B}} = ([\mathcal{T}]_{\mathcal{B}})^{-1}$.

EXAMPLE 2.2.10. Let $\mathcal{T} : \mathbb{R}^2 \to \mathbb{R}^2$ be given by $\mathcal{T}(v) = \begin{bmatrix} 65 & -24 \\ 149 & 55 \end{bmatrix} v$. Then $[\mathcal{T}]_{\mathcal{E}} = \begin{bmatrix} 65 & -24 \\ 149 & 55 \end{bmatrix}$. Let $\mathcal{B}$ be the basis $\mathcal{B} = \{b_1, b_2\}$ with $b_1 = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$ and $b_2 = \begin{bmatrix} 3 \\ 7 \end{bmatrix}$. Then $[\mathcal{T}]_{\mathcal{B}} = [[v_1]_{\mathcal{B}} \mid [v_2]_{\mathcal{B}}]$ where

$$v_1 = \mathcal{T}(b_1) = \begin{bmatrix} 65 & -24 \\ 149 & 55 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 17 \\ 39 \end{bmatrix}$$

and

$$v_2 = \mathcal{T}(b_2) = \begin{bmatrix} 65 & -24 \\ 149 & 55 \end{bmatrix} \begin{bmatrix} 3 \\ 7 \end{bmatrix} = \begin{bmatrix} 27 \\ 62 \end{bmatrix}.$$

We have computed $[v_1]_{\mathcal{B}}$ and $[v_2]_{\mathcal{B}}$ in Example 2.1.4(3) where we obtained $[v_1]_{\mathcal{B}} = \begin{bmatrix} 2 \\ 5 \end{bmatrix}$ and $[v_2]_{\mathcal{B}} = \begin{bmatrix} 3 \\ 8 \end{bmatrix}$, so $[\mathcal{T}]_{\mathcal{B}} = \begin{bmatrix} 2 & 3 \\ 5 & 8 \end{bmatrix}$. ◇

We shall see further examples of matrices of particularly interesting linear transformations in Example 2.3.18.

2.3 CHANGE OF BASIS

We now investigate how to change coordinates. In our metaphor of coordinates providing a language, changing coordinates is like translating between languages. We look at translation between languages first, in order to guide us later.

Suppose we wish to translate from English to English, for example, or from German to German. We could do this by using an English to English dictionary, or a German to German dictionary, which would look in part like:

English	English
star	star
arrow	arrow

German	German
Stern	Stern
Pfeil	Pfeil

The two columns are identical. Indeed, translating from any language to itself leaves every word unchanged, or to express it mathematically, it is the identity transformation.

Suppose we wish to translate from English to German or from German to English. We could use an English to German dictionary or a German to English dictionary, which would look in part like:

English	German
star	Stern
arrow	Pfeil

German	English
Stern	star
Pfeil	arrow

The effect of translating from German to English is to reverse the effect of translating from English to German, and vice versa. Mathematically, translating from German to English is the inverse of translating from English to German, and vice versa.

Suppose that we wish to translate from English to German but we do not have an English to German dictionary available. However, we do have an English to French dictionary, and a French to German dictionary available, and they look in part like:

English	French
star	étoile
arrow	flèche

French	German
étoile	Stern
flèche	Pfeil

We could translate from English to German by first translating from English to French, and then translating from French to German. Mathematically, translating from English to German is the composition of translating from English to French followed by translating from French to German.

We now turn from linguistics to mathematics.

Let V be an n-dimensional vector space with bases $\mathcal{B} = \{v_1, \ldots, v_n\}$ and $\mathcal{C} = \{w_1, \ldots, w_n\}$. Then we have isomorphisms $\mathcal{S} : V \to \mathbb{F}^n$ given by $\mathcal{S}(v) = [v]_{\mathcal{B}}$, and $\mathcal{T} : V \to \mathbb{F}^n$ given by $\mathcal{T}(v) = [v]_{\mathcal{C}}$. The composition $\mathcal{T} \circ \mathcal{S}^{-1} : \mathbb{F}^n \to \mathbb{F}^n$ is then an isomorphism, and $\mathcal{T} \circ \mathcal{S}^{-1}([v]_{\mathcal{B}}) = [v]_{\mathcal{C}}$. By Lemma 1.1.12, it isomorphism is given by multiplication by a unique (invertible) matrix. We make the following definition.

DEFINITION 2.3.1. Let V be an n-dimensional vector space with bases $\mathcal{B} = \{v_1, \ldots, v_n\}$ and $\mathcal{C} = \{w_1, \ldots, w_m\}$. The *change of basis matrix* $P_{\mathcal{C} \leftarrow \mathcal{B}}$, is the unique matrix such that

$$P_{\mathcal{C} \leftarrow \mathcal{B}}[v]_{\mathcal{B}} = [v]_{\mathcal{C}}$$

for every $v \in V$. $\diamond$

It is easy to write down, at least in principle, $P_{\mathcal{C} \leftarrow \mathcal{B}}$.

Lemma 2.3.2. *In the situation of Definition 2.3.1, the matrix $P_{\mathcal{C} \leftarrow \mathcal{B}}$ is given by*

$$P_{\mathcal{C} \leftarrow \mathcal{B}} = \left[[v_1]_{\mathcal{C}} \mid [v_2]_{\mathcal{C}} \mid \cdots \mid [v_n]_{\mathcal{C}} \right],$$

i.e., $P_{\mathcal{C} \leftarrow \mathcal{B}}$ is the matrix whose ith column is $[v_i]_{\mathcal{C}}$.

Proof. By Lemma 1.2.23, we need only verify the equation $P_{\mathcal{C}\leftarrow\mathcal{B}}[v]_{\mathcal{B}} = [v]_{\mathcal{C}}$ for $v = v_i$, $i = 1, \dots, n$. But $[v_i]_{\mathcal{B}} = e_i$ and $P_{\mathcal{C}\leftarrow\mathcal{B}}e_i$ is the ith column of $P_{\mathcal{C}\leftarrow\mathcal{B}}$, i.e., $P_{\mathcal{C}\leftarrow\mathcal{B}}[v_i]_{\mathcal{B}} = P_{\mathcal{C}\leftarrow\mathcal{B}}e_i = [v_i]_{\mathcal{C}}$ as required. □

REMARK 2.3.3. If we think of $\mathcal{B}$ as the "old" basis, i.e., the one we are translating from, and $\mathcal{C}$ as the "new" basis, i.e., the one we are translating to, then this lemma says that in order to solve the translation problem for an arbitrary vector $v \in V$, we need only solve the translation problem for the old basis vectors, and write down their translations in successive columns to form a matrix. Then multiplication by that matrix does translation for every vector. ◇

We have a theorem that parallels our discussion of translation between human languages.

Theorem 2.3.4. *Let V be a finite-dimensional vector space.*

(1) For any basis $\mathcal{B}$ of V, $P_{\mathcal{B}\leftarrow\mathcal{B}} = I$ is the identity matrix.

(2) For any two bases $\mathcal{B}$ and $\mathcal{C}$ of V, $P_{\mathcal{C}\leftarrow\mathcal{B}}$ is invertible and $(P_{\mathcal{C}\leftarrow\mathcal{B}})^{-1} = P_{\mathcal{B}\leftarrow\mathcal{C}}$.

(3) For any three bases $\mathcal{B}$, $\mathcal{C}$, and $\mathcal{D}$ of V, $P_{\mathcal{D}\leftarrow\mathcal{B}} = P_{\mathcal{D}\leftarrow\mathcal{C}}P_{\mathcal{C}\leftarrow\mathcal{B}}$.

Proof. (1) For any $v \in V$,

$$[v]_{\mathcal{B}} = I[v]_{\mathcal{B}} = P_{\mathcal{B}\leftarrow\mathcal{B}}[v]_{\mathcal{B}},$$

so $P_{\mathcal{B}\leftarrow\mathcal{B}} = I$.

(2) For any $v \in V$,

$$(P_{\mathcal{B}\leftarrow\mathcal{C}}P_{\mathcal{C}\leftarrow\mathcal{B}})[v]_{\mathcal{B}} = P_{\mathcal{B}\leftarrow\mathcal{C}}(P_{\mathcal{C}\leftarrow\mathcal{B}}[v]_{\mathcal{B}}) = P_{\mathcal{B}\leftarrow\mathcal{C}}[v]_{\mathcal{C}} = [v]_{\mathcal{B}},$$

so $P_{\mathcal{B}\leftarrow\mathcal{C}}P_{\mathcal{C}\leftarrow\mathcal{B}} = I$, and similarly $P_{\mathcal{C}\leftarrow\mathcal{B}}P_{\mathcal{B}\leftarrow\mathcal{C}} = I$ so $(P_{\mathcal{C}\leftarrow\mathcal{B}})^{-1} = P_{\mathcal{B}\leftarrow\mathcal{C}}$.

(3) $P_{\mathcal{D}\leftarrow\mathcal{B}}$ is the matrix defined by $P_{\mathcal{D}\leftarrow\mathcal{B}}[v]_{\mathcal{B}} = [v]_{\mathcal{D}}$. But

$$(P_{\mathcal{D}\leftarrow\mathcal{C}}P_{\mathcal{C}\leftarrow\mathcal{B}})[v]_{\mathcal{B}} = P_{\mathcal{D}\leftarrow\mathcal{C}}(P_{\mathcal{C}\leftarrow\mathcal{B}}[v]_{\mathcal{B}}) = P_{\mathcal{D}\leftarrow\mathcal{C}}[v]_{\mathcal{C}} = [v]_{\mathcal{D}},$$

so $P_{\mathcal{D}\leftarrow\mathcal{B}} = P_{\mathcal{D}\leftarrow\mathcal{C}}P_{\mathcal{C}\leftarrow\mathcal{B}}$. □

REMARK 2.3.5. There is no uniform notation for $P_{\mathcal{C}\leftarrow\mathcal{B}}$. We have chosen a notation that we feel is mnemonic: $P_{\mathcal{C}\leftarrow\mathcal{B}}[v]_{\mathcal{B}} = [v]_{\mathcal{C}}$ as the subscript "$\mathcal{B}$" of $[v]_{\mathcal{B}}$ is near the "$\mathcal{B}$" in the subscript "$\mathcal{C} \leftarrow \mathcal{B}$" of $P_{\mathcal{C}\leftarrow\mathcal{B}}$, and this subscript goes to "$\mathcal{C}$", which is the subscript in the answer $[v]_{\mathcal{C}}$. Some other authors denote $P_{\mathcal{C}\leftarrow\mathcal{B}}$ by $P_{\mathcal{C}}^{\mathcal{B}}$ and some by $P_{\mathcal{B}}^{\mathcal{C}}$. The reader should pay careful attention to the author's notation as interchanging the two bases takes the change of basis matrix to its inverse. ◇

REMARK 2.3.6. (1) There is one case in which the change of basis matrix is easy to write down. Suppose $V = \mathbb{F}^n$, $\mathcal{B} = \{v_1, \dots, v_n\}$ is a basis of V, and $\mathcal{E} = \{e_1, \dots, e_n\}$ is the standard basis of V. Then, by Example 2.1.4(1), $[v_i]_{\mathcal{E}} = v_i$, so

$$P_{\mathcal{E}\leftarrow\mathcal{B}} = [v_1 \mid v_2 \mid \cdots \mid v_n].$$

Thus, the change of basis matrix into the standard basis is easy to find.

(2) It is more often the case that we wish to find the change of basis matrix out of the standard basis, i.e., we wish to find $P_{\mathcal{B}\leftarrow\mathcal{E}}$. Then it requires work to find $[e_i]_{\mathcal{B}}$. Instead we may write down $P_{\mathcal{E}\leftarrow\mathcal{B}}$ as in (1) and then find $P_{\mathcal{B}\leftarrow\mathcal{E}}$ by $P_{\mathcal{B}\leftarrow\mathcal{E}} = (P_{\mathcal{E}\leftarrow\mathcal{B}})^{-1}$.

(3) Suppose we have two bases $\mathcal{B}$ and $\mathcal{C}$ of $\mathbb{F}^n$ neither of which is the standard basis. We may find $P_{\mathcal{C}\leftarrow\mathcal{B}}$ directly, or else we may find $P_{\mathcal{C}\leftarrow\mathcal{B}}$ by $P_{\mathcal{C}\leftarrow\mathcal{B}} = P_{\mathcal{C}\leftarrow\mathcal{E}} P_{\mathcal{E}\leftarrow\mathcal{B}} = (P_{\mathcal{E}\leftarrow\mathcal{C}})^{-1} P_{\mathcal{E}\leftarrow\mathcal{B}}$. ◇

Lemma 2.3.7. *Let P be an n-by-n matrix. Then P is a change of basis matrix between two bases of $\mathbb{F}^n$ if and only if P is invertible.*

Proof. Let $P = (p_{ij})$. Choose a basis $\mathcal{C} = \{w_1, \dots, w_n\}$ of V. Let $v_i = \sum_j p_{ij} w_j$. Then $\mathcal{B} = \{v_1, \dots, v_n\}$ is a basis of V if and only if P is invertible, in which case $P = P_{\mathcal{C}\leftarrow\mathcal{B}}$. □

REMARK 2.3.8. Comparing Lemma 2.2.2 and Lemma 2.3.2, we observe that $P_{\mathcal{C}\leftarrow\mathcal{B}} = [\mathcal{I}]_{\mathcal{C}\leftarrow\mathcal{B}}$ where $\mathcal{I} : \mathbb{F}^n \to \mathbb{F}^n$ is the identity linear transformation ($\mathcal{I}(v) = v$ for every v in $\mathbb{F}^n$). ◇

EXAMPLE 2.3.9. Let $V = \mathbb{R}^2$, $\mathcal{E} = \left\{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right\}$, and $\mathcal{B} = \left\{\begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}3\\7\end{bmatrix}\right\}$. Let $v_1 = \begin{bmatrix}17\\39\end{bmatrix}$, so also $[v_1]_{\mathcal{E}} = \begin{bmatrix}17\\39\end{bmatrix}$. We computed directly in Example 2.1.4(3) that $[v_1]_{\mathcal{B}} = \begin{bmatrix}2\\5\end{bmatrix}$. Let $v_2 = \begin{bmatrix}27\\62\end{bmatrix}$, so also $[v_2]_{\mathcal{E}} = \begin{bmatrix}27\\62\end{bmatrix}$. We computed directly in Example 2.1.4(3) that $[v_2]_{\mathcal{B}} = \begin{bmatrix}3\\8\end{bmatrix}$.

We know from Remark 2.3.6(1) that $P_{\mathcal{E}\leftarrow\mathcal{B}} = \begin{bmatrix}1 & 3\\2 & 7\end{bmatrix}$ and from Remark 2.3.6(2) that $P_{\mathcal{B}\leftarrow\mathcal{E}} = \begin{bmatrix}1 & 3\\2 & 7\end{bmatrix}^{-1} = \begin{bmatrix}7 & -3\\-2 & 1\end{bmatrix}$. Then we can easily verify that

$$\begin{bmatrix}2\\5\end{bmatrix} = \begin{bmatrix}7 & -3\\-2 & 1\end{bmatrix}\begin{bmatrix}17\\39\end{bmatrix} \quad\text{and}\quad \begin{bmatrix}3\\8\end{bmatrix} = \begin{bmatrix}7 & -3\\-2 & 1\end{bmatrix}\begin{bmatrix}27\\62\end{bmatrix}.$$ ◇

We shall see further particularly interesting examples of change of basis matrices in Example 2.3.17.

Now we wish to investigate change of basis for linear transformations. Again we will return to our metaphor of language, and see how linguistic transformations work.

Let $\mathcal{T}$ be the transformation that takes an object to several of the same objects, $\mathcal{T}(\star) = \star \star \star \cdots \star$, $\mathcal{T}(\rightarrow) = \rightarrow\rightarrow\rightarrow \cdots \rightarrow$.

This is reflected in the linguistic transformation of taking the plural. Suppose we wish to take the plural of German words, but we do not know how. We consult our German to English and English to German dictionaries:

German	English
Stern	star
Sterne	stars
Pfeil	arrow
Pfeile	arrows

English	German
star	Stern
stars	Sterne
arrow	Pfeil
arrows	Pfeile

We thus see that to take the plural of the German word Stern, we may translate Stern into the English word star, take the plural (i.e., apply our linguistic transformation) of the English word star, and translate this word into German to obtain Sterne, the plural of the German word Stern. Similarly, the path Pfeil $\rightarrow$ arrow $\rightarrow$ arrows $\rightarrow$ Pfeile gives us the plural of the German word Pfeil.

The mathematical analog of this conclusion is the following theorem.

Theorem 2.3.10. *Let V be an n-dimensional vector space and let $\mathcal{T} : V \rightarrow V$ be a linear transformation. Let $\mathcal{B}$ and $\mathcal{C}$ be any two bases of V. Then*

$$[\mathcal{T}]_{\mathcal{C}} = P_{\mathcal{C}\leftarrow\mathcal{B}}[\mathcal{T}]_{\mathcal{B}} P_{\mathcal{B}\leftarrow\mathcal{C}}.$$

Proof. For any vector $v \in V$,

$$\begin{aligned}
\big(P_{\mathcal{C}\leftarrow\mathcal{B}}[\mathcal{T}]_{\mathcal{B}} P_{\mathcal{B}\leftarrow\mathcal{C}}\big)[v]_{\mathcal{C}} &= \big(P_{\mathcal{C}\leftarrow\mathcal{B}}[\mathcal{T}]_{\mathcal{B}}\big) P_{\mathcal{B}\leftarrow\mathcal{C}}[v]_{\mathcal{C}} \\
&= \big(P_{\mathcal{C}\leftarrow\mathcal{B}}[\mathcal{T}]_{\mathcal{B}}\big)[v]_{\mathcal{B}} \\
&= P_{\mathcal{C}\leftarrow\mathcal{B}}\big([\mathcal{T}]_{\mathcal{B}}[v]_{\mathcal{B}}\big) \\
&= P_{\mathcal{C}\leftarrow\mathcal{B}}\big[\mathcal{T}(v)\big]_{\mathcal{B}} = \big[\mathcal{T}(v)\big]_{\mathcal{C}}.
\end{aligned}$$

But $[\mathcal{T}]_{\mathcal{C}}$ is the unique matrix with

$$[\mathcal{T}]_{\mathcal{C}}[v]_{\mathcal{C}} = [\mathcal{T}(v)]_{\mathcal{C}}$$

for every $v \in V$, so we see that $[\mathcal{T}]_{\mathcal{C}} = P_{\mathcal{C}\leftarrow\mathcal{B}}[\mathcal{T}]_{\mathcal{B}} P_{\mathcal{B}\leftarrow\mathcal{C}}$. $\square$

Corollary 2.3.11. *In the situation of Theorem 2.3.10,*

$$\begin{aligned}[\mathcal{T}]_{\mathcal{C}} &= \left(P_{\mathcal{B}\leftarrow\mathcal{C}}\right)^{-1}[\mathcal{T}]_{\mathcal{B}}P_{\mathcal{B}\leftarrow\mathcal{C}} \\ &= P_{\mathcal{C}\leftarrow\mathcal{B}}[\mathcal{T}]_{\mathcal{B}}\left(P_{\mathcal{C}\leftarrow\mathcal{B}}\right)^{-1}.\end{aligned}$$

Proof. Immediate from Theorem 2.3.10 and Theorem 2.3.4(2). □

We are thus led to the following very important definition. (A priori, this definition may seem very unlikely, but in light of our development it is almost forced on us.)

DEFINITION 2.3.12. Two n-by-n matrices A and B are *similar* if there is an invertible matrix P with

$$A = P^{-1}BP. \qquad \diamond$$

REMARK 2.3.13. It is easy to check that similarity is an equivalence relation. ◇

The importance of this definition comes from the following theorem.

Theorem 2.3.14. *Let A and B be n-by-n matrices. Then A and B are similar if and only if they are matrices of the same linear transformation $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$ with respect to a pair of bases of $\mathbb{F}^n$.*

Proof. Immediate from Corollary 2.3.11. □

There is an alternate point of view.

Theorem 2.3.15. *Let V be a finite-dimensional vector space and let $\mathcal{S} : V \to V$ and $\mathcal{T} : V \to V$ be linear transformations. Then $\mathcal{S}$ and $\mathcal{T}$ are conjugate (i.e., $\mathcal{T} = \mathcal{R}^{-1}\mathcal{S}\mathcal{R}$ for some invertible linear transformation $\mathcal{R} : V \to V$) if and only if there are bases $\mathcal{B}$ and $\mathcal{C}$ of V with*

$$[\mathcal{S}]_{\mathcal{B}} = [\mathcal{T}]_{\mathcal{C}}.$$

Proof. If $[\mathcal{S}]_{\mathcal{B}} = [\mathcal{T}]_{\mathcal{C}}$, then by Corollary 2.3.11

$$[\mathcal{S}]_{\mathcal{B}} = [\mathcal{T}]_{\mathcal{C}} = P_{\mathcal{C}\leftarrow\mathcal{B}}[\mathcal{T}]_{\mathcal{B}}P_{\mathcal{C}\leftarrow\mathcal{B}}^{-1}$$

so $[\mathcal{S}]_{\mathcal{B}}$ and $[\mathcal{T}]_{\mathcal{B}}$ are conjugate by the matrix $P_{\mathcal{C}\leftarrow\mathcal{B}}$ and hence, since a linear transformation is determined by its matrix in any basis, $\mathcal{S}$ and $\mathcal{T}$ are conjugate. Conversely, if $\mathcal{T} = \mathcal{R}^{-1}\mathcal{S}\mathcal{R}$ then

$$[\mathcal{T}]_{\mathcal{E}} = [\mathcal{R}^{-1}]_{\mathcal{E}}[\mathcal{S}]_{\mathcal{E}}[\mathcal{R}]_{\mathcal{E}}$$

but $[\mathcal{R}]_{\mathcal{E}}$, being an invertible matrix, is a change of basis matrix $P_{\mathcal{C}\leftarrow\mathcal{B}}$ for some basis $\mathcal{C}$. Then

$$[\mathcal{T}]_{\mathcal{E}} = P_{\mathcal{C}\leftarrow\mathcal{E}}^{-1}[\mathcal{S}]P_{\mathcal{C}\leftarrow\mathcal{E}},$$

so

$$P_{\mathcal{C}\leftarrow\mathcal{E}}[\mathcal{T}]_{\mathcal{E}}P_{\mathcal{C}\leftarrow\mathcal{E}}^{-1} = [\mathcal{S}]_{\mathcal{E}},$$

i.e.,

$$[\mathcal{T}]_{\mathcal{C}} = [\mathcal{S}]_{\mathcal{E}}. \qquad \square$$

EXAMPLE 2.3.16. Let $\mathcal{T} : \mathbb{R}^2 \to \mathbb{R}^2$ be $\mathcal{T} = \mathcal{T}_A$, where $A = \begin{bmatrix} 65 & -24 \\ 149 & 55 \end{bmatrix}$. Let $\mathcal{B} = \left\{\begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 3 \\ 7 \end{bmatrix}\right\}$, a basis of $\mathbb{R}^2$. Then $[\mathcal{T}]_{\mathcal{B}} = P_{\mathcal{B}\leftarrow\mathcal{E}}[\mathcal{T}]_{\mathcal{E}}P_{\mathcal{E}\leftarrow\mathcal{B}} = P_{\mathcal{B}\leftarrow\mathcal{E}}^{-1}[\mathcal{T}]_{\mathcal{E}}P_{\mathcal{B}\leftarrow\mathcal{E}}$. Since $[\mathcal{T}]_{\mathcal{E}} = A$ we see that

$$[\mathcal{T}]_{\mathcal{B}} = \begin{bmatrix} 1 & 3 \\ 2 & 7 \end{bmatrix}^{-1} \begin{bmatrix} 65 & -24 \\ 149 & 55 \end{bmatrix} \begin{bmatrix} 1 & 3 \\ 2 & 7 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 5 & 8 \end{bmatrix},$$

verifying the result of Example 2.2.10, where we computed $[\mathcal{T}]_{\mathcal{B}}$ directly. $\diamond$

EXAMPLE 2.3.17. Let $V = P_n(\mathbb{R})$ and let $\mathcal{B}$ and $\mathcal{C}$ be the bases

$$\mathcal{B} = \{1, x, x^{(2)}, x^{(3)}, \ldots, x^{(n)}\},$$

where $x^{(i)} = x(x-1)(x-2)\cdots(x-i+1)$, and

$$\mathcal{C} = \{1, x, x^2, \ldots, x^n\}.$$

Let $P = (p_{ij}) = P_{\mathcal{C}\leftarrow\mathcal{B}}$ and $Q = (q_{ij}) = P_{\mathcal{B}\leftarrow\mathcal{C}} = P^{-1}$. The entries p_{ij} are called *Stirling numbers of the first kind* and the entries q_{ij} are called *Stirling numbers of the second kind*. Here we number the rows/columns of the respective matrices from 0 to n, not from 1 to $n+1$. For example, if $n = 5$ we have

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 2 & -6 & 24 \\ 0 & 0 & 1 & -3 & 11 & -50 \\ 0 & 0 & 0 & 1 & -6 & 35 \\ 0 & 0 & 0 & 0 & 1 & -10 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad Q = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 3 & 7 & 15 \\ 0 & 0 & 0 & 1 & 6 & 25 \\ 0 & 0 & 0 & 0 & 1 & 10 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

(The numbers p_{ij} and q_{ij} are independent of n as long as $i, j \leq n$.) $\diamond$

EXAMPLE 2.3.18. Let $V = P_5(\mathbb{R})$ with bases $\mathcal{B} = \{1, x, \ldots, x^{(5)}\}$ and $\mathcal{C} = \{1, x, \ldots, x^5\}$ as in Example 2.3.17.

(1) Let $\mathbf{D} : V \to V$ be differentiation, $\mathbf{D}(p(x)) = p'(x)$. Then

$$[\mathbf{D}]_{\mathcal{B}} = \begin{bmatrix} 0 & 1 & -1 & 2 & -6 & 24 \\ 0 & 0 & 2 & -6 & 22 & -100 \\ 0 & 0 & 0 & 3 & -18 & -105 \\ 0 & 0 & 0 & 0 & 4 & -40 \\ 0 & 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{and} \quad [\mathbf{D}]_{\mathcal{C}} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

so these two matrices are similar. Indeed,

$$[\mathbf{D}]_{\mathcal{B}} = P^{-1}[\mathbf{D}]_{\mathcal{C}} P = Q[\mathbf{D}]_{\mathcal{C}} Q^{-1}$$

where P and Q are the matrices of Example 2.3.17.

(2) Let $\Delta : V \to V$ be the forward difference operator, $\Delta(p(x)) = p(x+1) - p(x)$. Then

$$[\Delta]_{\mathcal{B}} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{and} \quad [\Delta]_{\mathcal{C}} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 2 & 3 & 4 & 5 \\ 0 & 0 & 0 & 3 & 6 & 10 \\ 0 & 0 & 0 & 0 & 4 & 10 \\ 0 & 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

so these two matrices are similar. Again,

$$[\Delta]_{\mathcal{B}} = P^{-1}[\Delta]_{\mathcal{C}} P = Q[\Delta]_{\mathcal{C}} Q^{-1}$$

where P and Q are the matrices of Example 2.3.17.

(3) Since $[\mathbf{D}]_{\mathcal{C}} = [\Delta]_{\mathcal{B}}$, we see that $\mathbf{D} : V \to V$ and $\Delta : V \to V$ are conjugate. $\diamond$

2.4 THE MATRIX OF THE DUAL

Let $\mathcal{T} : V \to X$ be a linear transformation between finite-dimensional vector spaces. Once we choose bases $\mathcal{B}$ and $\mathcal{C}$ of V and X respectively, we can represent $\mathcal{T}$ by a unique matrix $[\mathcal{T}]_{\mathcal{C} \leftarrow \mathcal{B}}$. We also have the dual linear transformation $\mathcal{T}^* : X^* \to V^*$ and the dual bases $\mathcal{C}^*$ and $\mathcal{B}^*$ of X^* and V^* respectively, and it is natural to consider the matrix $[\mathcal{T}^*]_{\mathcal{B}^* \leftarrow \mathcal{C}^*}$.

DEFINITION 2.4.1. Let $\mathcal{T} : V \to X$ be a linear transformation between finite dimensional vector spaces, and let A be the matrix $A = [\mathcal{T}]_{\mathcal{C} \leftarrow \mathcal{B}}$. The *transpose* of A is the matrix ${}^tA$ given by ${}^tA = [\mathcal{T}^*]_{\mathcal{B}^* \leftarrow \mathcal{C}^*}$. ◇

Let us first see that this gives the usual definition of the transpose of a matrix.

Lemma 2.4.2. *Let $A = (a_{ij})$ be an m-by-n matrix. Then $B = {}^tA = (b_{ij})$ is the n-by-m matrix with entries $b_{ij} = a_{ji}$, $i = 1, \ldots, m$, $j = 1, \ldots, n$.*

Proof. Let $\mathcal{B} = \{v_1, \ldots, v_n\}$, $\mathcal{B}^* = \{w_1^*, \ldots, w_n^*\}$, $\mathcal{C} = \{x_1, \ldots, x_m\}$, and $\mathcal{C}^* = \{y_1^*, \ldots, y_m^*\}$. Then, by definition,

$$\mathcal{T}(v_j) = \sum_{k=1}^{m} a_{kj} x_k \quad \text{for } j = 1, \ldots, n$$

and

$$\mathcal{T}^*(y_i^*) = \sum_{k=1}^{n} b_{ki} w_k^* \quad \text{for } i = 1, \ldots, m.$$

Now

$$y_i^*(\mathcal{T}(v_j)) = a_{ij} \quad \text{as } y_i^*(x_i) = 1,\ y_i^*(x_k) = 0 \text{ for } k \neq i$$

and

$$(\mathcal{T}^*(y_i^*))(v_j) = b_{ji} \quad \text{as } w_j^*(v_j) = 1,\ w_k^*(v_j) = 0 \text{ for } k \neq j.$$

By the definition of $\mathcal{T}^*$, for any $y^* \in X^*$ and any $v \in V$

$$(\mathcal{T}^*(y^*))(v) = y^*(\mathcal{T}(v))$$

so we see $b_{ji} = a_{ij}$, as claimed. □

REMARK 2.4.3. Every matrix is the matrix of a linear transformation with respect to a pair of bases, so ${}^tA$ is defined for any matrix A. Our definition appears to depend on the choice of the bases $\mathcal{B}$ and $\mathcal{C}$, so to see that ${}^tA$ is well-defined we must show it is independent of the choice of bases. This follows from first principles, but it is easier to observe that Lemma 2.4.2 gives a formula for ${}^tA$ that is independent of the choice of bases. ◇

REMARK 2.4.4. It easy to see that ${}^t(A_1 + A_2) = {}^tA_1 + {}^tA_2$ and that ${}^t(cA) = c\,{}^tA$. ◇

Other properties of the transpose are a little more subtle.

Lemma 2.4.5. ${}^t(AB) = {}^tB\,{}^tA$.

Proof. Let $\mathcal{T} : V \to X$ with $[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}} = B$ and let $\mathcal{S} : X \to Z$ with $[\mathcal{T}]_{\mathcal{D}\leftarrow\mathcal{C}} = A$. Then, as we have seen, $\mathcal{S}\circ\mathcal{T} : V \to Z$ with $[\mathcal{S}\circ\mathcal{T}]_{\mathcal{D}\leftarrow\mathcal{B}} = AB$. By Definition 2.4.1 and Lemma 1.6.23,

$$\begin{aligned}{}^t(AB) &= [(\mathcal{S}\circ\mathcal{T})^*]_{\mathcal{B}^*\leftarrow\mathcal{D}^*} = [\mathcal{T}^*\circ\mathcal{S}^*]_{\mathcal{B}^*\leftarrow\mathcal{D}^*}\\ &= [\mathcal{T}^*]_{\mathcal{B}^*\leftarrow\mathcal{C}^*}[\mathcal{S}^*]_{\mathcal{C}^*\leftarrow\mathcal{D}^*} = {}^tB\,{}^tA.\end{aligned}$$ □

Lemma 2.4.6. *Let A be an invertible matrix. Then,* ${}^t(A^{-1}) = ({}^tA)^{-1}$.

Proof. Clearly if $\mathcal{T} : V \to V$ is the identity, then $\mathcal{T}^* : V^* \to V^*$ is the identity, ($w^*(\mathcal{T}(v)) = w^*(v) = (\mathcal{T}^*(w^*))(v)$ if $\mathcal{T}$ and $\mathcal{T}^*$ are both the respective identities). Choose a basis $\mathcal{B}$ of V and let $\mathcal{R} : V \to V$ be the linear transformation with $[\mathcal{R}]_{\mathcal{B}} = A$. Then $[\mathcal{R}^{-1}]_{\mathcal{B}} = A^{-1}$, and

$$\begin{aligned}I &= [\mathcal{I}]_{\mathcal{B}} = \left[\mathcal{I}^*\right]_{\mathcal{B}^*} = \left[\left(\mathcal{R}^{-1}\circ\mathcal{R}\right)^*\right]_{\mathcal{B}^*}\\ &= \left[\mathcal{R}^*\right]_{\mathcal{B}^*}\left[\left(\mathcal{R}^{-1}\right)^*\right]_{\mathcal{B}^*} = {}^tA\,{}^t\left(A^{-1}\right),\end{aligned}$$

and

$$\begin{aligned}I &= [\mathcal{I}]_{\mathcal{B}} = \left[\mathcal{I}^*\right]_{\mathcal{B}^*} = \left[\left(\mathcal{R}\circ\mathcal{R}^{-1}\right)^*\right]_{\mathcal{B}^*}\\ &= \left[\left(\mathcal{R}^{-1}\right)^*\right]_{\mathcal{B}^*}\left[\mathcal{R}^*\right]_{\mathcal{B}^*} = {}^t\left(A^{-1}\right){}^tA.\end{aligned}$$ □

As an application of these ideas, we have a theorem from elementary linear algebra.

Theorem 2.4.7. *Let A be an m-by-n matrix. Then the row rank of A and the column rank of A are equal.*

Proof. Let $\mathcal{T} = \mathcal{T}_A : \mathbb{F}^n \to \mathbb{F}^m$ be given by $\mathcal{T}(v) = Av$. Then $[\mathcal{T}]_{\mathcal{E}_m\leftarrow\mathcal{E}_n} = A$, so the column rank of A, which is the dimension of the subspace of $\mathbb{F}^m$ spanned by the columns of A, is the dimension of the subspace $\operatorname{Im}(\mathcal{T})$ of $\mathbb{F}^m$.

Consider the dual $\mathcal{T}^* : (\mathbb{F}^m)^* \to (\mathbb{F}^n)^*$. As we have seen, $[\mathcal{T}^*]_{\mathcal{E}_n^*\leftarrow\mathcal{E}_m^*} = {}^tA$, so the column rank of ${}^tA$ is equal to the dimension of $\operatorname{Im}(\mathcal{T}^*)$. By Corollary 1.6.20, $\dim\operatorname{Im}(\mathcal{T}^*) = \dim\operatorname{Im}(\mathcal{T})$, and obviously the column space of ${}^tA$ is identical to the row space of A. □

We have considered the dual. Now let us consider the double dual. In Lemma 1.6.26 we defined the linear transformation $\mathcal{H}$ from a vector space to its double dual.

Lemma 2.4.8. *Let $\mathcal{T} : V \to X$ be a linear transformation between finite-dimensional $\mathbb{F}$-vector spaces. Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a basis of V and $\mathcal{C} = \{x_1, \ldots, x_m\}$ be a basis of X.*

Let $\mathcal{B}^{**} = \{v_1^{**}, \ldots, v_n^{**}\}$ and $\mathcal{C}^{**} = \{x_1^{**}, \ldots, x_m^{**}\}$, bases of V^{**} and X^{**} respectively (where $v_i^{**} = \mathcal{H}(v_i)$ and $x_j^{**} = \mathcal{H}(x_j)$). Then

$$\left[\mathcal{T}^{**}\right]_{\mathcal{C}^{**} \leftarrow \mathcal{B}^{**}} = [\mathcal{T}]_{\mathcal{C} \leftarrow \mathcal{B}}.$$

Proof. An inspection of Definition 1.6.29 shows that $\mathcal{T}^{**}$ is the composition $\mathcal{H} \circ \mathcal{T} \circ \mathcal{H}^{-1}$ where the right-hand $\mathcal{H}$ is $\mathcal{H} : V \to V^{**}$ and the left-hand $\mathcal{H}$ is $\mathcal{H} : W \to W^{**}$. But $[\mathcal{H}]_{\mathcal{B}^{**} \leftarrow \mathcal{B}} = I$ and $[\mathcal{H}]_{\mathcal{C}^{**} \leftarrow \mathcal{C}} = I$ so

$$\begin{aligned} \left[\mathcal{T}^{**}\right]_{\mathcal{C}^{**} \leftarrow \mathcal{B}^{**}} &= [\mathcal{H}]_{\mathcal{C}^{**} \leftarrow \mathcal{C}} [\mathcal{T}]_{\mathcal{C} \leftarrow \mathcal{B}} [\mathcal{H}^{-1}]_{\mathcal{B} \leftarrow \mathcal{B}^{**}} \\ &= I [\mathcal{T}]_{\mathcal{C} \leftarrow \mathcal{B}} I^{-1} = [\mathcal{T}]_{\mathcal{C} \leftarrow \mathcal{B}}. \end{aligned}$$ □

The following corollary is obvious from direct computation but we present another proof.

Corollary 2.4.9. *Let A be an m-by-n matrix. Then ${}^t({}^tA) = A$.*

Proof. Let $\mathcal{T} : V \to W$ be a linear transformation with $[\mathcal{T}]_{\mathcal{C} \leftarrow \mathcal{B}} = A$. Then by Lemma 2.4.8,

$$A = [\mathcal{T}]_{\mathcal{C} \leftarrow \mathcal{B}} = [\mathcal{T}^{**}]_{\mathcal{C}^{**} \leftarrow \mathcal{B}^{**}} = {}^t\big({}^t[\mathcal{T}]_{\mathcal{C} \leftarrow \mathcal{B}}\big) = {}^t\big({}^tA\big),$$

as $\mathcal{T}^{**}$ is the dual of the dual of $\mathcal{T}$. □

CHAPTER 3

Determinants

In this chapter we deal with the determinant of a square matrix. The determinant has a simple geometric meaning, that of signed volume, and we use that to develop it in Section 3.1. We then present a more traditional and fuller development in Section 3.2. In Section 3.3 we derive important and useful properties of the determinant. In Section 3.4 we consider integrality questions, e.g., the question of the existence of integer (not just rational) solutions of the linear system $Ax = b$, a question best answered using determinants. In Section 3.5 we consider orientations, and see how to explain the meaning of the sign of the determinant in the case of real vector spaces. In Section 3.6 we present an interesting family of examples, the Hilbert matrices.

3.1 The geometry of volumes

The determinant of a matrix A has a simple geometric meaning. It is the (signed) volume of the image of the unit cube under the linear transformation $\mathcal{T}_A$.

We will begin by doing some elementary geometry to see what properties (signed) volume should have, and use that as the basis for the not-so-simple algebraic definition.

Henceforth we drop the word "signed" and just refer to volume.

In considering properties that volume should have, suppose we are working in $\mathbb{R}^2$, where volume is area. Let A be the matrix $A = [v_1 \mid v_2]$. The unit square in $\mathbb{R}^2$ is the parallelogram determined by the standard unit vectors e_1 and e_2. $\mathcal{T}_A(e_1) = v_1$ and $\mathcal{T}_A(e_2) = v_2$, so we are looking at the area of the parallelogram P determined by v_1 and v_2, the two columns of A.

The area of a parallelogram should certainly have the following two properties:

(1) If we multiply one side of P by a number c, e.g., if we replace P by the parallelogram P' determined by v_1 and cv_2, the area of P' should be c times the area of P.

(2) If we add a multiple of one side of P to another, e.g., if we replace P by the parallelogram P' determined by v_1 and $v_2 + cv_1$, the area of P' should be the same as the area of P. (To see this, note that the area of a parallelogram is base times height, and while this operation changes the shape of the parallelogram, it does not change its base or its height.)

Property (1) should in particular hold if $c = 0$, when one of the sides becomes the zero vector, in which case the parallelogram degenerates to a line (or to a point if both sides are the zero vector), and a line or a point has area 0.

We now consider an arbitrary field $\mathbb{F}$, and consider n-by-n matrices. We are still guided by properties (1) and (2), extending them to n-by-n matrices using the idea that if only one or two columns are changed as in (1) or (2), and the other $n-1$ or $n-2$ columns are unchanged, then the volume should change as in (1) or (2). We are thus led to the following definition.

DEFINITION 3.1.1. A volume function $\mathrm{Vol} : M_n(\mathbb{F}) \to \mathbb{F}$ is a function satisfying the properties:

(1) For any scalar c, and any i,

$$\begin{aligned}&\mathrm{Vol}\left(\left[v_1 \mid \cdots \mid v_{i-1} \mid cv_i \mid v_{i+1} \mid \cdots \mid v_n\right]\right)\\&\quad = c\,\mathrm{Vol}\left(\left[v_1 \mid \cdots \mid v_{i-1} \mid v_i \mid v_{i+1} \mid \cdots \mid v_n\right]\right).\end{aligned}$$

(2) For any scalar c, and any $j \neq i$,

$$\begin{aligned}&\mathrm{Vol}\left(\left[v_1 \mid \cdots \mid v_{i-1} \mid v_i + cv_j \mid v_{i+1} \mid \cdots \mid v_n\right]\right)\\&\quad = \mathrm{Vol}\left(\left[v_1 \mid \cdots \mid v_{i-1} \mid v_i \mid v_{i+1} \mid \cdots \mid v_n\right]\right).\end{aligned}$$

Note we have not shown that Vol exists, but we will proceed on the assumption it does to derive properties that it must have, and we will use them to prove existence.

As we have defined it, Vol cannot be unique, as we can scale it by an arbitrary factor. Once we specify the scale we obtain a unique function that we will denote by Vol_1, and we will let the determinant be Vol_1. But it is convenient to work with arbitrary volume functions and normalize the result at the end. Vol_1 (or the determinant) will be Vol scaled so that the signed volume of the unit n-cube, with the columns arranged in the standard order, is $+1$. ◇

Lemma 3.1.2. *(1) If some column of A is zero, then* $\mathrm{Vol}(A) = 0$.

(2) If the columns of A are not linearly independent, then $\mathrm{Vol}(A) = 0$. *In particular, if two columns of A are equal, then* $\mathrm{Vol}(A) = 0$.

(3)

$$\begin{aligned} &\mathrm{Vol}\left(\left[v_1 \mid \cdots \mid v_j \mid \cdots \mid v_i \mid \cdots \mid v_n\right]\right) \\ &\qquad = -\mathrm{Vol}\left(\left[v_1 \mid \cdots \mid v_i \mid \cdots \mid v_j \mid \cdots \mid v_n\right]\right). \end{aligned}$$

(4)

$$\begin{aligned} &\mathrm{Vol}\left(\left[v_1 \mid \cdots \mid au + bw \mid \cdots \mid v_n\right]\right) \\ &\qquad = a\,\mathrm{Vol}\left(\left[v_1 \mid \cdots \mid u \mid \cdots \mid v_n\right]\right) \\ &\qquad\quad + b\,\mathrm{Vol}\left(\left[v_1 \mid \cdots \mid w \mid \cdots \mid v_n\right]\right). \end{aligned}$$

Proof. (1) Let $v_i = 0$. Then $v_i = 0v_i$, so by property (1)

$$\mathrm{Vol}\left(\left[v_1 \mid \cdots \mid v_i \mid \cdots \mid v_n\right]\right) = 0 \cdot \mathrm{Vol}\left(\left[v_1 \mid \cdots \mid v_i \mid \cdots \mid v_n\right]\right) = 0.$$

(2) Let $v_i = a_1v_1 + a_2v_2 + \cdots + a_{i-1}v_{i-1} + a_{i+1}v_{i+1} + \cdots + a_nv_n$. Let $v_i' = a_2v_2 + \cdots + a_{i-1}v_{i-1} + a_{i+1}v_{i+1} + \cdots + a_nv_n$, so that $v_i = a_1v_1 + v_i'$. Then, applying property (2),

$$\begin{aligned} \mathrm{Vol}\left(\left[v_1 \mid \cdots \mid v_i \mid \cdots \mid v_n\right]\right) &= \mathrm{Vol}\left(\left[v_1 \mid \cdots \mid a_1v_1 + v_i' \mid \cdots \mid v_n\right]\right) \\ &= \mathrm{Vol}\left(\left[v_1 \mid \cdots \mid v_i' \mid \cdots \mid v_n\right]\right). \end{aligned}$$

Proceeding in the same way, applying property (2) repeatedly, we obtain

$$\mathrm{Vol}\left(\left[v_1 \mid \cdots \mid v_i \mid \cdots \mid v_n\right]\right) = \mathrm{Vol}\left(\left[v_1 \mid \cdots \mid 0 \mid \cdots \mid v_n\right]\right) = 0.$$

(3)

$$\begin{aligned} &\mathrm{Vol}\left(\left[v_1 \mid \cdots \mid v_j \mid \cdots \mid v_i \mid \cdots \mid v_n\right]\right) \\ &\qquad = \mathrm{Vol}\left(\left[v_1 \mid \cdots \mid v_j \mid \cdots \mid v_j + v_i \mid \cdots \mid v_n\right]\right) \\ &\qquad = \mathrm{Vol}\left(\left[v_1 \mid \cdots \mid -v_i \mid \cdots \mid v_j + v_i \mid \cdots \mid v_n\right]\right) \\ &\qquad = \mathrm{Vol}\left(\left[v_1 \mid \cdots \mid -v_i \mid \cdots \mid v_j \mid \cdots \mid v_n\right]\right) \\ &\qquad = -\mathrm{Vol}\left(\left[v_1 \mid \cdots \mid v_i \mid \cdots \mid v_j \mid \cdots \mid v_n\right]\right). \end{aligned}$$

(4) First, suppose $\{v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n\}$ is not linearly independent. Then, by part (3), the equation in (4) becomes $0 = a \cdot 0 + b \cdot 0$, which is true.

Now for the heart of the proof. Suppose $\{v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n\}$ is linearly independent. By Corollary 1.2.10(1), we may extend this set to a basis $\{v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n, z\}$ of $\mathbb{F}^n$. Then we may write

$$\begin{aligned} u &= c_1 v_1 + \cdots + c_{i-1} v_{i-1} + c_{i+1} v_{i+1} + \cdots + c_n v_n + c' z, \\ w &= d_1 v_1 + \cdots + d_{i-1} v_{i-1} + d_{i+1} v_{i+1} + \cdots + d_n v_n + d' z. \end{aligned}$$

Let $v = au + bw$. Then

$$v = e_1 v_1 + \cdots + e_{i-1} v_{i-1} + e_{i+1} v_{i+1} + \cdots + e_n v_n + e' z$$

where $e' = ac' + bd'$.

Applying property (2) repeatedly, and property (1), we see that

$$\begin{aligned} \operatorname{Vol}\left(\left[v_1 \mid \cdots \mid v \mid \cdots \mid v_n\right]\right) &= e' \operatorname{Vol}\left(\left[v_1 \mid \cdots \mid z \mid \cdots \mid v_n\right]\right), \\ \operatorname{Vol}\left(\left[v_1 \mid \cdots \mid u \mid \cdots \mid v_n\right]\right) &= c' \operatorname{Vol}\left(\left[v_1 \mid \cdots \mid z \mid \cdots \mid v_n\right]\right), \\ \operatorname{Vol}\left(\left[v_1 \mid \cdots \mid w \mid \cdots \mid v_n\right]\right) &= d' \operatorname{Vol}\left(\left[v_1 \mid \cdots \mid z \mid \cdots \mid v_n\right]\right), \end{aligned}$$

yielding the theorem. □

REMARK 3.1.3. Setting $v_i = v_j = z$ (z arbitrary) in Lemma 3.1.2(3) gives $2\operatorname{Vol}([v_1 \mid \cdots \mid z \mid \cdots \mid z \mid \cdots \mid v_n]) = 0$ and hence $\operatorname{Vol}([v_1 \mid \cdots \mid z \mid \cdots \mid z \mid \cdots \mid v_n]) = 0$ if $\mathbb{F}$ does not have characteristic z. This latter condition is stronger if $\operatorname{char}(\mathbb{F}) = 2$, and it is this stronger condition, coming directly from the geometry, that we need. ◇

Theorem 3.1.4. *A function $f : M_n(\mathbb{F}) \to \mathbb{F}$ is a volume function if and only if it satisfies:*

(1) Multilinearity: If $A = [v_1 \mid \cdots \mid v_n]$ with $v_i = au + bw$ for some i, then

$$\begin{aligned} f\left(\left[v_1 \mid \cdots \mid v_i \mid \cdots \mid v_n\right]\right) = {} & af\left(\left[v_1 \mid \cdots \mid u \mid \cdots \mid v_n\right]\right) \\ & + bf\left(\left[v_1 \mid \cdots \mid w \mid \cdots \mid v_n\right]\right). \end{aligned}$$

(2) Alternation: If $A = [v_1 \mid \cdots \mid v_n]$ with $v_i = v_j$ for some $i \neq j$, then

$$f\left(\left[v_1 \mid \cdots \mid v_n\right]\right) = 0.$$

Proof. We have seen that any volume function satisfies Lemma 3.1.2(3) and (4), which gives alternation and multilinearity. Conversely, it is easy to see that multilinearity and alternation give properties (1) and (2) in Definition 3.1.1. □

REMARK 3.1.5. The conditions of Theorem 3.1.4 are usually taken to be the definition of a volume function. ◇

REMARK 3.1.6. In characteristic 2, the function $f\left(\left[\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right]\right) = ac$ is multilinear and satisfies $f([v_2 \mid v_1]) = f([v_1 \mid v_2]) = -f([v_1 \mid v_2])$, but is not alternating. ◇

Theorem 3.1.7. *Suppose there exists a nontrivial volume function* $\mathrm{Vol} : M_n(\mathbb{F}) \to \mathbb{F}$. *Then there is a unique volume function* Vol_1 *satisfying* $\mathrm{Vol}_1(I) = 1$. *Furthermore, any volume function is* Vol_a *for some* $a \in \mathbb{F}$, *where* Vol_a *is the function* $\mathrm{Vol}_a(A) = a\,\mathrm{Vol}_1(A)$.

Proof. Let A be a matrix with $\mathrm{Vol}(A) \neq 0$. Then, by Lemma 3.1.2(2), A must be nonsingular. Then there is a sequence of elementary column operations taking A to I. By Definition 3.1.1(1) and (2), and by Lemma 3.1.2(4), each of these operations has the effect of multiplying $\mathrm{Vol}(A)$ by a nonzero scalar, so $\mathrm{Vol}(I) \neq 0$.

Any scalar multiple of a volume function is a volume function, so we may obtain a volume function Vol_1 by $\mathrm{Vol}_1(A) = (1/\mathrm{Vol}(I))\,\mathrm{Vol}(A)$, and clearly $\mathrm{Vol}_1(I) = 1$. Then set $\mathrm{Vol}_a(A) = a\,\mathrm{Vol}_1(A)$.

Now let f be any volume function. Set $a = f(I)$. If A is singular, then $f(A) = 0$. Suppose A is nonsingular. Then there is a sequence of column operations taking I to A, and each of these column operations has the effect of multiplying the value of any volume function by a nonzero constant independent of the choice of volume function. Thus, if we let b be the product of these constants, we have

$$f(A) = bf(I) = ba = b\,\mathrm{Vol}_a(I) = \mathrm{Vol}_a(A),$$

so $f = \mathrm{Vol}_a$. In particular, if f is any volume function with $f(I) = 1$, then $f = \mathrm{Vol}_1$, which shows that Vol_1 is unique. □

Note the proof of this theorem does not show that Vol_1 exists, as a priori we could choose two different sequences of elementary column operations to get from I to A and obtain two different values for $\mathrm{Vol}_1(A)$. In fact Vol_1 does exist, as we now see.

Theorem 3.1.8. *There is a unique volume function* $\mathrm{Vol}_1 : M_n(\mathbb{F}) \to \mathbb{F}$ *with* $\mathrm{Vol}_1(I) = 1$.

Proof. We proceed by induction on n. For $n = 1$ we define $\det([a]) = a$.

Suppose det is defined on $(n-1)$-by-$(n-1)$ matrices. We define det on n-by-n matrices by

$$\det(A) = \sum_{j=1}^{n} (-1)^{1+j} a_{1j} \det(M_{1j})$$

where $A = (a_{ij})$ and M_{1j} is the $(n-1)$-by-$(n-1)$ matrix obtained by deleting row 1 and column j of A. (M_{1j} is known as the $(1, j)$-minor of A.)

We need to check that the properties of a volume function are satisfied. Instead of checking the properties in Definition 3.1.1 directly, we will check the equivalent properties in Theorem 3.1.4. We use the notation of that theorem.

We prove the properties of det by induction on n. We assume that det has the properties of a volume function given in Theorem 3.1.4 for $(n-1)$-by-$(n-1)$ matrices, and in particular that the conclusions of Lemma 3.1.2 hold for det on $(n-1)$-by-$(n-1)$ matrices.

We first prove multilinearity. In the notation of Theorem 3.1.4, let $v_i = au + bw$, and let $A = (a_{ij})$. Then $a_{1i} = au^1 + bw^1$, where u^1 and w^1 are the first entries of u and w respectively. Also, $M_{1i} = [v_1 \mid \cdots \mid v_{i-1} \mid v_{i+1} \mid \cdots \mid v_n]$. Inspecting the sum for $\det(A)$, and applying Lemma 3.1.2(4), we see that multilinearity holds.

We next prove alternation. Again follow the notation of Theorem 3.1.4 and let $v_i = v_j$ for some $i \neq j$. If $k \neq i$ and $k \neq j$, the minor M_{1k} has two identical columns and so by Lemma 3.1.2(2), $\det(M_{1k}) = 0$. Then, inspecting the sum for $\det(A)$, we see that it reduces to

$$\det(A) = (-1)^{1+i} a_{1i} \det\left(M_{1i}\right) + (-1)^{1+j} a_{1j} \det\left(M_{1j}\right)$$

with $a_{1i} = a_{1j}$. Let $i < j$. Then

$$M_{1i} = \left[\overline{v}_1 \mid \cdots \mid \overline{v}_{i-1} \mid \overline{v}_{i+1} \mid \cdots \mid \overline{v}_{j-1} \mid \overline{v}_j \mid \overline{v}_{j+1} \mid \cdots \mid \overline{v}_n\right]$$

and

$$M_{1j} = \left[\overline{v}_1 \mid \cdots \mid \overline{v}_{i-1} \mid \overline{v}_j \mid \overline{v}_{i+1} \mid \cdots \mid \overline{v}_{j-1} \mid \overline{v}_{j+1} \mid \cdots \mid \overline{v}_n\right],$$

where $\overline{v}_k$ is the vector obtained from v_k by deleting its first entry, and $\overline{v}_i = \overline{v}_j$.

We may obtain M_{1i} from M_{1j} as follows: First interchange $\overline{v}_i$ with $\overline{v}_{i+1}$, then interchange $\overline{v}_i$ with $\overline{v}_{i+2}, \ldots$, and finally interchange $\overline{v}_i$ with $\overline{v}_{j-1}$. There is a total of $j - i - 1$ interchanges, and by Lemma 3.1.2(3) each interchange has the effect of multiplying det by -1, so we see that

$$\det(M_{1i}) = (-1)^{j-i-1} \det(M_{1j}).$$

Hence, letting $a = a_{1j}$ and $m = \det(M_{1j})$,

$$\begin{aligned}\det(A) &= (-1)^{1+i} a(-1)^{j-i-1} m + (-1)^{1+j} am \\ &= (-1)^j am\bigl(1 + (-1)\bigr) = 0.\end{aligned}$$

Finally, $\det([1]) = 1$ and by induction we have that $\det(I_n) = 1 \cdot \det(I_{n-1}) = 1$, where I_n (respectively I_{n-1}) denotes the n-by-n (respectively $(n-1)$-by-$(n-1)$) identity matrix. □

DEFINITION 3.1.9. The unique volume function Vol_1 is the *determinant* function, denoted $\det(A)$. ◇

Corollary 3.1.10. *Let A be an n-by-n matrix. Then* $\det(A) \neq 0$ *if and only if A is nonsingular.*

Proof. By Lemma 3.1.2(2), for any volume function Vol_a, $\mathrm{Vol}_a(A) = 0$ if A is singular. For any nontrivial volume function, i.e., for any function Vol_a with $a \neq 0$, we observed in the course of the proof of Theorem 3.1.7 that, for any nonsingular matrix A, $\mathrm{Vol}_a(A) = c\,\mathrm{Vol}_a(I) = ca$ for some $c \neq 0$. □

REMARK 3.1.11. Let us give a heuristic argument as to why Corollary 3.1.10 should be true, from a geometric viewpoint. Let $A = [v_1 \mid \cdots \mid v_n]$ be an n-by-n matrix. Then $v_i = Ae_i = \mathcal{T}_A(e_i)$, $i = 1, \ldots, n$, where $I = [e_1 \mid \cdots \mid e_n]$. Thus the n-parallelogram P spanned by the columns of A is the image of the unit n-cube under the linear transformation $\mathcal{T}_A$, and the determinant of A is the signed volume of P.

If $\det(A) \neq 0$, i.e., if P has nonzero volume, then the translates of P "fill up" $\mathbb{F}^n$, and so for any $w \in \mathbb{F}^n$, there is a $v \in \mathbb{F}^n$ with $\mathcal{T}_A(v) = Av = w$. Thus in this case $\mathcal{T}_A$ is onto $\mathbb{F}^n$, and hence is an isomorphism by Corollary 1.3.2, so A is invertible.

If $\det(A) = 0$, i.e., if P has zero volume, then it is a degenerate n-parallelogram, and so is a nondegenerate k-parallelogram for some $k < n$, and its translates only "fill up" a k-dimensional subspace of $\mathbb{F}^n$. Thus in this case $\mathcal{T}_A$ is not onto $\mathbb{F}^n$, and hence A is not invertible. $\diamond$

REMARK 3.1.12. Another well-known and important property of determinants, that we shall prove in Theorem 3.3.1, is that for any two n-by-n matrices A and B, $\det(AB) = \det(A)\det(B)$. Let us also give a heuristic argument as to why this should be true, again from a geometric viewpoint. But we need to change our viewpoint slightly, from a "static" one to a "dynamic" one. In the notation of Remark 3.1.11,

$$\begin{aligned}\det\left[v_1 \mid \cdots \mid v_n\right] &= \det(A) = \det(A)\cdot 1 = \det(A)\det(I)\\ &= \det(A)\det\left(\left[e_1 \mid \cdots \mid e_n\right]\right).\end{aligned}$$

We then think of the determinant of A as the factor by which the linear transformation $\mathcal{T}_A$ multiplies signed volume when it takes the unit n-cube to the n-parallelogram P. A linear transformation is homogeneous in that it multiplies each "bit" of signed volume by the same factor. That is, if instead of starting with I we start with any n-parallelogram J and take its image Q under the linear transformation $\mathcal{T}_A$, the signed volume of Q will be $\det(A)$ times the signed volume of J.

To apply this we begin with the linear transformation $\mathcal{T}_B$ and let J be the n-parallelogram that is the image of I under $\mathcal{T}_B$.

In going from I to J, i.e., in taking the image of I under $\mathcal{T}_B$, we multiply signed volume by $\det(B)$, and in going from J to Q, i.e., in taking the image of J under $\mathcal{T}_A$, we multiply signed volume by $\det(A)$, so in going from I to Q, i.e., in taking the image of I under $\mathcal{T}_A \circ \mathcal{T}_B$, we multiply signed volume by $\det(A)\det(B)$. But $\mathcal{T}_A \circ \mathcal{T}_B = \mathcal{T}_{AB}$, so $\mathcal{T}_{AB}$ takes I to Q, and so $\mathcal{T}_{AB}$ multiplies signed volume by $\det(AB)$. Hence, $\det(AB) = \det(A)\det(B)$. $\diamond$

REMARK 3.1.13. The fact that the determinant is the factor by which linear transformations multiply signed volume is the reason for the appearance of the Jacobian in the transformation formula for multiple integrals. $\diamond$

We have carried our argument this far in order to show that we can obtain the existence of the determinant purely from the geometric viewpoint. In the next section we present an algebraic viewpoint, which only uses our work up through Theorem 3.1.4. We use this second viewpoint to derive the results of Section 3.3. But we note that the formula for the determinant we have obtained in Theorem 3.1.4 is a special case of the Laplace expression of Theorem 3.3.6. (The geometric viewpoint is simpler, but the algebraic viewpoint is technically more useful, which is why we present both.)

3.2 EXISTENCE AND UNIQUENESS OF DETERMINANTS

We now present a more traditional approach to the determinant.

Lemma 3.2.1. *Let $V_{n,m} = \{$multilinear functions $f : \mathrm{M}_{n,m}(\mathbb{F}) \to \mathbb{F}\}$. Then $V_{m,n}$ is a vector space of dimension n^m with basis $\{f_\rho\}$, where $\rho : \{1, \ldots, m\} \to \{1, \ldots, n\}$ is any function and, if $A = (a_{ij})$,*

$$f_\rho(A) = a_{\rho(1),1} a_{\rho(2),2} \ldots a_{\rho(m),m}.$$

Proof. We proceed by induction on m. Let $m = 1$. Then, by multilinearity, $f \in V_{n,1}$ is given by

$$\begin{aligned} f\left(\begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{bmatrix}\right) &= f\left(a_{11} \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + a_{21} \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \cdots + a_{n1} \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} \right) \\ &= c_{11} a_{11} + \cdots + c_{n1} a_{n1} \end{aligned}$$

where $c_{11} = f(e_1), \ldots, c_{n1} = f(e_n)$, and the lemma holds.

Now for the inductive step. Assume the lemma holds for m and consider $f \in V_{n,m+1}$. Let $A \in \mathrm{M}_{n,m+1}$ and write A' for the n-by-m submatrix of A consisting of the first m columns of A. Then, by multilinearity,

$$\begin{aligned} f&\left(\left[\begin{array}{c|c} A' & \begin{bmatrix} a_{1m+1} \\ \vdots \\ a_{nm+1} \end{bmatrix} \end{array}\right]\right) \\ &= a_{1m+1} f\big(\big[A' \mid e_1\big]\big) + \cdots + a_{nm+1} f\big(\big[A' \mid e_n\big]\big). \end{aligned}$$

But $g(A') = f([A' \mid e_i])$ is a multilinear function on m-by-n matrices, so by induction $g(A') = \sum c_{\rho'} f_{\rho'}(A')$ where $\rho' : \{1, \ldots, m\} \to \{1, \ldots, n\}$, and so we see that

$$\begin{aligned} f(A) &= \sum_{i=1}^{n} c_{\rho'} f\big(\big[A' \mid e_1\big]\big) a_{\rho'(1),1} \cdots a_{\rho'(m),m} a_{i,m+1} \\ &= \sum_{i=1}^{n} c_\rho a_{\rho(1),1} \cdots a_{\rho(m+1),m+1} \end{aligned}$$

where $\rho : \{1, \ldots, m+1\} \to \{1, \ldots, n\}$ is given by $\rho(k) = \rho'(k)$ for $1 \le k \le m$, and $\rho(m+1) = i$, and the lemma holds. $\square$

We now specialize to the case $m = n$. In this case, Vol, being a multilinear function, is a linear combination of basis elements. We have not used the condition of alternation yet. We do so now, in two stages.

We let P_{ρ_0} be the n-by-n matrix defined by $P_{\rho_0} = (p_{ij})$ where $p_{ij} = 1$ if $i = \rho_0(j)$ and $p_{ij} = 0$ if $i \neq \rho_0(j)$. P_{ρ_0} has exactly one nonzero entry in each column: an entry of 1 in row $\rho_0(j)$ of column j. We then observe that if

$$f(A) = \sum_{\rho} c_{\rho} \cdot a_{\rho(1),1} \cdots a_{\rho(n),n},$$

then $f(P_{\rho_0}) = c_{\rho_0}$. For if $\rho = \rho_0$ then each factor $p_{\rho(j),j}$ is 1, so the product is 1, but if $\rho \neq \rho_0$ then some factor $P_{\rho(j),j}$ is 0, so the product is 0.

Lemma 3.2.2. *Let $f \in V_{n,n}$ be alternating and write*

$$f(A) = \sum_{\rho} c_{\rho} a_{\rho(1),1} \cdots a_{\rho(n),n}$$

where $\rho : \{1, \ldots, n\} \to \{1, \ldots, n\}$. If ρ_0 is not 1*-to-*1*, then $c_{\rho_0} = 0$.*

Proof. Suppose ρ_0 is not 1-to-1. As we have observed, $f(P_{\rho_0}) = c_{\rho_0}$. But in this case P_{ρ_0} is a matrix with two identical columns (columns j_1 and j_2 where $\rho_0(j_1) = \rho_0(j_2)$), so by the definition of alternation, $f(P_{\rho_0}) = 0$. $\square$

We restrict our attention to 1-1 functions $\rho : \{1, \ldots, n\} \to \{1, \ldots, n\}$. We denote the set of such functions by S_n, and elements of this set by σ. S_n forms a group under composition of functions, as any $\sigma \in S_n$ is invertible. S_n is known as the *symmetric group*, and $\sigma \in S_n$ is a *permutation*. (We think of σ as giving a reordering of $\{1, \ldots, n\}$ as $\{\sigma(1), \ldots, \sigma(n)\}$.)

We now cite some algebraic facts without proof. A *transposition* is an element of S_n that interchanges two elements of $\{1, \ldots, n\}$ and leaves all the others fixed. (More formally, $\sigma \in S_n$ is a transposition if for some $1 \leq i \neq j \leq n$, $\sigma(i) = j$, $\sigma(j) = i$, $\sigma(k) = k$ for $k \neq i, j$.) Every element of S_n can be written as a product (i.e., composition) of transpositions. If σ is the product of t transpositions, we define its *sign* by $\text{sign}(\sigma) = (-1)^t$. Though t is not well-defined, $\text{sign}(\sigma)$ is well-defined, i.e., if σ is written as a product of t_1 transpositions and as a product of t_2 transpositions, then $t_1 \equiv t_2 \pmod 2$.

Lemma 3.2.3. *Let $f \in V_{n,n}$ be alternating and write*

$$f(A) = \sum_{\sigma \in S_n} c_\sigma a_{\sigma(1),1} \cdots a_{\sigma(n),n}.$$

Then $f(P_{\sigma_0}) = \operatorname{sign}(\sigma_0) f(I)$.

Proof. The matrix P_{σ_0} is obtained by starting with I and performing t interchanges of pairs of columns, where σ_0 is the product of t transpositions, and the only term in the sum that contributes is when $\sigma = \sigma_0$, so the lemma follows from Lemma 3.1.2(3). $\square$

Theorem 3.2.4. *Any multilinear, alternating function* $\operatorname{Vol} : M_n(\mathbb{F}) \to \mathbb{F}$ *is given by*

$$\operatorname{Vol}(A) = \operatorname{Vol}_a(A) = a\left(\sum_{\sigma \in S_n} \operatorname{sign}(\sigma) a_{\sigma(1),1} \cdots a_{\sigma(n),n}\right)$$

for some $a \in \mathbb{F}$, and every function defined in this way is multilinear and alternating.

Proof. We have essentially already shown the first part. Let $a = f(I)$. Then by Lemma 3.2.3, for every $\sigma \in S_n$, $c_\sigma = a \operatorname{sign}(\sigma)$.

It clearly suffices to verify the second part when $a = 1$. Suppose $A = [v_1 \mid \cdots \mid v_n]$ and $v_i = v_i' + v_i''$. Let

$$v_i = \begin{bmatrix} a_{1i} \\ \vdots \\ a_{ni} \end{bmatrix}, \qquad v_i' = \begin{bmatrix} b_{1i} \\ \vdots \\ b_{ni} \end{bmatrix}, \quad \text{and} \quad v_i'' = \begin{bmatrix} c_{1i} \\ \vdots \\ c_{ni} \end{bmatrix},$$

so $a_{ki} = b_{ki} + c_{ki}$.

Then

$$\begin{aligned}
&\sum_{\sigma \in S_n} \operatorname{sign}(\sigma) a_{\sigma(1),1} \cdots a_{\sigma(i),i} \cdots a_{\sigma(n),n} \\
&\qquad = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) a_{\sigma(1),1} \cdots \left(b_{\sigma(i),i} + c_{\sigma(i),i}\right) \cdots a_{\sigma(n),n} \\
&\qquad = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) a_{\sigma(1),1} \cdots b_{\sigma(i),i} \cdots a_{\sigma(n),n} \\
&\qquad\quad + \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) a_{\sigma(1),1} \cdots c_{\sigma(i),i} \cdots a_{\sigma(n),n},
\end{aligned}$$

showing multilinearity. Suppose columns i and j of A are equal, and let $\tau \in S_n$ be the transposition that interchanges i and j. To every $\sigma \in S_n$ we can associate $\sigma' = \tau\sigma \in S_n$, and σ is associated to σ' as τ^2 is the identity, and hence $\sigma = \tau^2\sigma = \tau\sigma'$. Write this association as $\sigma' \sim \sigma$. Then

$$\begin{aligned}\sum_{\sigma \in S_n} & \operatorname{sign}(\sigma) a_{\sigma(1),1} \cdots a_{\sigma(i),i} \cdots a_{\sigma(j),j} \cdots a_{\sigma(n),n} \\ &= \sum_{\sigma \sim \sigma'} \big(\operatorname{sign}(\sigma) a_{\sigma(1),1} \cdots a_{\sigma(i),i} \cdots a_{\sigma(j),j} \cdots a_{\sigma(n),n} \\ &\qquad\qquad + \operatorname{sign}(\sigma') a_{\sigma'(1),1} \cdots a_{\sigma'(i),i} \cdots a_{\sigma'(j),j} \cdots a_{\sigma'(n),n} \big).\end{aligned}$$

But $\operatorname{sign}(\sigma) = -\operatorname{sign}(\sigma')$ and the two products of elements are equal because columns i and j of A are identical, so the terms cancel in pairs and the sum is 0, showing alternation. □

DEFINITION 3.2.5. The function $\det : M_n(\mathbb{F}) \to \mathbb{F}$, given by

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) a_{\sigma(1),1} \cdots a_{\sigma(n),n}$$

is the *determinant* function. ◇

3.3 FURTHER PROPERTIES

We now derive some important properties of the determinant.

Theorem 3.3.1. *Let $A, B \in M_n(\mathbb{F})$. Then*

$$\det(AB) = \det(A)\det(B).$$

Proof. Define a function $f : M_n(\mathbb{F}) \to \mathbb{F}$ by $f(B) = \det(AB)$. It is straightforward to check that f is multilinear and alternating, so f is a volume function $f(B) = \mathrm{Vol}_a(B) = a\det(B)$ where $a = f(I) = \det(AI) = \det(A)$. □

Corollary 3.3.2. *(1)* $\det(A) \neq 0$ *if and only if A is invertible.*

(2) If A is invertible, then $\det(A^{-1}) = 1/\det(A)$. *Furthermore, for any matrix B,* $\det(ABA^{-1}) = \det(B)$.

Proof. We have already seen in Lemma 3.1.2 that for any volume function f, $f(A) = 0$ if A is not invertible. If A is invertible we have $1 = \det(I) = \det(AA^{-1}) = \det(A)\det(A^{-1})$ from which the corollary follows. □

Lemma 3.3.3. *(1) Let A be a diagonal matrix. Then* $\det(A)$ *is the product of its diagonal entries.*

(2) More generally, let A be an upper triangular, or a lower triangular, matrix. Then $\det(A)$ *is the product of its diagonal entries.*

Proof. (1) If A is diagonal, then there is only one nonzero term in Definition 3.2.5, the term corresponding to the identity permutation ($\sigma(i) = i$ for every i), which has sign $+1$.

(2) If σ is not the identity then there is a j with $\sigma(j) < j$, and a k with $\sigma(k) > k$, so for a triangular matrix there is again only the diagonal term. □

Theorem 3.3.4. *(1) Let M be a block diagonal matrix,*

$$M = \begin{bmatrix} A & 0 \\ 0 & D \end{bmatrix}.$$

Then $\det(M) = \det(A)\det(D)$.

(2) More generally, let M be a block upper triangular or a block lower triangular matrix,

$$M = \begin{bmatrix} A & B \\ 0 & D \end{bmatrix} \quad \text{or} \quad M = \begin{bmatrix} A & 0 \\ C & D \end{bmatrix}.$$

Then $\det(M) = \det(A)\det(D)$.

Proof. (1) Define a function $f : M_n(\mathbb{F}) \to \mathbb{F}$ by

$$f(D) = \det\left(\begin{bmatrix} A & 0 \\ 0 & D \end{bmatrix}\right).$$

Then f is multilinear and alternating, so $f(D) = f(I)\det(D)$. But $f(I) = \det\left(\left[\begin{smallmatrix} A & 0 \\ 0 & I \end{smallmatrix}\right]\right) = \det(A)$. (This last equality is easy to see as any permutation that contributes nonzero to $\det\left(\left[\begin{smallmatrix} A & 0 \\ 0 & I \end{smallmatrix}\right]\right)$ must fix all but (possibly) the first n entries.)

(2) Suppose M is upper triangular (the lower triangular case is similar). If A is singular then there is a vector $v \neq 0$ with $Av = 0$. Then let w be the vector whose first n entries are that of v and whose remaining entries are 0. Then $Mw = 0$. Thus M is singular as well, and $0 = 0 \cdot \det(D)$.

Suppose that A is nonsingular. Then

$$\begin{bmatrix} A & B \\ 0 & D \end{bmatrix} = \begin{bmatrix} A & 0 \\ 0 & D \end{bmatrix} \begin{bmatrix} I & A^{-1}B \\ 0 & I \end{bmatrix}.$$

The first matrix on the right-hand side has determinant $\det(A)\det(D)$, and the second matrix on the right-hand side has determinant 1, as it is upper triangular, and the theorem follows. □

Lemma 3.3.5. *Let ${}^tA$ be the matrix obtained from A by interchanging the rows and columns of A. Then* $\det({}^tA) = \det(A)$.

Proof. For any $\sigma \in S_n$, $\operatorname{sign}(\sigma^{-1}) = \operatorname{sign}(\sigma)$. Let $B = (b_{ij}) = {}^tA$. Then

$$\begin{aligned}
\det(A) &= \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) a_{\sigma(1),1} \cdots a_{\sigma(n),n} \\
&= \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) a_{1,\sigma^{-1}(1)} \cdots a_{n,\sigma^{-1}(n)} \\
&= \sum_{\sigma \in S_n} \operatorname{sign}(\sigma^{-1}) a_{1,\sigma^{-1}(1)} \cdots a_{n,\sigma^{-1}(n)} \\
&= \sum_{\sigma^{-1} \in S_n} \operatorname{sign}(\sigma^{-1}) b_{\sigma^{-1}(1),1} \cdots b_{\sigma^{-1}(n),n} \\
&= \det({}^tA).
\end{aligned}$$

□

Let A_{ij} denote the (i,j)-minor of the matrix A, the submatrix obtained by deleting row i and column j of A.

Theorem 3.3.6 (Laplace expansion)**.** *Let A be an n-by-n matrix, $A = (a_{ij})$.*

(1) For any i,

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det\left(A_{ij}\right).$$

(2) For any j,

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det\left(A_{ij}\right).$$

(3) For any i, and for any $k \neq i$,

$$0 = \sum_{j=1}^{n} (-1)^{i+j} a_{kj} \det\left(A_{ij}\right).$$

(4) For any j, and for any $k \neq j$,

$$0 = \sum_{i=1}^{n} (-1)^{i+j} a_{ik} \det\left(A_{ij}\right).$$

Proof. We prove (1) and (3) simultaneously, so we fix k (which may or may not equal i).

The sum on the right-hand side is the sum of multilinear functions so is itself multilinear. (This is also easy to see directly.)

We now show it is alternating. Let A be a matrix with columns p and q equal, where $1 \le p < q \le n$. If $j \ne p, q$ then A_{ij} is a matrix with two columns equal, so $\det(A_{ij}) = 0$. Thus the only two terms that contribute to the sum are

$$(-1)^{i+p} a_{kp} \det\left(A_{ip}\right) + (-1)^{i+q} a_{kq} \det\left(A_{iq}\right).$$

By hypothesis, $a_{kq} = a_{kp}$. Now

$$\begin{aligned} A_{ip} &= \left[v_1 \mid \cdots \mid v_{p-1} \mid v_{p+1} \mid \cdots \mid v_{q-1} \mid v_q \mid v_{q+1} \mid \cdots \mid v_n\right], \\ A_{iq} &= \left[v_1 \mid \cdots \mid v_{p-1} \mid v_p \mid v_{p+1} \mid \cdots \mid v_{q-1} \mid v_{q+1} \mid \cdots \mid v_n\right]. \end{aligned}$$

where v_m denotes column m of the matrix obtained from A by deleting row i of A. By hypothesis, $v_p = v_q$, so these two matrices have the same columns but in a different order. We get from the first of these to the second by successively performing $q - p - 1$ column interchanges (first switching v_q and v_{q-1}, then switching v_q and $v_{q-2}, \ldots$, and finally switching v_q and v_{p+1}), so $\det(A_{iq}) = (-1)^{q-p-1} \det(A_{ip})$. Thus we see that the contribution of these two terms to the sum is

$$(-1)^{i+p} a_{kp} \det\left(A_{ip}\right) + (-1)^{i+q} a_{kp} (-1)^{q-p-1} \det\left(A_{ip}\right)$$

and since $(-1)^{i+p}$ and $(-1)^{i+2q-p-1}$ always have opposite signs, they cancel.

By our uniqueness result, the right-hand side is a multiple $a \det(A)$ for some a. A computation shows that if $A = I$, the right-hand side gives 1 if $k = i$ and 0 if $k \ne i$, proving the theorem in these cases.

For cases (2) and (4), using the fact that $\det(B) = \det({}^t B)$ for any matrix B, we can take the transpose of these formulas and use cases (1) and (3). □

REMARK 3.3.7. Theorem 3.3.6(1) (respectively, (3)) is known as *expansion by minors* of the jth column (respectively, of the ith row). ◇

DEFINITION 3.3.8. The *classical adjoint* of A is the matrix $\operatorname{Adj}(A)$ defined by $\operatorname{Adj}(A) = (b_{ij})$ where $b_{ij} = (-1)^{i+j} \det(A_{ji})$. ◇

Note carefully the subscript in the definition—it is A_{ji}, as written, not A_{ij}.

Corollary 3.3.9. *(1) For any matrix A,*

$$\big(\operatorname{Adj}(A)\big) = A\big(\operatorname{Adj}(A)\big) = \det(A)I.$$

(2) If A is invertible,

$$A^{-1} = \frac{1}{\det(A)}\operatorname{Adj}(A).$$

Proof. (1) can be verified by a computation that follows directly from Theorem 3.3.6. Then (2) follows immediately. □

REMARK 3.3.10. We have given the formula in Corollary 3.3.9(2) for its theoretical interest (and we shall see some applications of it later) but as a practical matter it should almost never be used to find the inverse of a matrix. ◇

Corollary 3.3.11 (Cramer's rule)**.** *Let A be an invertible n-by-n matrix and let b be a vector in $\mathbb{F}^n$. Let x be the unique vector in $\mathbb{F}^n$ with $Ax = b$. Write $x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$. Then, for $1 \leq i \leq n$, $x_i = \det(A_i(b))/\det(A)$, where $A_i(b)$ is the matrix obtained from A by replacing its ith column by b.*

Proof. Let the columns of A be $a_1, \ldots, a_n$. By linearity, it suffices to prove the corollary for all elements of any basis $\mathcal{B}$ of $\mathbb{F}^n$. We choose the basis $\mathcal{B} = \{a_1, \ldots, a_n\}$.

Fix i and consider $Ax = a_i$. Then $A_i(a_i) = A$, so the above formula gives $x_i = 1$. For $j \neq i$, $A_i(a_j)$ is a matrix with two identical columns, so the above formula gives $x_j = 0$. Thus $x = e_i$, the ith standard basis vector, and indeed $Ae_i = a_i$. □

REMARK 3.3.12. Again this formula is of theoretical interest but should almost never be used in practice. ◇

Here is a familiar result from elementary linear algebra.

DEFINITION 3.3.13. If the matrix A has a a k-by-k submatrix with nonzero determinant, but does not have a $(k+1)$-by-$(k+1)$ submatrix with nonzero determinant, then the *determinantal rank* of A is k. ◇

Theorem 3.3.14. *Let A be a matrix. Then the row rank, column rank, and determinantal rank of A are all equal.*

Proof. We showed that the row rank and column rank of A are equal in Theorem 2.4.7. We now show that the column rank of A is equal to the determinantal rank of A.

Write $A = [v_1 \mid \cdots \mid v_n]$, where A is m-by-n. Let A have a k-by-k submatrix B with nonzero determinant. For simplicity, we assume that B is the upper left-hand corner of A. Suppose B is k-by-k. Let $\pi : \mathbb{F}^m \to \mathbb{F}^k$ be defined by

$$\pi\left(\begin{bmatrix} a_1 \\ \vdots \\ a_m \end{bmatrix}\right) = \begin{bmatrix} a_1 \\ \vdots \\ a_k \end{bmatrix}.$$

Then $B = [\pi(v_1) \mid \cdots \mid \pi(v_k)]$. Since $\det(B) \neq 0$, B is nonsingular, so $\{\pi(v_1), \ldots, \pi(v_k)\}$ is linearly independent, and hence $\{v_1, \ldots, v_k\}$ is linearly independent. But then this set spans a k-dimensional subspace of the column space of A, so A has column rank at least k.

On the other hand, suppose A has k linearly independent columns. Again, for simplicity, suppose these are the leftmost k columns of A. Now $\{v_1, \ldots, v_k\}$ is linearly independent and $\{e_1, \ldots, e_m\}$ spans $\mathbb{F}^m$, so $\{v_1, \ldots, v_k, e_1, \ldots, e_m\}$ spans $\mathbb{F}^m$ as well. Then, by Theorem 1.2.9, there is a basis $\mathcal{B}$ of $\mathbb{F}^m$ with $\{v_1, \ldots, v_k\} \subseteq \mathcal{B} \subseteq \{v_1, \ldots, v_k, e_1, \ldots, e_m\}$. Write $\mathcal{B} = \{v_1, \ldots, v_k, v_{k+1}, \ldots, v_m\}$ and note that, for each $i \geq k+1$, $v_i = e_j$ for some j. Form the matrix $B' = [v_1 \mid \cdots \mid v_k \mid v_{k+1} \mid \cdots \mid v_n]$ and note that $\det(B') \neq 0$. Expand by minors of columns $n, n-1, \ldots, k+1$ to obtain $0 \neq \det(B') = \pm \det(B)$ where B is a k-by-k submatrix of A, so A has determinantal rank at least k. □

We have defined the determinant for matrices. We can define the determinant for linear transformations $\mathcal{T} : V \to V$, where V is a finite-dimensional vector space.

DEFINITION 3.3.15. Let $\mathcal{T} : V \to V$ be a linear transformation with V a finite-dimensional vector space. The *determinant* $\det(\mathcal{T})$ is defined to be $\det(\mathcal{T}) = \det\left([(\mathcal{T})_{\mathcal{B}}]\right)$ where $\mathcal{B}$ is any basis of V. ◇

To see that this is well-defined we have to know that it is independent of the choice of the basis $\mathcal{B}$. That follows immediately from Corollary 2.3.11 and Corollary 3.3.2(2).

We have defined the general linear groups $\mathrm{GL}_n(\mathbb{F})$ and $\mathrm{GL}(V)$ in Definition 1.1.29.

Lemma 3.3.16. $\mathrm{GL}_n(\mathbb{F}) = \{A \in M_n(\mathbb{F}) \mid \det(A) \neq 0\}$. *For V finite dimensional,*

$$\mathrm{GL}(V) = \{\mathcal{T} : V \to V \mid \det(\mathcal{T}) \neq 0\}.$$

Proof. Immediate from Corollary 3.3.2. □

We can now make a related definition.

DEFINITION 3.3.17. The *special linear group* $\mathrm{SL}_n(\mathbb{F})$ is the group

$$\mathrm{SL}_n(\mathbb{F}) = \{A \in \mathrm{GL}_n(\mathbb{F}) \mid \det(A) = 1\}.$$

For V finite dimensional,

$$\mathrm{SL}_n(V) = \{\mathcal{T} \in \mathrm{GL}(V) \mid \det(\mathcal{T}) = 1\}. \qquad \diamond$$

Theorem 3.3.18. *(1)* $\mathrm{SL}_n(\mathbb{F})$ *is a normal subgroup of* $\mathrm{GL}_n(\mathbb{F})$.

(2) For V finite dimensional, $\mathrm{SL}(V)$ *is a normal subgroup of* $\mathrm{GL}(V)$.

Proof. $\mathrm{SL}_n(\mathbb{F})$ is the kernel of the homomorphism $\det : \mathrm{GL}_n(\mathbb{F}) \to \mathbb{F}^*$, and similarly for $\mathrm{SL}(V)$. (By Theorem 3.3.1, det is a homomorphism.) Here $\mathbb{F}^*$ denotes the multiplicative group of nonzero elements of $\mathbb{F}$. □

3.4 INTEGRALITY

While we almost exclusively work over a field, it is natural to ask the question of integrality, and we consider that here.

Let R be an integral domain with quotient field $\mathbb{F}$. An element u of R is a unit if there is an element v of R with $uv = vu = 1$. (The reader unfamiliar with quotient fields can simply take $R = \mathbb{Z}$ and $\mathbb{F} = \mathbb{Q}$, and note that the units of $\mathbb{Z}$ are ± 1.)

Theorem 3.4.1. *Let A be an n-by-n matrix with entries in R and suppose that it is invertible, considered as a matrix with entries in $\mathbb{F}$. The following are equivalent:*

(1) A^{-1} *has entries in R.*

(2) $\det(A)$ *is a unit in R.*

(3) For every vector b all of whose entries are in R, the unique solution of $Ax = b$ is a vector all of whose entries are in R.

Proof. First we show that (1) and (3) are equivalent and then we show that (1) and (2) are equivalent.

Suppose (1) is true. Then the solution of $Ax = b$ is $x = A^{-1}b$, whose entries are in R. Conversely, suppose (3) is true. Let $Ax_i = e_i$, $i = 1, \dots, n$, where $\{e_i\}$ is the set of standard unit vectors in $\mathbb{F}^n$. Form the matrix $B = [x_1 \mid x_2 \mid \cdots \mid x_n]$. Then B is a matrix all of whose entries are in R, and $AB = I$, so $B = A^{-1}$ by Corollary 1.3.3.

Suppose (1) is true. Let $\det(A) = u$ and $\det(A^{-1}) = v$. Then u and v are elements of R and $uv = \det(A)\det(A^{-1}) = \det(I) = 1$, so u is a unit in R. Conversely, suppose (2) is true, so $\det(A) = u$ is a unit in R. Let $uv = 1$ with $v \in R$, so $v = 1/u$. Then Corollary 3.3.9(2) shows that all of the entries of A^{-1} are in R. $\square$

REMARK 3.4.2. Let A be an n-by-n matrix with entries in R and suppose that A is invertible, considered as a matrix with entries in $\mathbb{F}$. Let $d = \det(A)$.

(1) If b is a vector in R^n all of whose entries are divisible by d, then $x = A^{-1}b$, the unique solution of $Ax = b$, has all its entries in R.

(2) This condition on the entries of b is sufficient but not necessary. It is possible to have a vector b whose entries are not all divisible by d with the solution of $Ax = b$ having all its entries in R. For example, let $R = \mathbb{Z}$ and take $A = \left[\begin{smallmatrix} 1 & 1 \\ 1 & 3 \end{smallmatrix}\right]$, a matrix of determinant 2. Then $Ax = \left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right]$ has solution $x = \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$. (By Theorem 3.4.1, if d is not a unit, this is not possible for all b.) $\diamond$

We can now generalize the definitions of $\mathrm{GL}_n(\mathbb{F})$ and $\mathrm{SL}_n(\mathbb{F})$.

DEFINITION 3.4.3. The *general linear group* $\mathrm{GL}_n(R)$ is defined by

$$\mathrm{GL}_n(R) = \big\{A \in M_n(R) \mid A \text{ has an inverse in } M_n(R)\big\}. \qquad \diamond$$

Corollary 3.4.4.

$$\mathrm{GL}_n(R) = \big\{A \in M_n(R) \mid \det(A) \textit{ is a unit in } R\big\}.$$

DEFINITION 3.4.5. The *special linear group* $\mathrm{SL}_n(R)$ is defined by

$$\mathrm{SL}_n(R) = \big\{A \in \mathrm{GL}_n(R) \mid \det(A) = 1\big\}. \qquad \diamond$$

Lemma 3.4.6. $\mathrm{SL}_n(R)$ *is a normal subgroup of* $\mathrm{GL}_n(R)$.

Proof. $\mathrm{SL}_n(R)$ is the kernel of the determinant homomorphism. $\square$

REMARK 3.4.7. If $R = \mathbb{Z}$, the units in R are $\{\pm 1\}$. Thus $\mathrm{SL}_n(\mathbb{Z})$ is a subgroup of index 2 of $\mathrm{GL}_n(\mathbb{Z})$. $\diamond$

It follows from our previous work that for any nonzero vector $v \in \mathbb{F}^n$ there is an invertible matrix A with $Ae_1 = v$ (where e_1 is the first vector in the standard basis of $\mathbb{F}^n$). One can ask the same question over the integers: Given a nonzero vector $v \in \mathbb{Z}^n$, is there a matrix A with integer entries, invertible as an integer matrix, with $Ae_1 = v$? There is an obvious necessary condition, that the entries of v be relatively prime. This condition turns out to be sufficient. We prove a slightly more precise result.

Theorem 3.4.8. *Let $n \geq 2$ and let $v = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$ be a nonzero vector with integral entries. Let $d = \gcd(a_1, \ldots, a_n)$. Then there is a matrix $A \in \mathrm{SL}_n(\mathbb{Z})$ with $A(de_1) = v$.*

Proof. We proceed by induction on n. We begin with $n = 2$. If $d = \gcd(a_1, a_2)$, let $a_1' = a_1/d$ and $b_1' = b_1/d$. Then there are integers p and q with $a_1'p + a_2'q = 1$. Set

$$A = \begin{bmatrix} a_1' & -q \\ a_2' & p \end{bmatrix}.$$

Suppose the theorem is true for $n-1$, and consider $v \in \mathbb{Z}^n$. It is easy to see that the theorem is true if $a_1 = \cdots = a_{n-1} = 0$, so suppose not. Let $d_0 = \gcd(a_1, \ldots, a_{n-1})$. Then $d = \gcd(d_0, a_n)$. By the proof of the $n = 2$ case, there is an n-by-n matrix A_1 with

$$A_1(de_1) = \begin{bmatrix} d_0 \\ 0 \\ \vdots \\ 0 \\ a_n \end{bmatrix}.$$

(A_1 has suitable entries in its "corners" and an $(n-2)$-by-$(n-2)$ identity matrix in its "middle".) By the inductive assumption, there is an n-by-n matrix A_2 with

$$A_2\left(\begin{bmatrix} d_0 \\ 0 \\ \vdots \\ 0 \\ a_n \end{bmatrix}\right) = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}.$$

(A_2 is a block diagonal matrix with a suitable $(n-1)$-by-$(n-1)$ matrix in its upper left-hand corner and an entry of 1 in its lower right-hand corner.)

Set $A = A_2 A_1$. □

Corollary 3.4.9. *Let $n \geq 2$ and let $v = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$ be a nonzero vector with integer entries, and suppose that $\{a_1, \ldots, a_n\}$ is relatively prime. Then there is a matrix $A \in \mathrm{SL}_n(\mathbb{Z})$ whose first column is v.*

Proof. A is the matrix constructed in the proof of Theorem 3.4.8. □

Let $\mathbb{Z}/N\mathbb{Z}$ denote the ring of integers mod N. We have the map $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ by $a \mapsto a \pmod{N}$. This induces a map on matrices as well.

Theorem 3.4.10. *For every $n \geq 1$, the map $\varphi : \mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z})$ given by the reduction of entries* $\pmod{N}$ *is an epimorphism.*

Proof. We prove the theorem by induction on n. For $n = 1$ it is obvious.

Suppose $n > 1$. Let $\overline{M} \in \mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z})$ be arbitrary. Then there is certainly a matrix M with integer entries with $\varphi(M) = \overline{M}$, and then $\det(M) \equiv 1 \pmod{N}$. But this is not good enough. We need $\det(M) = 1$.

Let $v_1 = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$ be the first column of M. Then $\overline{M} \in \mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z})$ implies $\gcd(a_1, \ldots, a_n, N) = 1$.

Let $d = \gcd(a_1, \ldots, a_n)$. Then d and N are relatively prime. By Theorem 3.4.8, there is a matrix $A \in \mathrm{SL}_n(\mathbb{Z})$ with AM a matrix of the form

$$AM = \left[\begin{array}{c|c|c|c} d & & & \\ 0 & & & \\ \vdots & w_2 & \cdots & w_n \\ 0 & & & \end{array}\right].$$

If $d = 1$ we may set $M_1 = M$, $B = I$, and $P = AM = BAM_1$. Otherwise, let L be the matrix with an entry of N in the $(2,1)$ position and all other entries 0. Let $M_1 = M + A^{-1}L$. Then

$$AM_1 = \left[\begin{array}{c|c|c|c} d & & & \\ N & & & \\ 0 & w_2 & \cdots & w_n \\ \vdots & & & \\ 0 & & & \end{array}\right]$$

and $M_1 \equiv M \pmod{N}$.

As in the proof of Theorem 3.4.8, we choose integers p and q with $dp + Nq = 1$. Let E be the 2-by-2 matrix

$$E = \begin{bmatrix} p & q \\ -N & d \end{bmatrix}$$

and let B be the n-by-n block matrix

$$B = \begin{bmatrix} E & 0 \\ 0 & I \end{bmatrix}.$$

Then $P = BAM_1$ is of the form

$$P = \left[\begin{array}{c|c|c|c} 1 & & & \\ 0 & & & \\ \vdots & u_2 & \cdots & u_n \\ 0 & & & \end{array}\right].$$

Write P as a block matrix

$$P = \begin{bmatrix} 1 & X \\ 0 & U \end{bmatrix}.$$

Then $\det(P) \equiv \det(M) \equiv 1 \pmod{N}$, so $\det(U) \equiv 1 \pmod{N}$. U is an $(n-1)$-by-$(n-1)$ matrix, so by the inductive hypothesis there is a matrix $V \in \mathrm{SL}_{n-1}(\mathbb{Z})$ with $V \equiv U \pmod{N}$. Set

$$Q = \begin{bmatrix} 1 & X \\ 0 & V \end{bmatrix}.$$

Then $Q \in \mathrm{SL}_n(\mathbb{Z})$ and

$$Q \equiv P = BAM_1 \equiv BAM \pmod{N}.$$

Thus

$$R = (BA)^{-1}Q \in \mathrm{SL}_n(\mathbb{Z}) \quad \text{and} \quad R \equiv M \pmod{N},$$

i.e., $\varphi(R) = \varphi(M) = \overline{M}$, as required. □

3.5 Orientation

We now study orientations of real vector spaces, where we will see the geometric meaning of the sign of the determinant. Before we consider orientation per se it is illuminating to study the topology of the general linear group $\mathrm{GL}_n(\mathbb{R})$, the group of invertible n-by-n matrices with real entries.

Theorem 3.5.1. *The general linear group* $\mathrm{GL}_n(\mathbb{R})$ *has two components.*

Proof. We have the determinant function $\det : M_n(\mathbb{R}) \to \mathbb{R}$. Since a matrix is invertible if and only if its determinant is nonzero,

$$\mathrm{GL}_n(\mathbb{R}) = \det^{-1}(\mathbb{R} - \{0\}).$$

Now $\mathbb{R} - \{0\}$ has two components, so $\mathrm{GL}_n(\mathbb{R})$ has at least two components, {matrices with positive determinant} and {matrices with negative determinant}. We will show that each of these two sets is path-connected. (Since $\mathrm{GL}_n(\mathbb{R})$ is an open subset of Euclidean space, components and path components are the same.)

We know that every nonsingular matrix can be transformed to the identity matrix by left-multiplication by a sequence of elementary matrices, that have the effect of performing a sequence of elementary row operations. (We could equally well right-multiply and perform column operations with no change in the proof.) We will consider a variant on elementary row operations, namely operations of the following type:

(1) Left multiplication by a matrix

$$\widetilde{E} = \begin{bmatrix} 1 & & & \\ & 1 & a & \\ & & \ddots & \\ & & & 1 \end{bmatrix}$$

with a in the (i, j) position, which has the effect of adding a times row j to row i. (This is a usual row operation.)

(2) Left multiplication by a matrix

$$\widetilde{E} = \begin{bmatrix} 1 & & & & & \\ & 1 & & & & \\ & & \ddots & & & \\ & & & c & & \\ & & & & \ddots & \\ & & & & & 1 \end{bmatrix}$$

with $c > 0$ in the (i, i) position, which has the effect of multiplying row i by c. (This is a usual row operation, but here we restrict c to be positive.)

(3) Left multiplication by a matrix

$$\widetilde{E} = \begin{bmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 0 & & & -1 & & & \\ & & & 1 & & & & & \\ & & & & \ddots & & & & \\ & & & & & 1 & & & \\ & & 1 & & & & 0 & & \\ & & & & & & & 1 & \\ & & & & & & & & \ddots & \\ & & & & & & & & & 1 \end{bmatrix}$$

with 1 in the (i, j) position and -1 in the (j, i) position, which has the effect of replacing row i by row j and row j by the negative of row i. (This differs by a sign from a usual row operation, which replaces each of these two rows by the other.)

There is a path in $\mathrm{GL}_n(\mathbb{R})$ connecting the identity to each of these elements $\widetilde{E}$.

In case (1), we have the path given by

$$\widetilde{E}(t) = \begin{bmatrix} 1 & & \\ & \ddots & ta \\ & & 1 \end{bmatrix}$$

for $0 \leq t \leq 1$.

In case (2), we have the path given by

$$\widetilde{E}(t) = \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & \exp\big(t\ln(c)\big) & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{bmatrix}$$

for $0 \leq t \leq 1$.

In case (3), we have the path given by

$$\widetilde{E}(t) = \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & \cos\left(t\pi/2\right) & & -\sin\left(t\pi/2\right) & & \\ & & & \ddots & & & \\ & & \sin\left(t\pi/2\right) & & \cos\left(t\pi/2\right) & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix}$$

for $0 \le t \le 1$.

Now let A be an invertible matrix and suppose we have a sequence of elementary row operations that reduces A to the identity, so that $E_k \cdots E_2 E_1 A = I$. Replacing each E_i by the corresponding matrix $\widetilde{E}_i$ we see that $\widetilde{E}_k \cdots \widetilde{E}_1 A = \widetilde{I}$ is a matrix differing by I in at most the sign of its entries, i.e., $\widetilde{I}$ is a diagonal matrix with each diagonal entry equal to ± 1. As t goes from 0 to 1, the product $\widetilde{E}_1(t)A$ gives a path from A to $\widetilde{E}_1 A$; as t goes from 0 to 1, $\widetilde{E}_2(t)\widetilde{E}_1 A$ gives a path from $\widetilde{E}_1 A$ to $\widetilde{E}_2\widetilde{E}_1 A$, and so forth. In the end we have path from A to $\widetilde{I}$, so A and $\widetilde{I}$ are in the same path component of $\mathrm{GL}_n(\mathbb{R})$. Note that A and $\widetilde{I}$ have determinants with the same sign. Thus there are two possibilities:

(1) A has a positive determinant. In this case $\widetilde{I}$ has an even number of -1 entries on the diagonal, which can be paired. Suppose there is a pair of -1 entries in positions (i,i) and (j,j). If $\widetilde{E}$ is the appropriate matrix of type (3), $\widetilde{E}^2\widetilde{I}$ will be a matrix of the same form as $\widetilde{I}$, but with both of these entries equal to $+1$ and the others unchanged. As above, we have a path from $\widetilde{I}$ to $\widetilde{E}^2\widetilde{I}$. Continue in this fashion to obtain a path from $\widetilde{I}$ to I, and hence a path from A to I. Thus A is in the same path component as I.

(2) A has a negative determinant. In this case $\widetilde{I}$ has an odd number of -1 entries. Proceeding as in (1), we pair up all but one of the -1 entries to obtain a path from $\widetilde{I}$ to a diagonal matrix with a single -1 entry on the diagonal and all other diagonal entries equal to 1. If the -1 entry is in the $(1,1)$ position there is nothing more to do. If it is in the (i,i) position for $i \neq 1$ (and hence the entry in the $(1,1)$ position is 1) we apply an appropriate matrix $\widetilde{E}$ of type (3) to obtain the diagonal matrix with -1 as the first entry on the diagonal and all other entries equal to 1, and hence a path from A to this matrix, which we shall denote by I_-. Thus in this case A is in the same path component as I_-. □

We now come to the notion of an orientation of a real vector space. We assume V is finite dimensional and $\dim(V) > 0$.

DEFINITION 3.5.2. Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ and $\mathcal{C} = \{w_1, \ldots, w_n\}$ be two bases of the n-dimensional real vector space V. Then $\mathcal{B}$ and $\mathcal{C}$ give the *same orientation* of V if the change of basis matrix $P_{\mathcal{C} \leftarrow \mathcal{B}}$ has positive determinant, while they give *opposite orientations* of V if the change of basis matrix $P_{\mathcal{C} \leftarrow \mathcal{B}}$ has negative determinant. $\diamond$

REMARK 3.5.3. It is easy to check that "giving the same orientation" is an equivalence relation on bases. It then follows that we can regard an orientation on a real vector space (of positive finite dimension) as an equivalence class of bases of V, and there are two such equivalence classes. $\diamond$

In general, there is no preferred orientation on a real vector space, but in one very important special case there is.

DEFINITION 3.5.4. Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a basis of $\mathbb{R}^n$. Then $\mathcal{B}$ gives the *standard orientation* of $\mathbb{R}^n$ if $\mathcal{B}$ gives the same orientation as the standard basis $\mathcal{E}$ of $\mathbb{R}^n$. Otherwise $\mathcal{B}$ gives the *nonstandard orientation* of $\mathbb{R}^n$. $\diamond$

REMARK 3.5.5. (1) $\mathcal{E}$ itself gives the standard orientation of $\mathbb{R}^n$ as $P_{\mathcal{E} \leftarrow \mathcal{E}} = I$ has determinant 1.

(2) The condition in Definition 3.5.4 can be phrased more simply. By Remark 2.3.6(1), $P_{\mathcal{E} \leftarrow \mathcal{B}}$ is the matrix $P_{\mathcal{E} \leftarrow \mathcal{B}} = [v_1 \mid v_2 \mid \cdots \mid v_n]$. So B gives the standard orientation of $\mathbb{R}^n$ if $\det(P_{\mathcal{E} \leftarrow \mathcal{B}}) > 0$ and the nonstandard orientation of $\mathbb{R}^n$ if $\det(P_{\mathcal{E} \leftarrow \mathcal{B}}) < 0$.

(3) In Definition 3.5.4, recalling that $P_{\mathcal{C} \leftarrow \mathcal{B}} = (P_{\mathcal{E} \leftarrow \mathcal{C}})^{-1} P_{\mathcal{E} \leftarrow \mathcal{B}}$, we see that $\mathcal{B}$ and $\mathcal{C}$ give the same orientation of $\mathbb{R}^n$ if the determinants of the matrices $[v_1 \mid v_2 \mid \cdots \mid v_n]$ and $[w_1 \mid w_2 \mid \cdots \mid w_n]$ have the same sign and opposite orientations if they have opposite signs. $\diamond$

Much of the significance of the orientation of a real vector space comes from topological considerations. We continue to let V be a real vector space of finite dimension $n > 0$, and we choose a basis $\mathcal{B}_0$ of V. For any basis $\mathcal{C}$ of V we have a map $f_0 : \{\text{bases of } V\} \to \mathrm{GL}_n(\mathbb{R})$ given by $f_0(\mathcal{C}) = P_{\mathcal{B}_0 \leftarrow \mathcal{C}}$. (If $\mathcal{C} = \{w_1, \ldots, w_n\}$ then $f_0(\mathcal{C})$ is the matrix $[[w_1]_{B_0} \mid \cdots \mid [w_n]_{B_0}]$.) This map is 1-1 and onto. We then give $\{\text{bases of } V\}$ a topology by requiring that f_0 be a homeomorphism. That is, we define a subset $\mathcal{O}$ of $\{\text{bases of } V\}$ to be open if and only if $f_0(\mathcal{O})$ is an open subset of $\mathrm{GL}_n(\mathbb{R})$. A priori, this topology depends on the choice of $\mathcal{B}_0$, but in fact it does not. For if we choose a different basis $\mathcal{B}_1$ and let $f_1(C) = P_{\mathcal{B}_1 \leftarrow \mathcal{C}}$, then

$f_1(C) = P f_0(\mathcal{C})$ where P is the constant matrix $P = P_{\mathcal{B}_1 \leftarrow \mathcal{B}_0}$, and multiplication by the constant matrix P is a homeomorphism from $\mathrm{GL}_n(\mathbb{R})$ to itself.

We then have:

Corollary 3.5.6. *Let V be an n-dimensional real vector space and let $\mathcal{B}$ and $\mathcal{C}$ be two bases of V. Then $\mathcal{B}$ and $\mathcal{C}$ give the same orientation of V if and only if $\mathcal{B}$ can continuously be deformed to $\mathcal{C}$, i.e., if and only if there is a continuous function $p : [0,1] \to \{\text{bases of } V\}$ with $p(0) = \mathcal{B}$ and $p(1) = \mathcal{C}$.*

Proof. The bases $\mathcal{B}$ and $\mathcal{C}$ of V give the same orientation of V if and only if $P_{\mathcal{C} \leftarrow \mathcal{B}}$ has positive determinant, and by Theorem 3.5.1 this is true if and only if there is a path in $\mathrm{GL}_n(\mathbb{R})$ joining I to $P_{\mathcal{C} \leftarrow \mathcal{B}}$.

To be more explicit, let $p : [0,1] \to \mathrm{GL}_n(\mathbb{R})$ with $p(0) = I$ and $p(1) = P_{\mathcal{C} \leftarrow \mathcal{B}}$. For any t between 0 and 1, let $\mathcal{B}_t$ be the basis defined by $P_{\mathcal{B}_t \leftarrow \mathcal{B}} = p(t)$. Then $\mathcal{B}_0 = \mathcal{B}$ and $\mathcal{B}_1 = \mathcal{C}$. □

That there is no corresponding analog of orientation for complex vector spaces. This is a consequence of the following theorem.

Theorem 3.5.7. *The general linear group $\mathrm{GL}_n(\mathbb{C})$ is connected.*

Proof. We show that it is path connected (which is equivalent as $\mathrm{GL}_n(\mathbb{C})$ is an open subset of Euclidean space). The proof is very much like the proof of Theorem 3.5.1, but easier. We show that there are paths joining the identity matrix to the usual elementary matrices.

(1) For

$$E = \begin{bmatrix} 1 & & & \\ & 1 & & a \\ & & \ddots & \\ & & & 1 \end{bmatrix}$$

we have

$$p(t) = \begin{bmatrix} 1 & & & \\ & 1 & & a_t \\ & & \ddots & \\ & & & 1 \end{bmatrix}$$

with $a_t = ta$.

(2) For

$$E = \begin{bmatrix} 1 &&&&&& \\ & \ddots &&&&& \\ && 1 &&&& \\ &&& c &&& \\ &&&& 1 && \\ &&&&& \ddots & \\ &&&&&& 1 \end{bmatrix} \quad \text{with } c = re^{i\theta},$$

we have

$$p(t) = \begin{bmatrix} 1 &&&&&& \\ & 1 &&&&& \\ && \ddots &&&& \\ &&& c_t &&& \\ &&&& 1 && \\ &&&&& \ddots & \\ &&&&&& 1 \end{bmatrix} \quad \text{with } c_t = e^{t\ln(r)}e^{ti\theta}.$$

(3) For

$$E = \begin{bmatrix} 1 &&&&&&&&& \\ & \ddots &&&&&&&& \\ && 1 &&&&&&& \\ &&& 0 &&& 1 &&& \\ &&&& 1 &&&&& \\ &&&&& \ddots &&&& \\ &&&&&& 1 &&& \\ &&& 1 &&&& 0 && \\ &&&&&&&& 1 & \\ &&&&&&&&& \ddots & \\ &&&&&&&&&& 1 \end{bmatrix}$$

we have

$$p(t) = \begin{bmatrix} 1 & & & & & & & & & & \\ & \ddots & & & & & & & & & \\ & & 1 & & & & & & & & \\ & & & a_t & & & & b_t & & & \\ & & & & 1 & & & & & & \\ & & & & & \ddots & & & & & \\ & & & & & & 1 & & & & \\ & & & c_t & & & & d_t & & & \\ & & & & & & & & 1 & & \\ & & & & & & & & & \ddots & \\ & & & & & & & & & & 1 \end{bmatrix}$$

with

$$\begin{bmatrix} a_t & b_t \\ c_t & d_t \end{bmatrix} = \begin{bmatrix} \cos\left(\pi t/2\right) & -e^{\pi i t}\sin\left(\pi t/2\right) \\ \sin\left(\pi t/2\right) & e^{\pi i t}\cos\left(\pi t/2\right) \end{bmatrix}. \qquad \square$$

We may also consider the effect of nonsingular linear transformations on orientation.

DEFINITION 3.5.8. Let V be an n-dimensional real vector space and let $\mathcal{T} : V \to V$ be a nonsingular linear transformation. Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a basis of V. Then $\mathcal{C} = \{\mathcal{T}(v_1), \ldots, \mathcal{T}(v_n\})$ is also a basis of V. If $\mathcal{B}$ and $\mathcal{C}$ give the same orientation of V then $\mathcal{T}$ is *orientation preserving*, while if $\mathcal{B}$ and $\mathcal{C}$ give opposite orientations of V then $\mathcal{T}$ is *orientation reversing*. $\diamond$

The fact that this is well-defined, i.e., independent of the choice of basis $\mathcal{B}$, follows from the following proposition, which proves a more precise result.

Proposition 3.5.9. *Let V be an n-dimensional real vector space and let $\mathcal{T} : V \to V$ be a nonsingular linear transformation. Then $\mathcal{T}$ is orientation preserving if* $\det(\mathcal{T}) > 0$, *and $\mathcal{T}$ is orientation reversing if* $\det(\mathcal{T}) < 0$.

REMARK 3.5.10. Suppose we begin with a complex vector space V of dimension n. We may then "forget" the fact that we have complex numbers acting as scalars and in this way regard V as a real vector space $V_{\mathbb{R}}$ of dimension $2n$. In this situation $V_{\mathbb{R}}$ has a canonical orientation. Choosing any basis $\mathcal{B} = \{v_1, \ldots, v_n\}$ of V, we obtain a basis $\mathcal{B}_{\mathbb{R}} = \{v_1, iv_1, \ldots, v_n, iv_n\}$

of $V_{\mathbb{R}}$. It is easy to check that if $\mathcal{C}$ is any other basis of V, then $\mathcal{C}_{\mathbb{R}}$ gives the same orientation of $V_{\mathbb{R}}$ as $\mathcal{B}_{\mathbb{R}}$ does. Furthermore, suppose we have an arbitrary linear transformation $\mathcal{T} : V \to V$. By "forgetting" the complex structure we similarly obtain a linear transformation $\mathcal{T}_{\mathbb{R}} : V_{\mathbb{R}} \to V_{\mathbb{R}}$. In this situation $\det(\mathcal{T}_{\mathbb{R}}) = \det(\mathcal{T})\overline{\det(\mathcal{T})}$. In particular, if $\mathcal{T}$ is nonsingular, then $\mathcal{T}_{\mathbb{R}}$ is not only nonsingular but also orientation preserving. $\diamond$

3.6 HILBERT MATRICES

In this section we present, without proofs, a single family of examples, the Hilbert matrices. This family is both interesting and important. More information on it can be found in the article "Tricks or Treats with the Hilbert Matrix" by M. D. Choi, Amer. Math Monthly 90 (1983), 301–312.

In this section we adopt the convention that the rows and columns of an n-by-n matrix are numbered from 0 *to* $n-1$.

DEFINITION 3.6.1. The n-by-n Hilbert matrix is the matrix $H = (h_{ij})$ with $h_{ij} = 1/(i+j+1)$. $\diamond$

Theorem 3.6.2. *(1) The determinant of H_n is*

$$\det\left(H_n\right) = \frac{\left(1!2!\cdots(n-1)!\right)^4}{1!2!\cdots(2n-1)!}.$$

(2) Let $G_n = (g_{ij}) = H_n^{-1}$. Then G_n has entries

$$g_{ij} = (-1)^{i+j}(i+j+1)\binom{n+i}{n-1-j}\binom{n+i}{n-1-i}\binom{i+j}{i}\binom{i+j}{j}.$$

REMARK 3.6.3. The entries of H_n^{-1} are all integers, and it is known that $\det(H_n)$ is the reciprocal of an integer. $\diamond$

EXAMPLE 3.6.4. (1) $\det(H_2) = 1/12$ and

$$H_2^{-1} = \begin{bmatrix} 4 & -6 \\ -6 & 12 \end{bmatrix}.$$

(2) $\det(H_3) = 1/2160$ and

$$H_3^{-1} = \begin{bmatrix} 9 & -36 & 30 \\ -36 & 192 & -180 \\ 30 & -180 & 180 \end{bmatrix}.$$

(3) $\det(H_4) = 1/6048000$ and

$$H_4^{-1} = \begin{bmatrix} 16 & -120 & 240 & -140 \\ -120 & 1200 & -2700 & 1680 \\ 240 & -2700 & 6480 & -4200 \\ -140 & 1680 & -4200 & 2800 \end{bmatrix}.$$

(4) $\det(H_5) = 1/266716800000$ and

$$H_5^{-1} = \begin{bmatrix} 25 & -300 & 1050 & -1400 & 630 \\ -300 & 4800 & -18900 & 26880 & -12600 \\ 1050 & -18900 & 79380 & -117600 & 56700 \\ -1400 & 26880 & -117600 & 179200 & -88200 \\ 630 & -12600 & 56700 & -88200 & 44100 \end{bmatrix}.$$

While we do not otherwise deal with numerical linear algebra in this book, the Hilbert matrices present examples that are so pretty and striking, that we cannot resist giving a pair.

These examples arise from the fact that, while H_n is nonsingular, its determinant is very close to zero. (In technical terms, H_n is "ill-conditioned".) We can already see this when $n = 3$. $\diamond$

EXAMPLE 3.6.5. (1) Consider the equation

$$H_3 v = \begin{bmatrix} 11/6 \\ 13/12 \\ 47/60 \end{bmatrix} = \begin{bmatrix} 1.833\ldots \\ 1.0833\ldots \\ 0.7833\ldots \end{bmatrix}.$$

It has solution

$$v = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}.$$

Let us round off the right-hand side to two significant digits and consider the equation

$$H_3 v = \begin{bmatrix} 1.8 \\ 1.1 \\ 0.78 \end{bmatrix}.$$

It has solution

$$v = \begin{bmatrix} 0 \\ 6 \\ -3.6 \end{bmatrix}.$$

(2) Let us round off the entries of H_3 to two significant figures to obtain the matrix

$$\begin{bmatrix} 1 & 0.5 & 0.33 \\ 0.5 & 0.33 & 0.25 \\ 0.33 & 0.25 & 0.2 \end{bmatrix}.$$

It has inverse

$$\frac{1}{63}\begin{bmatrix} 3500 & -17500 & 16100 \\ -17500 & 91100 & -85000 \\ 16100 & -85000 & 80000 \end{bmatrix}.$$

Rounding the entries off to the nearest integer, it is

$$\begin{bmatrix} 56 & -278 & 256 \\ -278 & 1446 & -1349 \\ 256 & -1349 & 1270 \end{bmatrix}. \qquad \diamond$$

CHAPTER 4

The structure of a linear transformation I

In this chapter we begin our analysis of the structure of a linear transformation $\mathcal{T} : V \to V$, where V is a finite-dimensional $\mathbb{F}$-vector space.

We have arranged our exposition in order to bring some of the most important concepts to the fore first. Thus we begin with the notions of eigenvalues and eigenvectors, and we introduce the characteristic and minimum polynomials of a linear transformation early in this chapter as well. In this way we can get to some of the most important structural results, including results on diagonalizability and the Cayley-Hamilton theorem, as quickly as possible.

Recall our metaphor of coordinates as a language in which to speak about vectors and linear transformations. Consider a linear transformation $\mathcal{T} : V \to V$, V a finite-dimensional vector space. Once we choose a basis $\mathcal{B}$ of V, i.e., a language, we have the coordinate vector $[v]_{\mathcal{B}}$ of every vector v in V, a vector in $\mathbb{F}^n$, and the matrix $[\mathcal{T}]_{\mathcal{B}}$ of the linear transformation $\mathcal{T}$, an n-by-n matrix, (where n is the dimension of V) with the property that $[\mathcal{T}(v)]_{\mathcal{B}} = [\mathcal{T}]_{\mathcal{B}}[v]_{\mathcal{B}}$. If we choose a different basis $\mathcal{C}$, i.e., a different language, we get different coordinate vectors $[v]_{\mathcal{C}}$ and a different matrix $[\mathcal{T}]_{\mathcal{C}}$ of $\mathcal{T}$, though again we have the identity $[\mathcal{T}(v)]_{\mathcal{C}} = [\mathcal{T}]_{\mathcal{C}}[v]_{\mathcal{C}}$. We have also seen change of basis matrices, which tell us how to translate between languages.

But here, mathematical language is different than human language. In human language, if we have a problem expressed in English, and we translate it into German, we haven't helped the situation. We have the same problem, expressed differently, but no easier to solve.

In linear algebra the situation is different. Given a linear transformation $\mathcal{T} : V \to V$, V a finite-dimensional vector space, there is a preferred basis $\mathcal{B}$ of V, i.e., a best language in which to study the problem, one that makes $[\mathcal{T}]_{\mathcal{B}}$ as simple as possible and makes the structure of $\mathcal{T}$ easiest to understand. This is the language of eigenvalues, eigenvectors, and generalized eigenvectors.

We first consider a simple example to motivate our discussion.

Let A be the matrix

$$A = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$$

and consider $\mathcal{T}_A : \mathbb{R}^2 \to \mathbb{R}^2$ (where, as usual, $\mathcal{T}_A(v) = Av$). Also, consider the standard basis $\mathcal{E}$, so $\begin{bmatrix} x \\ y \end{bmatrix}_{\mathcal{E}} = \begin{bmatrix} x \\ y \end{bmatrix}$ for every vector $\begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{R}^2$, and furthermore $[\mathcal{T}_A]_{\mathcal{E}} = A$. $\mathcal{T}_A$ looks simple, and indeed it is easy to understand. We observe that $\mathcal{T}_A(e_1) = 2e_1$, where $e_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ is the first standard basis vector in $\mathcal{E}$, and $\mathcal{T}_A(e_2) = 3e_2$, where $e_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ is the second standard basis vector in $\mathcal{E}$. Geometrically, $\mathcal{T}_A$ takes the vector e_1 and stretches it by a factor of 2 in its direction, and takes the vector e_2 and stretches it by a factor of 3 in its direction.

On the other hand, let B be the matrix

$$B = \begin{bmatrix} -4 & -14 \\ 3 & 9 \end{bmatrix}$$

and consider $\mathcal{T}_B : \mathbb{R}^2 \to \mathbb{R}^2$. Now $\mathcal{T}_B(e_1) = B\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} -4 \\ 3 \end{bmatrix}$, and $\mathcal{T}_B(e_2) = B\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -14 \\ 9 \end{bmatrix}$, and $\mathcal{T}_B$ looks like a mess. $\mathcal{T}_B$ takes each of these vectors to some seemingly random vector in the plane, and there seems to be no rhyme or reason here. But this appearance is deceptive, and comes from the fact that we are studying B by using the standard basis $\mathcal{E}$, i.e., in the $\mathcal{E}$ language, which is the wrong language for the problem. Instead, let us choose the basis $\mathcal{B} = \{b_1, b_2\} = \left\{\begin{bmatrix} 7 \\ -3 \end{bmatrix}, \begin{bmatrix} -2 \\ 1 \end{bmatrix}\right\}$. Then $\mathcal{T}_B(b_1) = B\begin{bmatrix} 7 \\ -3 \end{bmatrix} = \begin{bmatrix} 14 \\ -6 \end{bmatrix} = 2\begin{bmatrix} 7 \\ -3 \end{bmatrix} = 2b_1$, and $\mathcal{T}_B(b_2) = B\begin{bmatrix} -2 \\ 1 \end{bmatrix} = \begin{bmatrix} -6 \\ 3 \end{bmatrix} = 3\begin{bmatrix} -2 \\ 1 \end{bmatrix} = 3b_2$. Thus $\mathcal{T}_B$ has exactly the same geometry as $\mathcal{T}_A$: It takes the vector b_1 and stretches it by a factor of 2 in its direction, and it takes the vector b_2 and stretches it by a factor of 3 in its direction. So we should study $\mathcal{T}_B$ by using the $\mathcal{B}$ basis, i.e., in the $\mathcal{B}$ language. This is the right language for our problem, as it makes $\mathcal{T}_B$ easiest to understand. Referring to Remark 2.2.8 we see that

$$[\mathcal{T}_B]_{\mathcal{B}} = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} = [\mathcal{T}_A]_{\mathcal{E}}.$$

This "right" language is the language of eigenvalues, eigenvectors, and generalized eigenvectors, and the language that lets us express the matrix of a linear transformation in "canonical form".

But before we proceed further, let me make two more remarks.

On the one hand, even if V is not finite dimensional, it is often the case that we still want to study eigenvalues and eigenvectors for a linear transformation $\mathcal{T}$, as these are important structural features of $\mathcal{T}$ and still give us a good way (sometimes the best way) of understanding $\mathcal{T}$.

On the other hand, in studying a linear transformation $\mathcal{T}$ on a finite-dimensional vector space, it is often a big mistake to pick a basis $\mathcal{B}$ and study $[\mathcal{T}]_{\mathcal{B}}$. It may be unnatural to pick any basis at all. $\mathcal{T}$ is what comes naturally and is usually what we want to study, even if in the end we can get important information about $\mathcal{T}$ by looking at $[\mathcal{T}]_{\mathcal{B}}$. Let me again emphasize this point: Linear algebra is about linear transformations, not matrices.

4.1 EIGENVALUES, EIGENVECTORS, AND GENERALIZED EIGENVECTORS

In this section we introduce some of the most important structural information associated to a linear transformation.

DEFINITION 4.1.1. Let $\mathcal{T} : V \to V$ be a linear transformation. Let $\lambda \in \mathbb{F}$. If $\operatorname{Ker}(\mathcal{T} - \lambda\mathcal{I}) \neq \{0\}$, then λ is an *eigenvalue* of $\mathcal{T}$. In this case, any nonzero $v \in \operatorname{Ker}(\mathcal{T} - \lambda\mathcal{I})$ is an *eigenvector* of $\mathcal{T}$, and the subspace $\operatorname{Ker}(\mathcal{T} - \lambda\mathcal{I})$ of V is an *eigenspace* of $\mathcal{T}$. In this situation, λ, v, and $\operatorname{Ker}(\mathcal{T} - \lambda\mathcal{I})$ are *associated.* ◇

REMARK 4.1.2. Let $v \in V$, $v \neq 0$. If $v \in \operatorname{Ker}(\mathcal{T} - \lambda\mathcal{I})$, then $(\mathcal{T} - \lambda\mathcal{I})(v) = 0$, i.e., $\mathcal{T}(v) = \lambda v$, and conversely, the traditional definition of an eigenvector. ◇

We will give some examples of this very important concept shortly, but it is convenient to generalize it first.

DEFINITION 4.1.3. Let $\mathcal{T} : V \to V$ be a linear transformation and let $\lambda \in \mathbb{F}$ be an eigenvalue of $\mathcal{T}$. The *generalized eigenspace* of $\mathcal{T}$ associated to λ is the subspace of V given by

$$\{v \mid (\mathcal{T} - \lambda\mathcal{I})^k(v) = 0 \text{ for some positive integer } k\}.$$

If v is a nonzero vector in this generalized eigenspace, then v is a *generalized eigenvector* associated to the eigenvalue λ. For such a v, the smallest positive integer k for which $(\mathcal{T} - \lambda\mathcal{I})^k(v) = 0$ is the *index* of v. ◇

REMARK 4.1.4. A generalized eigenvector of index 1 is just an eigenvector. ◇

For a linear transformation $\mathcal{T}$ and an eigenvalue λ of $\mathcal{T}$, we let E_λ denote the eigenspace $E_\lambda = \operatorname{Ker}(\mathcal{T} - \lambda\mathcal{I})$. For a positive integer k, we let E_λ^k be the subspace $E_\lambda^k = \operatorname{Ker}(\mathcal{T} - \lambda\mathcal{I})^k$. We let E_λ^∞ denote the generalized eigenspace associated to the eigenvalue λ. We see that $E_\lambda^1 \subseteq E_\lambda^2 \subseteq \cdots$ and that the union of these subspaces is E_λ^∞.

EXAMPLE 4.1.5. (1) Let $V = {}^r\mathbb{F}^\infty$ and let $\mathbf{L} : V \to V$ be left shift. Then $\mathbf{L}$ has the single eigenvalue $\lambda = 0$ and the eigenspace E_0 is 1-dimensional, $E_0 = \{(a_1, a_2, \ldots) \in V \mid a_i = 0 \text{ for } i > 1\}$. More generally, $E_0^k = \{(a_1, a_2, \ldots) \in V \mid a_i = 0 \text{ for } i > k\}$, so $\dim E_0^k = k$ for every k, and finally $V = E_0^\infty$. In contrast, $\mathbf{R} : V \to V$ does not have any eigenvalues.

(2) Let $V = {}^r\mathbb{F}^{\infty\infty}$ and let $\mathbf{L} : V \to V$ be left shift. Then for any $\lambda \in \mathbb{F}$, E_λ is 1-dimensional with basis $\{(1, \lambda, \lambda^2, \ldots)\}$. It is routine to check that E_λ^k is k-dimensional for every $\lambda \in \mathbb{F}$ and every positive integer k. In contrast, $\mathbf{R} : V \to V$ does not have any eigenvalues.

(3) Let $\mathbb{F}$ be a field of characteristic 0 and let $V = P(\mathbb{F})$, the space of all polynomials with coefficients in $\mathbb{F}$. Let $\mathbf{D} : V \to V$ be differentiation, $\mathbf{D}(p(x)) = p'(x)$. Then $\mathbf{D}$ has the single eigenvalue 0 and the corresponding eigenspace E_0 is 1-dimensional, consisting of the constant polynomials. More generally, E_0^k is k-dimensional, consisting of all polynomials of degree at most $k - 1$.

(4) Let $V = P(\mathbb{F})$ be the space of all polynomials with coefficients in a field of characteristic 0 and let $\mathcal{T} : V \to V$ be defined by $\mathcal{T}(p(x)) = xp'(x)$. Then the eigenvalues of $\mathcal{T}$ are the nonnegative integers, and for every nonnegative integer m the eigenspace E_m is 1-dimensional with basis $\{x^m\}$.

(5) Let V be the space of holomorphic functions on $\mathbb{C}$, and let $\mathbf{D} : V \to V$ be differentiation, $\mathbb{D}(f(z)) = f'(z)$. For any complex number λ, E_λ

is 1-dimensional with basis $f(z) = e^{\lambda z}$. Also, E_λ^k is k-dimensional with basis $\{e^{\lambda z}, ze^{\lambda z}, \ldots, z^{k-1}e^{\lambda z}\}$. ◇

Now we turn to some finite-dimensional examples. We adopt the standard language that the eigenvalues, eigenvectors, etc. of an n-by-n matrix A are the eigenvalues, eigenvectors, etc. of $\mathcal{T}_A : \mathbb{F}^n \to \mathbb{F}^n$ (where $\mathcal{T}_A(v) = Av$).

EXAMPLE 4.1.6. (1) Let $\lambda_1, \ldots, \lambda_n$ be distinct elements of $\mathbb{F}$ and let A be the n-by-n diagonal matrix

$$A = \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix}.$$

For each $i = 1, \ldots, n$, λ_i is an eigenvalue of A with 1-dimensional eigenspace E_{λ_i} with basis $\{e_i\}$.

(2) Let λ be an element of $\mathbb{F}$ and let A be the n-by-n matrix

$$A = \begin{bmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & & 1 \\ & & & & \lambda \end{bmatrix}$$

with entries of λ on the diagonal, 1 immediately above the diagonal, and 0 everywhere else. For each $k = 1, \ldots, n$, e_k is a generalized eigenvector of index k, and the generalized eigenspace E_λ^k is k-dimensional with basis $\{e_1, \ldots, e_k\}$. ◇

Now we introduce the characteristic polynomial.

DEFINITION 4.1.7. Let A be an n-by-n matrix. The *characteristic polynomial* $c_A(x)$ of A is the polynomial

$$c_A(x) = \det(xI - A). \qquad ◇$$

REMARK 4.1.8. By properties of the determinant it is clear that $c_A(x)$ is a monic polynomial of degree n. ◇

Lemma 4.1.9. *Let A and B be similar matrices. Then $c_A(x) = c_B(x)$.*

Proof. If $B = PAP^{-1}$, then $c_B(x) = \det(xI - B) = \det(xI - PAP^{-1}) = \det(P(xI - A)P^{-1}) = \det(xI - A) = c_A(x)$ by Corollary 3.3.2. □

DEFINITION 4.1.10. Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. Let $\mathcal{B}$ be any basis of V and let $A = [\mathcal{T}]_{\mathcal{B}}$. The characteristic polynomial $c_{\mathcal{T}}(x)$ is the polynomial

$$c_{\mathcal{T}}(x) = c_A(x) = \det(xI - A).$$

◇

REMARK 4.1.11. By Corollary 2.3.11 and Lemma 4.1.9, $c_{\mathcal{T}}(x)$ is well-defined (i.e., independent of the choice of basis $\mathcal{B}$ of V). ◇

Theorem 4.1.12. *Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. Then λ is an eigenvalue of $\mathcal{T}$ if and only if λ is a root of the characteristic polynomial $c_{\mathcal{T}}(x)$, i.e., if and only if $c_{\mathcal{T}}(\lambda) = 0$.*

Proof. Let $\mathcal{B}$ be a basis of V and let $A = [\mathcal{T}]_{\mathcal{B}}$. Then by definition λ is an eigenvalue of $\mathcal{T}$ if and only if there is a nonzero vector v in $\mathrm{Ker}(\mathcal{T} - \lambda\mathcal{I})$, i.e., if and only if $(A - \lambda I)u = 0$ for some nonzero vector u in $\mathbb{F}^n$ (where the connection is that $u = [v]_{\mathcal{B}}$). This is the case if and only if $A - \lambda I$ is singular, which is the case if and only if $\det(A - \lambda I) = 0$. But $\det(A - \lambda I) = (-1)^n \det(\lambda I - A)$, where $n = \dim(V)$, so this is the case if and only if $c_{\mathcal{T}}(\lambda) = c_A(\lambda) = \det(\lambda I - A) = 0$. □

REMARK 4.1.13. We have defined $c_A(x) = \det(xI - A)$ and this is the correct definition, as we want $c_A(x)$ to be a monic polynomial. In actually finding eigenvectors or generalized eigenvectors, it is generally more convenient to work with $A - \lambda I$ rather than $\lambda I - A$. Indeed, when it comes to finding chains of generalized eigenvectors, it is almost essential to use $A - \lambda I$, as using $\lambda I - A$ would introduce spurious minus signs, which would have to be corrected for. ◇

For the remainder of this section we assume that V is finite dimensional.

DEFINITION 4.1.14. Let $\mathcal{T} : V \to V$ and let λ be an eigenvalue of $\mathcal{T}$. The *algebraic multiplicity* of λ, alg-mult(λ), is the multiplicity of λ as a root of the characteristic polynomial $c_{\mathcal{T}}(x)$. The *geometric multiplicity* of λ, geom-mult (λ), is the dimension of the associated eigenspace $E_\lambda = \mathrm{Ker}(\mathcal{T} - \lambda\mathcal{I})$. ◇

We use *multiplicity* to mean algebraic multiplicity, as is standard.

Lemma 4.1.15. *Let $\mathcal{T} : V \to V$ and let λ be an eigenvalue of $\mathcal{T}$. Then* $1 \leq \text{geom-mult}(\lambda) \leq \text{alg-mult}(\lambda)$.

Proof. By definition, if λ is an eigenvalue of $\mathcal{T}$ there exists a (nonzero) eigenvector, so $1 \leq \dim(E_\lambda)$.

Suppose $\dim(E_\lambda) = d$ and let $\{v_1, \dots, v_d\} = \mathcal{B}_1$ be a basis for E_λ. Extend $\mathcal{B}_1$ to a basis $\mathcal{B} = \{v_1, \dots, v_n\}$ of V. Then

$$[\mathcal{T}]_{\mathcal{B}} = \begin{bmatrix} \lambda I & B \\ 0 & D \end{bmatrix} = A,$$

a block matrix with the upper left-hand block d-by-d. Then

$$[x\mathcal{I} - \mathcal{T}]_{\mathcal{B}} = xI - A = \begin{bmatrix} xI - \lambda I & -B \\ 0 & xI - D \end{bmatrix} = \begin{bmatrix} (x-\lambda)I & -B \\ 0 & xI - D \end{bmatrix}$$

so

$$\begin{aligned} c_{\mathcal{T}}(x) &= \det(xI - A) = \det\big((x-\lambda)I\big)\det(xI - D) \\ &= (x-\lambda)^d \det(xI - D) \end{aligned}$$

and hence $d \leq \text{alg-mult}(\lambda)$. □

Corollary 4.1.16. *Let $\mathcal{T} : V \to V$ and let λ be an eigenvalue of $\mathcal{T}$ with* $\text{alg-mult}(\lambda) = 1$. *Then* $\text{geom-mult}(\lambda) = 1$.

It is important to observe that the existence of eigenvalues and eigenvectors depends on the field $\mathbb{F}$, as we see from the next example.

EXAMPLE 4.1.17. For any nonzero rational number t let A_t be the matrix

$$A_t = \begin{bmatrix} 0 & 1 \\ t & 0 \end{bmatrix},$$

so

$$A_t^2 = \begin{bmatrix} t & 0 \\ 0 & t \end{bmatrix} = tI.$$

Let λ be an eigenvalue of A_t with associated eigenvector v. Then, on the one hand,

$$A_t^2(v) = A_t\big(A_t(v)\big) = A_t(\lambda v) = \lambda A_t(v) = \lambda^2 v,$$

but, on the other hand,

$$A_t^2(v) = tI(v) = tv,$$

so $\lambda^2 = t$.

(1) Suppose $t = 1$. Then $\lambda^2 = 1$, $\lambda = \pm 1$, and we have the eigenvalue $\lambda = 1$ with associated eigenvector $v = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$, and the eigenvalue $\lambda = -1$ with associated eigenvector $v = \begin{bmatrix} 1 \\ -1 \end{bmatrix}$.

(2) Suppose $t = 2$. If we regard A as being defined over $\mathbb{Q}$, then there is no $\lambda \in \mathbb{Q}$ with $\lambda^2 = 2$, so A has no eigenvalues. If we regard A as being defined over $\mathbb{R}$, then $\lambda = \pm\sqrt{2}$, and $\lambda = \sqrt{2}$ is an eigenvalue with associated eigenvector $\begin{bmatrix} 1 \\ \sqrt{2} \end{bmatrix}$, and $\lambda = -\sqrt{2}$ is an eigenvalue with associated eigenvector $\begin{bmatrix} 1 \\ -\sqrt{2} \end{bmatrix}$.

(3) Suppose $t = -1$. If we regard A as being defined over $\mathbb{R}$, then there is no $\lambda \in \mathbb{R}$ with $\lambda^2 = -1$, so A has no eigenvalues. If we regard A as being defined over $\mathbb{C}$, then $\lambda = \pm i$, and $\lambda = i$ is an eigenvalue with associated eigenvector $\begin{bmatrix} 1 \\ i \end{bmatrix}$, and $\lambda = -i$ is an eigenvalue with associated eigenvector $\begin{bmatrix} 1 \\ -i \end{bmatrix}$. ◇

Now we introduce the minimum polynomial.

Lemma 4.1.18. *Let A be an n-by-n matrix. There is a nonzero polynomial $p(x)$ with $p(A) = 0$.*

Proof. The set of matrices $\{I, A, \ldots, A^{n^2}\}$ is a set of $n^2 + 1$ elements of a vector space of dimension n^2, and so must be linearly dependent. Thus there exist scalars $c_0, \ldots, c_{n^2}$, not all zero, with $c_0 I + c_1 A + \cdots + c_{n^2} A^{n^2} = 0$. Then $p(A) = 0$ where $p(x)$ is the nonzero polynomial $p(x) = c_{n^2} x^{n^2} + \cdots + c_1 x + c_0$. □

Theorem 4.1.19. *Let A be an n-by-n matrix. There is a unique monic polynomial $m_A(x)$ of lowest degree with $m_A(A) = 0$. Furthermore, $m_A(x)$ divides every polynomial $p(x)$ with $p(A) = 0$.*

Proof. By Lemma 4.1.18, there is some nonzero polynomial $p(x)$ with $p(A) = 0$.

If $p_1(x)$ and $p_2(x)$ are any polynomials with $p_1(A) = 0$ and $p_2(A) = 0$, and $q(x) = p_1(x) + p_2(x)$, then $q(A) = p_1(A) + p_2(A) = 0 + 0 = 0$. Also, if $p_1(x)$ is any polynomial with $p_1(A) = 0$, and $r(x)$ is any polynomial, and $q(x) = p_1(x)r(x)$, then $q(A) = p_1(A)r(A) = 0r(A) =$

0. Thus, in the language of Definition A.1.5, the set of polynomials $\{p(x) \mid p(A) = 0\}$ is a nonzero ideal, and so by Lemma A.1.8 there is a unique polynomial $m_A(x)$ as claimed. □

DEFINITION 4.1.20. The polynomial $m_A(x)$ of Theorem 4.1.19 is the *minimum polynomial* of A. ◇

Lemma 4.1.21. *Let A and B be similar matrices. Then $m_A(x) = m_B(x)$.*

Proof. If $B = PAP^{-1}$, and $p(x)$ is any polynomial with $p(A) = 0$, then $p(B) = Pp(A)P^{-1} = P0P^{-1} = 0$, and vice-versa. □

DEFINITION 4.1.22. Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. Let $\mathcal{B}$ be any basis of V and let $A = [\mathcal{T}]_{\mathcal{B}}$. The *minimum polynomial* of $\mathcal{T}$ is the polynomial $m_{\mathcal{T}}(x)$ defined by $m_{\mathcal{T}}(x) = m_A(x)$. ◇

REMARK 4.1.23. By Corollary 2.3.11 and Lemma 4.1.21, $m_{\mathcal{T}}(x)$ is well-defined (i.e., independent of the choice of basis $\mathcal{B}$ of V). Alternatively we can see that $m_{\mathcal{T}}(x)$ is well-defined as for any linear transformation $\mathcal{S} : V \to V$, $\mathcal{S} = 0$ (i.e., $\mathcal{S}$ is the 0 linear transformation) if and only if the matrix $[\mathcal{S}]_{\mathcal{B}} = 0$ (i.e., $[\mathcal{S}]_{\mathcal{B}}$ is the 0 matrix) in any and every basis $\mathcal{B}$ of V. ◇

4.2 SOME STRUCTURAL RESULTS

In this section we prove some basic but important structural results about a linear transformation, obtaining information about generalized eigenspaces, direct sum decompositions, and the relationship between the characteristic and minimum polynomials. As an application, we derive the famous Cayley-Hamilton theorem.

While we prove much stronger results later, the following result is so easy that we will pause to obtain it here.

DEFINITION 4.2.1. Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. $\mathcal{T}$ is *triangularizable* if there is a basis $\mathcal{B}$ of V in which the matrix $[\mathcal{T}]_{\mathcal{B}}$ is upper triangular. ◇

Theorem 4.2.2. *Let V be a finite-dimensional vector space over the field $\mathbb{F}$ and let $\mathcal{T} : V \to V$ be a linear transformation. Then $\mathcal{T}$ is triangularizable if and only if its characteristic polynomial $c_{\mathcal{T}}(x)$ is a product of linear factors. In particular, if $\mathbb{F}$ is algebraically closed then every $\mathcal{T} : V \to V$ is triangularizable.*

Proof. If $[\mathcal{T}]_{\mathcal{B}} = A$ is an upper triangular matrix with diagonal entries $d_1, \dots, d_n$, then $c_{\mathcal{T}}(x) = c_A(x) = \det(xI - A) = (x - d_1)\cdots(x - d_n)$ is a product of linear factors.

We prove the converse by induction on $n = \dim(V)$. Let $c_{\mathcal{T}}(x) = (x - d_1)\cdots(x - d_n)$. Then d_1 is an eigenvalue of $\mathcal{T}$; choose an eigenvector v_1 and let V_1 be the subspace of V generated by v_1. Let $\overline{V} = V/V_1$. Then $\mathcal{T}$ induces $\overline{\mathcal{T}} : \overline{V} \to \overline{V}$ with $c_{\overline{\mathcal{T}}}(x) = (x-d_2)\cdots(x-d_n)$. By induction, $\overline{V}$ has a basis $\overline{\mathcal{B}} = \{\overline{v}_2, \dots, \overline{v}_n\}$ with $[\overline{\mathcal{T}}]_{\overline{\mathcal{B}}} = D$ upper triangular. Let $v_i \in V$ with $\pi(v_i) = \overline{v}_i$ for $i = 2, \dots, n$, and let $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$. Then

$$[\mathcal{T}]_{\mathcal{B}} = \begin{bmatrix} d_1 & C \\ 0 & D \end{bmatrix}$$

for some 1-by-$(n-1)$ matrix C. Regardless of what C is, this matrix is upper triangular. □

Lemma 4.2.3. *(1) Let v be an eigenvector of $\mathcal{T}$ with associated eigenvalue λ and let $p(x) \in \mathbb{F}[x]$ be a polynomial. Then $p(\mathcal{T})(v) = p(\lambda)v$. Thus, if $p(\lambda) \neq 0$ then $p(\mathcal{T})(v) \neq 0$.*

(2) More generally, let v be a generalized eigenvector of $\mathcal{T}$ of index k with associated eigenvalue λ and let $p(x) \in \mathbb{F}[x]$ be a polynomial. Then $p(\mathcal{T})(v) = p(\lambda)v + v'$, where v' is a generalized eigenvector of $\mathcal{T}$ of index $k' < k$ with associated eigenvector λ. Thus if $p(\lambda) \neq 0$ then $p(\mathcal{T})(v) \neq 0$.

Proof. We can rewrite any polynomial $p(x) \in \mathbb{F}[x]$ in terms of $x - \lambda$:

$$p(x) = a_n(x-\lambda)^n + a_{n-1}(x-\lambda)^{n-1} + \cdots + a_1(x-\lambda) + a_0.$$

Setting $x = \lambda$ we see that $a_0 = p(\lambda)$.

(1) If v is an eigenvector of $\mathcal{T}$ with associated eigenvalue λ, then

$$\begin{aligned} p(\mathcal{T})(v) &= \big(a_n(\mathcal{T} - \lambda\mathcal{I})^n + \cdots + a_1(\mathcal{T} - \lambda\mathcal{I}) + p(\lambda)\mathcal{I}\big)(v) \\ &= p(\lambda)\mathcal{I}(v) = p(\lambda)v \end{aligned}$$

as all terms but the last vanish.

(2) If v is a generalized eigenvector of $\mathcal{T}$ of index k with associated eigenvalue λ, then

$$\begin{aligned} p(\mathcal{T})(v) &= \big(a_n(\mathcal{T} - \lambda\mathcal{I})^n + \cdots + a_1(\mathcal{T} - \lambda\mathcal{I}) + p(\lambda)\mathcal{I}\big)(v) \\ &= v' + p(\lambda)v \end{aligned}$$

where

$$\begin{aligned} v' &= \big(a_n(\mathcal{T} - \lambda\mathcal{I})^n + \cdots + a_1(\mathcal{T} - \lambda\mathcal{I})\big)(v) \\ &= \big(a_n(\mathcal{T} - \lambda\mathcal{I})^{n-1} + \cdots + a_1\big)(\mathcal{T} - \lambda\mathcal{I})(v) \end{aligned}$$

is a generalized eigenvector of $\mathcal{T}$ of index at most $k-1$ associated to λ. $\square$

Lemma 4.2.4. *Let $\mathcal{T} : V \to V$ be a linear transformation with $c_{\mathcal{T}}(x) = (x-\lambda_1)^{e_1} \cdots (x-\lambda_m)^{e_m}$, with $\lambda_1, \ldots, \lambda_m$ distinct. Let $W_i = E_{\lambda_i}^{\infty}$ be the generalized eigenspace of $\mathcal{T}$ associated to the eigenvalue λ_i. Then W_i is a subspace of V of dimension e_i. Also, $W_i = E_{\lambda_i}^{e_i}$, i.e., any generalized eigenvector of $\mathcal{T}$ associated to λ_i has index at most e_i.*

Proof. In proof of Theorem 4.2.2, we may choose the eigenvalues in any order, so we choose λ_i first, e_i times. Then we find a basis $\mathcal{B}$ of V with $[\mathcal{T}]_{\mathcal{B}}$ an upper triangular matrix

$$[\mathcal{T}]_{\mathcal{B}} = \begin{bmatrix} A & B \\ 0 & D \end{bmatrix},$$

where A is an upper triangular e_i-by-e_i matrix all of whose diagonal entries are equal to λ_i and D is an $(n-e_i)$-by-$(n-e_i)$ matrix all of whose diagonal entries are equal to the other λ_j's and thus are unequal to λ_i. Write $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_1'$ where $\mathcal{B}_1$ consists of the first e_i vectors in $\mathcal{B}$, $\mathcal{B}_1 = \{v_1, \ldots, v_{e_i}\}$. We claim that W_i is the subspace spanned by $\mathcal{B}_1$.

To see this, observe that

$$\big[\mathcal{T} - \lambda_i\mathcal{I}\big]_{\mathcal{B}} = \begin{bmatrix} A - \lambda_i I & B \\ 0 & D - \lambda_i I \end{bmatrix}$$

so

$$\big[\mathcal{T} - \lambda_i\mathcal{I}\big]_{\mathcal{B}}^{e_i} = \begin{bmatrix} \big(A - \lambda_i I\big)^{e_i} & B' \\ 0 & \big(D - \lambda_i I\big)^{e_i} \end{bmatrix}$$

for some submatrix B' (whose exact value is irrelevant). But $A - \lambda_i I$ is an e_i-by-e_i upper triangular matrix with all of its diagonal entries 0, and, as is easy to compute, $(A-\lambda_i I)^{e_i} = 0$. Also, $D - \lambda_i I$ is an e_i-by-e_i upper triangular matrix with none of its diagonal entries 0, and as is also easy to compute, $(D-\lambda_i I)^{e_i}$ is an upper triangular matrix with none of its diagonal entries equal to 0. Both of these statements remain true for any $e \geq e_i$.

Thus for any $e \geq e_i$,

$$\big[\mathcal{T} - \lambda_i\mathcal{I}\big]_{B}^{e} = \begin{bmatrix} 0 & B' \\ 0 & D' \end{bmatrix}$$

with D' an upper triangular matrix all of whose diagonal entries are nonzero. Then it is easy to see that for any $e \geq e_i$, $\mathrm{Ker}([\mathcal{T} - \lambda_i \mathcal{I}]^e_{\mathcal{B}})$ is the subspace of $\mathbb{F}^n$ generated by $\{e_1, \ldots, e_i\}$. Thus W_i is the subspace of V generated by $\{v_1, \ldots, v_{e_i}\} = B_1$, and is a subspace of dimension e_i. □

Lemma 4.2.5. *In the situation of Lemma 4.2.4,*

$$V = W_1 \oplus \cdots \oplus W_m.$$

Proof. Since $n = \deg c_{\mathcal{T}}(x) = e_1 + \cdots + e_m$, by Corollary 1.4.8(3) we need only show that if $0 = w_1 + \cdots + w_m$ with $w_i \in W_i$ for each i, then $w_i = 0$ for each i.

Suppose we have an expression

$$0 = w_1 + \cdots + w_i + \cdots + w_m$$

with $w_i \neq 0$. Let $q_i(x) = c_{\mathcal{T}}(x)/(x - \lambda_i)^{e_i}$, so $q_i(x)$ is divisible by $(x - \lambda_j)^{e_j}$ for every $j \neq i$, but $q_i(\lambda_i) \neq 0$. Then

$$\begin{aligned}
0 = q_i(\mathcal{T})(0) &= q_i(\mathcal{T})\big(w_1 + \cdots + w_i + \cdots + w_m\big)\\
&= q_i(\mathcal{T})\big(w_1\big) + \cdots + q_i(\mathcal{T})\big(w_i\big) + \cdots + q_i(\mathcal{T})\big(w_m\big)\\
&= 0 + \cdots + q_i(\mathcal{T})\big(w_i\big) + \cdots + 0\\
&= q_i(\mathcal{T})\big(w_i\big),
\end{aligned}$$

contradicting Lemma 4.2.3. □

Lemma 4.2.6. *Let $\mathcal{T} : V \to V$ be a linear transformation whose characteristic polynomial $c_{\mathcal{T}}(x)$ is a product of linear factors. Then*

(1) $m_{\mathcal{T}}(x)$ and $c_{\mathcal{T}}(x)$ have the same linear factors.

(2) $m_{\mathcal{T}}(x)$ divides $c_{\mathcal{T}}(x)$.

Proof. (1) Let $m_{\mathcal{T}}(x)$ have a factor $x - \lambda$, and let $n(x) = m_{\mathcal{T}}(x)/(x - \lambda)$. Then $n(\mathcal{T}) \neq 0$, so there is a vector v_0 with $v = n(\mathcal{T})(v_0) \neq 0$. Then $(\mathcal{T} - \lambda\mathcal{I})(v) = m_{\mathcal{T}}(\mathcal{T})(v) = 0$, i.e., $v \in \mathrm{Ker}(\mathcal{T} - \lambda\mathcal{I})$, so v is an eigenvector of $\mathcal{T}$ with associated eigenvalue λ. Thus $x - \lambda$ is a factor of $c_{\mathcal{T}}(x)$. Suppose $x - \lambda$ is a factor of $c_{\mathcal{T}}(x)$ that is not a factor of $m_{\mathcal{T}}(x)$, so that $m_{\mathcal{T}}(\lambda) \neq 0$. Choose an eigenvector v of $\mathcal{T}$ with associated eigenvector λ. Then on the one hand $m_{\mathcal{T}}(\mathcal{T}) = 0$ so $m_{\mathcal{T}}(\mathcal{T})(v) = 0$, but on the other hand, by Lemma 4.2.3, $m_{\mathcal{T}}(\mathcal{T})(v) = m_{\mathcal{T}}(\lambda)v \neq 0$, a contradiction.

(2) Since $V = W_1 \oplus \cdots \oplus W_m$ where $W_i = E^{e_i}_{\lambda_i}$, we can write any $v \in V$ as $v = w_1 + \cdots + w_m$ with $w_i \in W_i$.

Then

$$\begin{aligned} c_{\mathcal{T}}(\mathcal{T})(v) &= c_{\mathcal{T}}(\mathcal{T})\big(w_1 + \cdots + w_m\big) \\ &= c_{\mathcal{T}}(\mathcal{T})\big(w_1\big) + \cdots + c_{\mathcal{T}}(\mathcal{T})\big(w_m\big) \\ &= 0 + \cdots + 0 = 0 \end{aligned}$$

as for each i, $c_{\mathcal{T}}(x)$ is divisible by $(x - \lambda_i)^{e_i}$ and $(\mathcal{T} - \lambda_i \mathcal{I})^{e_i}(w_i) = 0$ by the definition of $E_{\lambda_i}^{e_i}$. But $m_{\mathcal{T}}(x)$ divides every polynomial $p(x)$ with $p(\mathcal{T}) = 0$, so $m_{\mathcal{T}}(x)$ divides $c_{\mathcal{T}}(x)$. □

This lemma has a famous corollary, originally proved by quite different methods.

Corollary 4.2.7 (Cayley-Hamilton theorem)**.** *Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. Then*

$$c_{\mathcal{T}}(\mathcal{T}) = 0.$$

Proof. In case $c_{\mathcal{T}}(x)$ factors into a product of linear factors,

$$c_{\mathcal{T}}(x) = (x - \lambda_1)^{e_1} \cdots (x - \lambda_m)^{e_m},$$

we showed this in the proof of Lemma 4.2.6.

In general, pick any basis $\mathcal{B}$ of V and let $A = [\mathcal{T}]_{\mathcal{B}}$. Then $c_{\mathcal{T}}(\mathcal{T}) = 0$ if and only if $c_A(A) = 0$. (Note $c_{\mathcal{T}}(x) = c_A(x)$.) Now A is a matrix with entries in $\mathbb{F}$, and we can consider the linear transformation $\mathcal{T}_A : \mathbb{F}^n \to \mathbb{F}^n$. But we may also take any extension field $\mathbb{E}$ of $\mathbb{F}$ and consider $\widetilde{\mathcal{T}} : \mathbb{E}^n \to \mathbb{E}^n$ defined by $\widetilde{\mathcal{T}}(v) = Av$. (So $\widetilde{\mathcal{T}} = \mathcal{T}_A$, but we are being careful to use a different notation as $\widetilde{\mathcal{T}}$ is defined on the new vector space $\mathbb{E}^n$.) Now $c_{\widetilde{\mathcal{T}}}(x) = c_A(x) = \det(xI - A) = c_{\mathcal{T}}(x)$. In particular, we may take $\mathbb{E}$ to be a field in which $c_A(x)$ splits into a product of linear factors. For example, we could take $\mathbb{E}$ to be the algebraic closure of $\mathbb{F}$, and then every polynomial $p(x) \in \mathbb{F}[x]$ splits into a product of linear factors over $\mathbb{E}$. Then by the first case of the corollary, $c_{\widetilde{\mathcal{T}}}(\widetilde{\mathcal{T}}) = 0$, i.e., $c_A(A) = 0$, i.e., $c_{\mathcal{T}}(\mathcal{T}) = 0$. (Expressed differently, A is similar, as a matrix with entries in $\mathbb{E}$, to a matrix B for which $c_B(B) = 0$. If $A = PBP^{-1}$, then for any polynomial $f(x)$, $f(A) = Pf(B)P^{-1}$. Also, since A and B are similar, $c_A(x) = c_B(x)$. Thus $c_A(A) = c_B(A) = Pc_B(B)P^{-1} = P0P^{-1} = 0$.) □

REMARK 4.2.8. For the reader familiar with tensor products, we observe that the second case of the corollary can be simplified to:

Consider $\widetilde{\mathcal{T}} = \mathcal{T} \otimes 1 : V \otimes_{\mathbb{F}} \mathbb{E} \to V \otimes_{\mathbb{F}} \mathbb{E}$. Then $c_{\mathcal{T}}(x) = c_{\widetilde{\mathcal{T}}}(x)$ and $c_{\widetilde{\mathcal{T}}}(\widetilde{\mathcal{T}}) = 0$ by the lemma, so $c_{\mathcal{T}}(\mathcal{T}) = 0$. ◇

REMARK 4.2.9. If $\mathbb{F}$ is algebraically closed (e.g., $\mathbb{F} = \mathbb{C}$, which is algebraically closed by the Fundamental Theorem of Algebra) then $c_{\mathcal{T}}(x)$ automatically splits into a product of linear factors, and we are in the first case of the Cayley-Hamilton theorem, and we are done—fine. If not, although our proof is correct, it is the "wrong" proof. We should not have to pass to a larger field $\mathbb{E}$ in order to investigate linear transformations over $\mathbb{F}$. We shall present a "right" proof later, where we will see how to generalize both Lemma 4.2.5 and Lemma 4.2.6 (see Theorem 5.3.1 and Corollary 5.3.4). $\diamond$

4.3 DIAGONALIZABILITY

Before we continue with our analysis of general linear transformations, we consider a particular but very useful case.

DEFINITION 4.3.1. (1) Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. Then $\mathcal{T}$ is *diagonalizable* if V has a basis $\mathcal{B}$ with $[\mathcal{T}]_{\mathcal{B}}$ a diagonal matrix.

(2) An n-by-n matrix A is *diagonalizable* if $\mathcal{T}_A : \mathbb{F}^n \to \mathbb{F}^n$ is diagonalizable. $\diamond$

REMARK 4.3.2. In light of Theorem 2.3.14, we may phrase (2) more simply as: A is diagonalizable if it is similar to a diagonal matrix. $\diamond$

Lemma 4.3.3. *Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. Then $\mathcal{T}$ is diagonalizable if and only if V has a basis $\mathcal{B}$ consisting of eigenvectors of $\mathcal{T}$.*

Proof. Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ and let $D = [\mathcal{T}]_{\mathcal{B}}$ be a diagonal matrix with diagonal entries $\mu_1, \ldots, \mu_n$. For each i,

$$\left[\mathcal{T}(v_i)\right]_{\mathcal{B}} = [\mathcal{T}]_{\mathcal{B}}\left[v_i\right]_{\mathcal{B}} = D\, e_i = \mu_i e_i = \mu_i \left[v_i\right]_{\mathcal{B}},$$

so $\mathcal{T}(v_i) = \mu_i v_i$ and v_i is an eigenvector.

Conversely, if $\mathcal{B} = \{v_1, \ldots, v_n\}$ is a basis of eigenvectors, so $\mathcal{T}(v_i) = \mu_i v_i$ for each i, then

$$\begin{aligned}[\mathcal{T}]_{\mathcal{B}} &= \left[\left[\mathcal{T}(v_1)\right]_{\mathcal{B}} \mid \left[\,T(v_2)\right]_{\mathcal{B}} \mid \cdots\right] \\ &= \left[\left[\mu_1 v_1\right]_{\mathcal{B}} \mid \left[\mu_2 v_2\right]_{\mathcal{B}} \mid \cdots\right] = \left[\mu_1 e_1 \mid \mu_2 e_2 \mid \cdots\right] = D\end{aligned}$$

is a diagonal matrix. $\square$

Theorem 4.3.4. *Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. If $c_{\mathcal{T}}(x)$ does not split into a product of linear factors, then $\mathcal{T}$ is not diagonalizable. If $c_{\mathcal{T}}(x)$ does split into a product of linear factors (which is always the case if $\mathbb{F}$ is algebraically closed) then the following are equivalent:*

(1) $\mathcal{T}$ is diagonalizable.

(2) $m_{\mathcal{T}}(x)$ splits into a product of distinct linear factors.

(3) For every eigenvalue λ of $\mathcal{T}$, $E_\lambda = E_\lambda^\infty$ (i.e., every generalized eigenvector of $\mathcal{T}$ is an eigenvector of $\mathcal{T}$).

(4) For every eigenvalue λ of $\mathcal{T}$, geom-mult(λ) = alg-mult(λ).

(5) The sum of the geometric multiplicities of the eigenvalues is equal to the dimension of V.

(6) If $\lambda_1, \dots, \lambda_m$ are the distinct eigenvalues of $\mathcal{T}$, then

$$V = E_{\lambda_1} \oplus \cdots \ominus E_{\lambda_m}.$$

Proof. We prove the contrapositive of the first claim: Suppose $\mathcal{T}$ is diagonalizable and let $\mathcal{B}$ be a basis of V with $D = [\mathcal{T}]_{\mathcal{B}}$ a diagonal matrix with diagonal entries $\mu_1, \dots, \mu_n$. Then $c_{\mathcal{T}}(x) = c_D(x) = \det(xI - D) = (x - \mu_1) \cdots (x - \mu_n)$.

Suppose $c_{\mathcal{T}}(x) = (x - \mu_1) \cdots (x - \mu_n)$. The scalars $\mu_1, \dots, \mu_n$ may not all be distinct, so we group them. Let the distinct eigenvalues be $\lambda_1, \dots, \lambda_m$ so $c_{\mathcal{T}}(x) = (x - \lambda_1)^{e_1} \cdots (x - \lambda_m)^{e_m}$ for positive integers $e_1, \dots, e_m$.

Let $n = \dim(V)$. Visibly, e_i is the algebraic multiplicity of λ_i, and $e_1 + \cdots + e_m = n$. Let f_i be the geometric multiplicity of λ_i. Then we know by Lemma 4.1.15 that $1 \le f_i \le e_i$, so $f_1 + \cdots + f_m = n$ if and only if $f_i = e_i$ for each i, so (4) and (5) are equivalent. We know by Lemma 4.2.4 that $e_i = \dim E_{\lambda_i}^\infty$, and by definition $f_i = \dim E_{\lambda_i}$, and $E_{\lambda_i} \subseteq E_{\lambda_i}^\infty$, so (3) and (4) are equivalent.

By Lemma 4.2.5, $V = E_{\lambda_1}^\infty \oplus \cdots \oplus E_{\lambda_k}^\infty$, so $V = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_k}$ if and only if $E_{\lambda_1} = E_{\lambda_1}^\infty$ for each i, so (3) and (6) are equivalent.

If $V = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_m}$, let $\mathcal{B}_i$ be a basis for E_{λ_i} and let $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_m$. Let $\mathcal{T}_i$ be the restriction of $\mathcal{T}$ to E_{λ_i}. Then $\mathcal{B}$ is a basis for V and

$$[\mathcal{T}]_{\mathcal{B}} = \begin{bmatrix} A_1 & & \\ & \ddots & \\ & & A_m \end{bmatrix} = A,$$

a block diagonal matrix with $A_i = [\mathcal{T}_i]_{\mathcal{B}_i}$. But in this case A_i is the e_i-by-e_i matrix $\lambda_i I$ (a scalar multiple of the identity matrix) so (6) implies (1).

If there is an eigenvalue λ_i of $\mathcal{T}$ for which $E_{\lambda_i} \subset E^{\infty}_{\lambda_i}$, let $v_i \in E^{\infty}_{\lambda_i}$ be a generalized eigenvector of index $k > 1$, so $(\mathcal{T} - \lambda_i \mathcal{I})^k(v_i) = 0$ but $(\mathcal{T} - \lambda_i \mathcal{I})^{k-1}(v_i) \neq 0$. For any polynomial $p(x)$ with $p(\lambda_i) \neq 0$, $p(\mathcal{T})(v_i)$ is another generalized eigenvector of the same index k. This implies that any polynomial $f(x)$ with $f(\mathcal{T})(v_i) = 0$, and in particular $m_{\mathcal{T}}(x)$, has a factor of $(x - \lambda_i)^k$. Thus not-(3) implies not-(2), or (2) implies (3).

Finally, let $\mathcal{T}$ be diagonalizable, $[\mathcal{T}]_{\mathcal{B}} = D$ in some basis $\mathcal{B}$, where D is a diagonal matrix with entries $\mu_1, \ldots, \mu_m$, and with distinct diagonal entries λ_1 repeated e_1 times, λ_2 repeated e_2 times, etc. We may reorder $\mathcal{B}$ so that

$$[\mathcal{T}]_{\mathcal{B}} = \begin{bmatrix} A_1 & & \\ & \ddots & \\ & & A_m \end{bmatrix} = A$$

with A_i the e_i-by-e_i matrix $\lambda_i I$. Then $A_i - \lambda_i I$ is the zero matrix, and an easy computation shows $(A - \lambda_1 I) \cdots (A - \lambda_m I) = 0$, so $m_{\mathcal{T}}(x)$ divides, and is easily seen to be equal to, $(x - \lambda_1) \cdots (x - \lambda_m)$, and (1) implies (2). $\square$

Corollary 4.3.5. *Let V be a finite-dimensional vector space and $\mathcal{T} : V \to V$ a linear transformation. Suppose that $c_{\mathcal{T}}(x) = (x - \lambda_1) \cdots (x - \lambda_n)$ is a product of distinct linear factors. Then $\mathcal{T}$ is diagonalizable.*

Proof. By Corollary 4.1.16, alg-mult$(\lambda_i) = 1$ implies geom-mult$(\lambda_i) = 1$ as well. $\square$

4.4 An application to differential equations

Let us look at a familiar situation, the solution of linear differential equations, and see how the ideas of linear algebra clarify what is going on. Since we are interested in the linear-algebraic aspects of the situation rather than the analytical ones, we will not try to make minimal differentiability assumptions, but rather make the most convenient ones.

We let V be the vector space of C^{∞} complex-valued functions on the real line $\mathbb{R}$. We let $\mathcal{L}$ be an nth order linear differential operator $\mathcal{L} = a_n(x)\mathbf{D}^n + \cdots + a_1(x)\mathbf{D} + a_0(x)$, where the $a_i(x)$ are functions in V and $\mathbf{D}$ denotes differentiation: $\mathbf{D}(f(x)) = f'(x)$ and $\mathbf{D}^k(f(x)) = f^{(k)}(x)$, the kth derivative. We further assume that $a_n(x) \neq 0$ for all $x \in \mathbb{R}$.

Theorem 4.4.1. *Let $\mathcal{L}$ be as above. Then* $\operatorname{Ker}(\mathcal{L})$ *is an n-dimensional subspace of V. For any $b(x) \in V$, $\{y \in V \mid \mathcal{L}(y) = b(x)\}$ is an affine subspace of V parallel to* $\operatorname{Ker}(\mathcal{L})$.

Proof. As the kernel of a linear transformation, $\operatorname{Ker}(\mathcal{L})$ is a subspace of V.

$\operatorname{Ker}(\mathcal{L}) = \{y \in V \mid \mathcal{L}(y) = 0\}$ is just the solution space of the linear differential equation $\mathcal{L}(y) = a_n(x)y^{(n)} + \cdots + a_1(x)y' + a_0(x)y = 0$. For $x_0 \in \mathbb{R}$ define a linear transformation $\mathcal{E} : \operatorname{Ker}(\mathcal{L}) \to \mathbb{C}^n$ by

$$\mathcal{E}(y) = \begin{bmatrix} y(x_0) \\ y'(x_0) \\ \vdots \\ y^{(n-1)}(x_0) \end{bmatrix}.$$

The fundamental existence and uniqueness theorem for linear differential equations tells us that $\mathcal{E}$ is onto (that's existence—there is a solution for any set of initial conditions) and that it is 1-1 (that's uniqueness), so $\mathcal{E}$ is an isomorphism and $\operatorname{Ker}(\mathcal{L})$ is n-dimensional. For any $b(x) \in V$ this theorem tells us that $\mathcal{L}(y) = b(x)$ has a solution, so now, by Theorem 1.5.7, the set of all solutions is an affine subspace parallel to $\operatorname{Ker}(\mathcal{L})$. □

Now we wish to solve $\mathcal{L}(y) = 0$ or $\mathcal{L}(y) = b(x)$.

To solve $\mathcal{L}(y) = 0$, we find a basis of $\operatorname{Ker}(\mathcal{L})$. Since we know $\operatorname{Ker}(\mathcal{L})$ is n-dimensional, we simply need to find n linearly independent functions $\{y_1(x), \dots, y_n(x)\}$ in $\operatorname{Ker}(\mathcal{L})$ and the general solution of $\mathcal{L}(y) = 0$ will be $y = c_1y_1(x) + \cdots + c_ny_n(x)$. Then, by Proposition1.5.6, in order to solve the inhomogeneous equation $\mathcal{L}(y) = b(x)$, we simply need to find a single solution, i.e., a single function $y_0(x)$ with $\mathcal{L}(y_0(x)) = b(x)$, and then the general solution of $\mathcal{L}(y) = b(x)$ will be $y = y_0(x) + c_1y_1(x) + \cdots + c_ny_n(x)$.

We now turn to the constant coefficient case, where we can find explicit solutions. That is, we assume $a_n, \dots, a_0$ are constants.

First let us see that a familiar property of differentiation is a consequence of a fact from linear algebra.

Theorem 4.4.2. *Let V be a (necessarily infinite-dimensional) vector space and let $\mathcal{T} : V \to V$ be a linear transformation such that $\mathcal{T}$ is onto and* $\operatorname{Ker}(\mathcal{T})$ *is* 1*-dimensional. Then for any positive integer k,* $\operatorname{Ker}(\mathcal{T}^k)$ *is k-dimensional and is the subspace $\{p(\mathcal{T})(v_k) \mid p(x)$ an arbitrary polynomial$\}$ for a single generalized eigenvector v_k of index k, (necessarily associated to the eigenvalue* 0*).*

Proof. We proceed by induction on k. By hypothesis the theorem is true for $k = 1$. Suppose it is true for k and consider $\mathcal{T}^{k+1}$. By hypothesis, there is a vector v_{k+1} with $\mathcal{T}(v_{k+1}) = v_k$, and v_{k+1} is then a generalized eigenvector of index $k+1$. The subspace $\{p(\mathcal{T})(v_{k+1}) \mid p(x) \text{ a polynomial}\}$ is a subspace of $\mathrm{Ker}(\mathcal{T}^{k+1})$ of dimension $k+1$. We must show this subspace is all of $\mathrm{Ker}(\mathcal{T}^{k+1})$. Let $w \in \mathrm{Ker}(\mathcal{T}^{k+1})$, so $\mathcal{T}^{k+1}(w) = \mathcal{T}^k(\mathcal{T}(w)) = 0$. By the inductive hypothesis, we can write $\mathcal{T}(w) = p(\mathcal{T})(v_k)$ for some polynomial $p(x)$. If we let $w_0 = p(\mathcal{T})(v_{k+1})$, then

$$\mathcal{T}(w_0) = \mathcal{T}p(\mathcal{T})(v_{k+1}) = p(\mathcal{T})\mathcal{T}(v_{k+1}) = p(\mathcal{T})(v_k) = \mathcal{T}(w).$$

Hence $w - w_0 \in \mathrm{Ker}(\mathcal{T})$, so $w = w_0 + av_1$ where $v_1 = \mathcal{T}^{k-1}(v_k) = \mathcal{T}^k(v_{k+1})$, i.e., $w = (p(\mathcal{T}) + a\mathcal{T}^k)(v_{k+1}) = q(\mathcal{T})(v_{k+1})$ where $q(x) = p(x) + ax^k$, and we are done. $\square$

Lemma 4.4.3. *(1)* $\mathrm{Ker}(\mathbf{D}^k)$ *has basis* $\{1, x, \ldots, x^{k-1}\}$.

(2) More generally, for any a, $\mathrm{Ker}(\mathbf{D} - a)^k$ *has basis* $\{e^{ax}, xe^{ax}, \ldots, x^{k-1}e^{ax}\}$.

Proof. We can easily verify that

$$(\mathbf{D} - a)^k(x^{k-1}e^{ax}) = 0 \quad \text{but} \quad (\mathbf{D} - a)^{k-1}(x^{k-1}e^{ax}) \neq 0$$

(and it is trivial to verify that $\mathbf{D}^k(x^{k-1}) = 0$ but $\mathbf{D}^{k-1}(x^{k-1}) \neq 0$). Thus $\mathcal{B} = \{e^{ax}, xe^{ax}, \ldots, x^{k-1}e^{ax}\}$ is a set of generalized eigenvectors of indices $1, 2, \ldots, k$ associated to the eigenvalue a. Hence $\mathcal{B}$ is linearly independent. We know from Theorem 4.4.1 that $\mathrm{Ker}((\mathbf{D} - a)^k)$ has dimension k, so $\mathcal{B}$ forms a basis.

Alternatively, we can use Theorem 4.4.2. We know $\mathrm{Ker}(\mathbf{D})$ consists precisely of the constant functions, so it is 1-dimensional with basis $\{1\}$. Furthermore, $\mathbf{D}$ is onto by the Fundamental Theorem of Calculus: If $F(x) = \int_{x_0}^{x} f(t)dt$, then $\mathbf{D}(F(x)) = f(x)$.

For $\mathbf{D} - a$ the situation is only a little more complicated. We can easily find that $\mathrm{Ker}(\mathbf{D} - a) = \{ce^{ax}\}$, a 1-dimensional space with basis $\{e^{ax}\}$. If we let

$$F(x) = e^{ax}\int_{x_0}^{x} e^{-at} f(t)\, dt,$$

the product rule and the Fundamental Theorem of Calculus show that

$$(\mathbf{D} - a)(F(x)) = f(x).$$

With notation as in the proof of Theorem 4.4.2, if we let $v_1 = e^{ax}$ and solve for $v_2, v_3, \ldots$, recursively, we obtain a basis of $\mathrm{Ker}(\mathbf{D} - a)$

$$\{e^{ax}, xe^{ax}, (x^2/2)e^{ax}, \ldots, (x^{k-1}/(k-1)!)e^{ax}\}$$

(or $\{1, x, x^2/2, \ldots, x^{k-1}/(k-1)!\}$ if $a = 0$) and since we can replace any basis element by a multiple of itself and still have a basis, we are done. $\square$

Theorem 4.4.4. *Let $\mathcal{L}$ be a constant coefficient differential operator with factorization*

$$\mathcal{L} = a_n(\mathbf{D} - \lambda_1)^{e_1} \cdots (\mathbf{D} - \lambda_m)^{e_m}$$

where $\lambda_1, \ldots, \lambda_m$ are distinct. Then

$$\{e^{\lambda_1 x}, \ldots, x^{e_1-1}e^{\lambda_1 x}, \ldots, e^{\lambda_m x}, \ldots, x^{e_m-1}\lambda_m x\}$$

is a basis for $\mathrm{Ker}(\mathcal{L})$, *so that the general solution of $\mathcal{L}(y) = 0$ is*

$$\begin{aligned} y = {} & c_{1,1}e^{\lambda_1 x} + \cdots + c_{1,e_1}x^{e_1-1}e^{\lambda_1 x} + \cdots \\ & + c_{m,1}e^{\lambda_m x} + \cdots + c_{m,e_m}x^{e_m-1}e^{\lambda_m x}. \end{aligned}$$

If $b(x) \in V$ is arbitrary, let $y_0 = y_0(x)$ be an element of V with $\mathcal{L}(y_0(x)) = b(x)$. (Such an element $y_0(x)$ always exists.) Then the general solution of $\mathcal{L}(y) = b(x)$ is

$$\begin{aligned} y = {} & y_0 + c_{1,1}e^{\lambda_1 x} + \cdots + c_{1,e_1}x^{e_1-1}e^{\lambda_1 x} + \cdots \\ & + c_{m,1}e^{\lambda_m x} + \cdots + c_{m,e_m}x^{e_m-1}e^{\lambda_m x}. \end{aligned}$$

Proof. We know that the set of generalized eigenspaces corresponding to distinct eigenvalues are linearly independent (this follows directly from the proof of Lemma 4.2.5, which does not require V to be finite dimensional) and then within each eigenspace a set of generalized eigenvectors with distinct indices is linearly independent as well, so this entire set of generalized eigenvectors is linearly independent. Since there are n of them, they form a basis for $\mathrm{Ker}(\mathcal{L})$. The inhomogeneous case then follows immediately from Proposition1.5.6. $\square$

REMARK 4.4.5. Suppose $\mathcal{L}$ has real coefficients and we want to solve $\mathcal{L}(y) = 0$ in real functions. We proceed as above to obtain the general solution, and look for conditions on the c's for the solution to be real. Since $a_n x^n + \cdots + a_0$ is a real polynomial, if the complex number λ is a root of it, so is its conjugate $\overline{\lambda}$, and then to obtain a real solution of $\mathcal{L}(y) = 0$

the coefficient of $e^{\overline{\lambda}x}$ must be the complex conjugate of the coefficient of $e^{\lambda x}$, etc. Thus in our expression for y there is a pair of terms $ce^{\lambda x} + \overline{c}e^{\overline{\lambda}x}$. Writing $c = c_1 + ic_2$ and $\lambda = a + bi$,

$$\begin{aligned} ce^{\lambda x} + \overline{c}e^{\overline{\lambda}x} &= \big(c_1 + ic_2\big)\big(e^{ax}\big(\cos(bx) + i\,\sin(bx)\big)\big) \\ &\quad + \big(c_1 - ic_2\big)\big(e^{ax}\big(\cos(bx) - i\,\sin(bx)\big)\big) \\ &= d_1 e^{ax}\cos(bx) + d_2 e^{ax}\sin(bx) \end{aligned}$$

for real numbers d_1 and d_2. That is, we can perform a change of basis and instead of using the basis given in Theorem 4.4.4, replace each pair of basis elements $\{e^{\lambda x}, e^{\overline{\lambda}x}\}$ by the pair of basis elements $\{e^{ax}\cos(bx), e^{ax}\sin(bx)\}$, etc., and express our solution in terms of this new basis. $\diamond$

CHAPTER 5

The structure of a linear transformation II

In this chapter we conclude our analysis of the structure of a linear transformation $\mathcal{T} : V \to V$. We derive our deepest structural results, the rational canonical form of $\mathcal{T}$ and, when V is a vector space over an algebraically closed field $\mathbb{F}$, the Jordan canonical form of $\mathcal{T}$.

Recall our metaphor of coordinates as giving a language in which to describe linear transformations. A basis $\mathcal{B}$ of V in which $[\mathcal{T}]_{\mathcal{B}}$ is in canonical form is a "right" language to describe the linear transformation $\mathcal{T}$. This is especially true for the Jordan canonical form, which is intimately related to eigenvalues, eigenvectors, and generalized eigenvectors.

The importance of the Jordan canonical form of $\mathcal{T}$ cannot be overemphasized. *Every* structural fact about a linear transformation is encoded in its Jordan canonical form.

We not only show the existence of the Jordan canonical form, but also derive an algorithm for finding the Jordan canonical form of $\mathcal{T}$ as well as finding a Jordan basis of V, assuming we can factor the characteristic polynomial $c_{\mathcal{T}}(x)$. (Of course, there is no algorithm for factoring polynomials, as we know from Galois theory.)

We have arranged our exposition in what we think is the clearest way, getting to the simplest (but still important) results as quickly as possible in the preceding chapter, and saving the deepest results for this chapter. However, this is not the logically most economical way. (That would have been to prove the most general and deepest structure theorems first, and to obtain the simpler results as corollaries.) This means that our approach involves a certain amount of repetition. For example, although we defined the characteristic and minimum polynomials of a linear transformation in the last chapter, we will be redefining them here, when we consider them more deeply. But we want to remark that this repetition is a deliberate choice arising from the order in which we have decided to present the material.

While our ultimate goal in this chapter is the Jordan canonical form, our path to it goes through rational canonical form. There are several reasons for this: First, rational canonical form always exists, while in order to obtain the Jordan canonical form for an arbitrary linear transformation we must be working over an algebraically closed field. (There is a generalization of Jordan canonical form that exists over an arbitrary field, and we will briefly mention it though not treat it in depth.) Second, rational canonical form is important in itself, and, as we shall see, has a number of applications. Third, the natural way to prove the existence of the Jordan canonical form of $\mathcal{T}$ is first to split V up into the direct sum of the generalized eigenspaces of $\mathcal{T}$ (this being the easy step), and then to analyze each generalized eigenspace (this being where the hard work comes in), and for a linear transformation with a single generalized eigenspace, rational and Jordan canonical forms are very closely related.

Here is how our argument proceeds. In Section 5.1 we introduce the minimum and characteristic polynomials of a linear transformation $\mathcal{T} : V \longrightarrow V$, and in particular we derive Theorem 5.1.11, which is both very useful and important in its own right. In Section 5.2 we consider $\mathcal{T}$-invariant subspaces W of V and the map $\overline{\mathcal{T}}$ induced by $\mathcal{T}$ on the quotient space V/W. In Section 5.3 we prove Theorem 5.3.1, giving the relationship between the minimum and characteristic polynomials of $\mathcal{T}$, and as a corollary derive the Cayley-Hamilton Theorem. (It is often thought that this theorem is a consequence of Jordan canonical form, but, as you will see, it is actually prior to Jordan canonical form.) In Section 5.4 we return to invariant subspaces, and prove the key technical results Theorem 5.4.6 and Theorem 5.4.10, which tell us when $\mathcal{T}$-invariant subspaces have $\mathcal{T}$-invariant complements. Using this work, we quickly derive rational canonical form in Section 5.5, and then we use rational canonical form to quickly derive Jordan canonical form in Section 5.6. Because of the importance and utility of this result, in Section 5.7 we give a well-illustrated algorithm for finding the Jordan canonical form of $\mathcal{T}$, and a Jordan basis of V, providing we can factor the characteristic polynomial of $\mathcal{T}$. In the last two sections of this chapter, Section 5.8 and Section 5.9, we apply our results to derive additional structural information on linear transformations.

5.1 ANNIHILATING, MINIMUM, AND CHARACTERISTIC POLYNOMIALS

Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. In this section we introduce three sorts of polynomials associated to $\mathcal{T}$: First, for any nonzero vector $v \in V$, we have its $\mathcal{T}$-annihilator $m_{\mathcal{T},v}(x)$. Then we have the minimum polynomial of $\mathcal{T}$, $m_{\mathcal{T}}(x)$, and the characteristic polynomial of $\mathcal{T}$, $c_{\mathcal{T}}(x)$. All of these polynomials will play important roles in our development.

Theorem 5.1.1. *Let V be a vector space of dimension n and let $v \in V$ be a vector, $v \neq 0$. Then there is a unique monic polynomial $m_{\mathcal{T},v}(x)$ of lowest degree with $m_{\mathcal{T},v}(\mathcal{T})(v) = 0$. This polynomial has degree at most n.*

Proof. Consider the vectors $\{v, \mathcal{T}(v), \dots, \mathcal{T}^n(v)\}$. This is a set of $n+1$ vectors in an n-dimensional vector space and so is linearly dependent, i.e., there are $a_0, \dots, a_n$ not all zero such that $a_0 v + a_1\mathcal{T}(v) + \cdots + a_n\mathcal{T}^n(v) = 0$. Thus if $p(x) = a_n x^n + \cdots + a_0$, $p(x)$ is a nonzero polynomial with $p(\mathcal{T})(v) = 0$. Now $\mathcal{J} = \{f(x) \in \mathbb{F}[x] \mid f(\mathcal{T})(v) = 0\}$ is a nonzero ideal in $\mathbb{F}[x]$ (if $f(\mathcal{T})(v) = 0$ and $g(\mathcal{T})(v) = 0$, then $(f+g)(\mathcal{T})(v) = 0$ and if $f(\mathcal{T})(v) = 0$ then $(cf)(\mathcal{T})(v) = 0$, and $p(x) \in \mathcal{J}$, so $\mathcal{J}$ is a nonzero ideal.) Hence by Lemma A.1.8 there is a unique monic polynomial $m_{\mathcal{T},v}(x)$ of lowest degree in $\mathcal{J}$. □

DEFINITION 5.1.2. The polynomial $m_{\mathcal{T},v}(x)$ is called the $\mathcal{T}$*-annihilator* of the vector v. ◇

EXAMPLE 5.1.3. Let V have basis $\{v_1, \dots, v_n\}$ and define $\mathcal{T}$ by $\mathcal{T}(v_1) = 0$ and $\mathcal{T}(v_i) = v_{i-1}$ for $i > 1$. Then $m_{\mathcal{T},v_k}(x) = x^k$ for $k = 1, \dots, n$. This shows that $m_{\mathcal{T},v}(x)$ can have any degree between 1 and n. ◇

EXAMPLE 5.1.4. Let $V = {}^r\mathbb{F}^\infty$ and let $\mathbf{L} : V \to V$ be left shift. Consider $v \in V$, $v \neq 0$. For some k, v is of the form $(a_1, a_2, \dots, a_k, 0, 0, \dots)$ with $a_k \neq 0$, and then $m_{\mathcal{T},v}(x) = x^k$. If $\mathbf{R} : V \to V$ is right shift, then for any vector $v \neq 0$, the set $\{v, \mathbf{R}(v), \mathbf{R}^2(v), \dots\}$ is linearly independent and so there is no nonzero polynomial $p(x)$ with $p(\mathcal{T})(v) = 0$. ◇

Theorem 5.1.5. *Let V be a vector space of dimension n. Then there is a unique monic polynomial $m_{\mathcal{T}}(x)$ of lowest degree with $m_{\mathcal{T}}(\mathcal{T})(v) = 0$ for every $v \in V$. This polynomial has degree at most n^2.*

Proof. Choose a basis $\mathcal{B} = \{v_1, \dots, v_n\}$ of V. For each $v_k \in B$ we have its $\mathcal{T}$-annihilator $p_k(x) = m_{\mathcal{T},v_k}(x)$. Let $q(x)$ be the least common multiple of $p_1(x), \dots, p_n(x)$. Since $p_k(x)$ divides $q(x)$ for each k, $q(\mathcal{T})(v_k) = 0$. Hence $q(\mathcal{T})(v) = 0$ for every $v \in V$ by Lemma 1.2.23. If $r(x)$ is any polynomial with $r(x)$ not divisible by $p_k(x)$ for some k, then for that value of k we have $r(\mathcal{T})(v_k) \neq 0$. Thus $m_{\mathcal{T}}(x) = q(x)$ is the desired polynomial. $m_{\mathcal{T}}(x)$ divides the product $p_1(x)p_2(x)\cdots p_n(x)$, of degree n^2, so $m_{\mathcal{T}}(x)$ has degree at most n^2. □

DEFINITION 5.1.6. The polynomial $m_{\mathcal{T}}(x)$ is the *minimum polynomial* of $\mathcal{T}$. ◇

REMARK 5.1.7. As we will see in Corollary 5.1.12, $m_{\mathcal{T}}(x)$ has degree at most n. ◇

EXAMPLE 5.1.8. Let V be n-dimensional with basis $\{v_1, \dots, v_n\}$ and for any fixed value of k between 1 and n, define $\mathcal{T} : V \to V$ by $\mathcal{T}(v_1) = 0$, $\mathcal{T}(v_i) = v_{i-1}$ for $2 \leq i \leq k$, $\mathcal{T}(v_i) = 0$ for $i > k$. Then $m_{\mathcal{T}}(x) = x^k$. This shows that $m_{\mathcal{T}}(x)$ can have any degree between 1 and n (compare Example 5.1.3). ◇

EXAMPLE 5.1.9. Returning to Example 5.1.4, we see that if $\mathcal{T} = \mathbf{R}$, given any nonzero vector $v \in V$ there is no nonzero polynomial $f(x)$ with $f(\mathcal{T})(v) = 0$, so there is certainly no nonzero polynomial $f(x)$ with $f(\mathcal{T}) = 0$. Thus $\mathcal{T}$ does not have a minimum polynomial. If $\mathcal{T} = \mathbf{L}$, then $m_{\mathcal{T},v}(x)$ exists for any nonzero vector $v \in V$, i.e., for every nonzero vector $v \in V$ there is a polynomial $f_x(x)$ with $f_v(\mathcal{T})(v) = 0$. But there is no single polynomial $f(x)$ with $f(\mathcal{T})(v) = 0$ for every $v \in V$, so again $\mathcal{T}$ does not have a minimum polynomial. (Such a polynomial would have to be divisible by x^k for every positive integer k.) Let $\mathcal{T} : V \to V$ be defined by $\mathcal{T}(a_1, a_2, a_3, a_4, \dots) = (-a_1, a_2, -a_3, a_4, \dots)$. If $v_0 = (a_1, a_2, \dots)$ with $a_i = 0$ whenever i is odd, then $\mathcal{T}(v_0) = v_0$ so $m_{\mathcal{T},v_0}(x) = x - 1$. If $v_1 = (a_1, a_2, \dots)$ with $a_i = 0$ whenever i is even, then $\mathcal{T}(v_1) = -v_1$ so $m_{\mathcal{T},v_1}(x) = x + 1$. If v is not of one of these two special forms, then $m_{\mathcal{T},v}(x) = x^2 - 1$. Thus $\mathcal{T}$ has a minimum polynomial, namely $m_{\mathcal{T}}(x) = x^2 - 1$. ◇

Lemma 5.1.10. *Let V be a vector space and let $\mathcal{T} : V \to V$ be a linear transformation. Let $v_1, \dots, v_k \in V$ with $\mathcal{T}$-annihilators $p_i(x) = m_{\mathcal{T},v_i}(x)$ for $i = 1, \dots, k$ and suppose that $p_1(x), \dots, p_k(x)$ are pairwise relatively prime. Let $v = v_1 + \cdots + v_k$ have $\mathcal{T}$-annihilator $p(x) = m_{\mathcal{T},v}(x)$. Then $p(x) = p_1(x)\cdots p_k(x)$.*

Proof. We proceed by induction on k. The case $k = 1$ is trivial. We do the crucial case $k = 2$, and leave $k > 2$ to the reader.

Let $v = v_1 + v_2$ where $p_1(\mathcal{T})(v_1) = p_2(\mathcal{T})(v_2) = 0$ with $p_1(x)$ and $p_2(x)$ relatively prime. Then there are polynomials $q_1(x)$ and $q_2(x)$ with $p_1(x)q_1(x) + p_2(x)q_2(x) = 1$, so

$$\begin{aligned} v = \mathcal{I}v &= \big(p_1(\mathcal{T})q_1(\mathcal{T}) + p_2(\mathcal{T})q_2(\mathcal{T})\big)\big(v_1 + v_2\big) \\ &= p_2(\mathcal{T})q_2(\mathcal{T})\big(v_1\big) + p_1(\mathcal{T})q_1(\mathcal{T})\big(v_2\big) \\ &= w_1 + w_2. \end{aligned}$$

Now

$$\begin{aligned} p_1(\mathcal{T})\big(w_1\big) &= p_1(\mathcal{T})\big(p_2(\mathcal{T})q_2(\mathcal{T})\big(v_1\big)\big) \\ &= \big(p_2(\mathcal{T})q_2(\mathcal{T})\big)\big(p_1(\mathcal{T})\big(v_1\big)\big) = 0, \end{aligned}$$

so $w_1 \in \operatorname{Ker}(p_1(\mathcal{T}))$ and similarly $w_2 \in \operatorname{Ker}(p_2(\mathcal{T}))$.

Let $r(x)$ be any polynomial with $r(\mathcal{T})(v) = 0$.

Now $v = w_1 + w_2$ so $p_2(\mathcal{T})(v) = p_2(\mathcal{T})(w_1 + w_2) = p_2(\mathcal{T})(w_1)$, so $0 = r(\mathcal{T})(v)$ gives $0 = r(\mathcal{T})p_2(\mathcal{T})q_2(\mathcal{T})(w_1)$. Also, $p_1(\mathcal{T})(w_1) = 0$ so we certainly have $0 = r(\mathcal{T})p_1(\mathcal{T})q_1(\mathcal{T})(w_1)$. Hence

$$\begin{aligned} 0 &= r(\mathcal{T})\big(p_1(\mathcal{T})q_1(\mathcal{T}) + p_2(\mathcal{T})q_2(\mathcal{T})\big)\big(w_1\big) \\ &= r(\mathcal{T})\big(\mathcal{I}\big)\big(w_1\big) \\ &= r(\mathcal{T})\big(w_1\big) \end{aligned}$$

(as $p_1(x)q_1(x) + p_2(x)q_2(x) = 1$), and similarly $0 = r(\mathcal{T})(w_2)$.

Now

$$r(\mathcal{T})(w_1) = r(\mathcal{T})(p_2(\mathcal{T})q_2(\mathcal{T}))(v_1).$$

But $p_1(x)$ is the $\mathcal{T}$-annihilator of v_1, so by definition $p_1(x)$ divides $r_1(x)(p_2(x)q_2(x))$. From $1 = p_1(x)q_1(x) + p_2(x)q_2(x)$ we see that $p_1(x)$ and $p_2(x)q_2(x)$ are relatively prime, so by Lemma A.1.21, $p_1(x)$ divides $r(x)$. Similarly, considering $r(\mathcal{T})(w_2)$, we see that $p_2(x)$ divides $r(x)$. By hypothesis $p_1(x)$ and $p_2(x)$ are relatively prime, so by Corollary A.1.22, $p_1(x)p_2(x)$ divides $r(x)$.

On the other hand, clearly

$$(p_1(\mathcal{T})p_2(\mathcal{T}))(v) = (p_1(\mathcal{T})p_2(\mathcal{T}))(v_1 + v_2) = 0.$$

Thus $p_1(x)p_2(x)$ is the $\mathcal{T}$-annihilator of v, as claimed. □

Theorem 5.1.11. *Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. Then there is a vector $v \in V$ such that the $\mathcal{T}$-annihilator $m_{\mathcal{T},v}(x)$ of v is equal to the minimum polynomial $m_{\mathcal{T}}(x)$ of $\mathcal{T}$.*

Proof. Choose a basis $\mathcal{B} = \{v_1, \ldots, v_n\}$ of V. As we have seen in Theorem 5.1.5, the minimum polynomial $m_{\mathcal{T}}(x)$ is the least common multiple of the $\mathcal{T}$-annihilators $m_{\mathcal{T},v_1}(x), \ldots, m_{\mathcal{T},v_n}(x)$. Factor $m_{\mathcal{T}}(x) = p_1(x)^{f_1} \cdots p_k(x)^{f_k}$ where $p_1(x), \ldots, p_k(x)$ are distinct irreducible polynomials, and hence $p_1(x)^{f_1}, \ldots, p_k(x)^{f_k}$ are pairwise relatively prime polynomials. For each i between 1 and k, $p_i(x)^{f_i}$ must appear as a factor of $m_{\mathcal{T},v_j}(x)$ for some j. Write $m_{\mathcal{T},v_j}(x) = p_i(x)^{f_i} q(x)$. Then the vector $u_i = q(\mathcal{T})(v_j)$ has $\mathcal{T}$-annihilator $p_i(x)^{f_i}$. By Lemma 5.1.10, the vector $v = u_1 + \cdots + u_k$ has $\mathcal{T}$-annihilator $p_1(x)^{f_1} \cdots p_k(x)^{f_k} = m_{\mathcal{T}}(x)$. □

Not only is Theorem 5.1.11 interesting in itself, but it plays a *key* role in future developments: We will often pick an element $v \in V$ with $m_{\mathcal{T},v}(x) = m_{\mathcal{T}}(x)$, and proceed from there.

Here is an immediate application of this theorem.

Corollary 5.1.12. *Let $\mathcal{T} : V \to V$ where V is a vector space of dimension n. Then $m_{\mathcal{T}}(x)$ is a polynomial of degree at most n.*

Proof. $m_{\mathcal{T}}(x) = m_{\mathcal{T},v}(x)$ for some $v \in V$. But for any $v \in V$, $m_{\mathcal{T},v}(x)$ has degree at most n. □

We now define a second very important polynomial associated to a linear transformation from a finite-dimensional vector space to itself.

We need a preliminary lemma.

Lemma 5.1.13. *Let A and B be similar matrices. Then* $\det(xI - A) = \det(xI - B)$ *(as polynomials in $\mathbb{F}[x]$).*

Proof. If $B = PAP^{-1}$ then

$$\begin{aligned} xI - B &= x(PIP^{-1}) - (PAP^{-1}) \\ &= P(xI)P^{-1} - PAP^{-1} = P(xI - A)P^{-1}, \end{aligned}$$

so

$$\begin{aligned} \det(xI - B) &= \det(P(xI - A)P^{-1}) = \det(P)\det(xI - A)\det(P^{-1}) \\ &= \det(P)\det(xI - A)\det(P)^{-1} = \det(xI - A). \end{aligned}$$ □

DEFINITION 5.1.14. Let A be a square matrix. The *characteristic polynomial* $c_A(x)$ of A is the polynomial $c_A(x) = \det(xI - A)$. Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. The *characteristic polynomial* $c_{\mathcal{T}}(x)$ is the polynomial defined as follows. Let $\mathcal{B}$ be any basis of V and let A be the matrix $A = [\mathcal{T}]_{\mathcal{B}}$. Then $c_{\mathcal{T}}(x) = \det(xI - A)$. ◇

REMARK 5.1.15. We see from Theorem 2.3.14 and Lemma 5.1.13 that $c_{\mathcal{T}}(x)$ is well defined, i.e., independent of the choice of basis $\mathcal{B}$. ◇

We now introduce a special kind of matrix, whose importance we will see later.

DEFINITION 5.1.16. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a monic polynomial in $\mathbb{F}[x]$ of degree $n \geq 1$. Then the *companion matrix* $C(f(x))$ of $f(x)$ is the n-by-n matrix

$$C\big(f(x)\big) = \begin{bmatrix} -a_{n-1} & 1 & 0 & \cdots & 0 \\ -a_{n-2} & 0 & 1 & \cdots & 0 \\ & & \vdots & \ddots & \\ -a_1 & 0 & 0 & \cdots & 1 \\ -a_0 & 0 & 0 & \cdots & 0 \end{bmatrix}.$$

(The 1's are immediately above the diagonal.) ◇

Theorem 5.1.17. *Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a monic polynomial and let $A = C(f(x))$ be its companion matrix. Let $V = \mathbb{F}^n$ and let $\mathcal{T} = \mathcal{T}_A : V \to V$ be the linear transformation $\mathcal{T}(v) = Av$. Let $v = e_n$ be the nth standard basis vector. Then the subspace W of V defined by $W = \{g(\mathcal{T})(v) \mid g(x) \in \mathbb{F}[x]\}$ is V. Furthermore, $m_{\mathcal{T}}(x) = m_{\mathcal{T},v}(x) = f(x)$.*

Proof. We see that $\mathcal{T}(e_n) = e_{n-1}$, $\mathcal{T}^2(e_n) = \mathcal{T}(e_{n-1}) = e_{n-2}$, and in general $\mathcal{T}^k(e_n) = e_{n-k}$ for $k \leq n-1$. Thus the subspace W of V contains the subspace spanned by $\{\mathcal{T}^{n-1}(v), \ldots, \mathcal{T}(v), v\} = \{e_1, \ldots, e_{n-1}, e_n\}$, which is all of V. We also see that this set is linearly independent, and hence that there is no nonzero polynomial $p(x)$ of degree less than or equal to $n-1$ with $p(\mathcal{T})(v) = 0$. From

$$\begin{aligned}\mathcal{T}^n(v) &= \mathcal{T}(e_1) = -a_{n-1}e_1 - a_{n-2}e_2 \cdots - a_1 e_{n-1} - a_0 e_n \\ &= -a_{n-1}\mathcal{T}^{n-1}(v) - a_{n-2}\mathcal{T}^{n-2}(v) - \cdots - a_1\mathcal{T}(v) - a_0 v\end{aligned}$$

we see that

$$0 = a_n\mathcal{T}^n(v) + \cdots + a_1\mathcal{T}(v) + a_0 v,$$

i.e., $f(\mathcal{T})(v) = 0$. Hence $m_{\mathcal{T},v}(x) = f(x)$.

On the one hand, $m_{\mathcal{T},v}(x)$ divides $m_{\mathcal{T}}(x)$. On the other hand, since every $w \in V$ is $w = g(\mathcal{T})(v)$ for some polynomial $g(x)$,

$$m_{\mathcal{T},v}(\mathcal{T})(w) = m_{\mathcal{T},v}(\mathcal{T})g(\mathcal{T})(v) = g(\mathcal{T})m_{\mathcal{T},v}(\mathcal{T})(v) = g(\mathcal{T})(0) = 0,$$

for every $w \in V$, and so $m_{\mathcal{T}}(x)$ divides $m_{\mathcal{T},v}(x)$. Thus

$$m_{\mathcal{T}}(x) = m_{\mathcal{T},v}(x) = f(x). \qquad \square$$

Lemma 5.1.18. *Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a monic polynomial of degree $n \geq 1$ and let $A = C(f(x))$ be its companion matrix. Then $c_A(x) = \det(xI - A) = f(x)$.*

Proof. We proceed by induction. If $n = 1$ then $A = C(f(x)) = [-a_0]$ so $xI - A = [x + a_0]$ has determinant $x + a_0$.

Assume the theorem is true for $k = n - 1$ and consider $k = n$. We compute the determinant by expansion by minors of the last row

$$\det \begin{bmatrix} x + a_{n-1} & -1 & 0 & \cdots & 0 \\ a_{n-2} & x & -1 & \cdots & 0 \\ \vdots & \vdots & \ddots & & \\ a_1 & 0 & & & -1 \\ a_0 & 0 & \cdots & & x \end{bmatrix}$$

$$= (-1)^{n+1}a_0 \det \begin{bmatrix} -1 & 0 & \cdots & 0 \\ x & -1 & \cdots & 0 \\ 0 & x & \ddots & 0 \\ \vdots & & & \vdots \\ 0 & & x & -1 \end{bmatrix} + x \det \begin{bmatrix} x + a_{n-1} & -1 & 0 & \cdots & 0 \\ a_{n-2} & x & -1 & \cdots & 0 \\ \vdots & & \ddots & & \vdots \\ a_2 & 0 & \cdots & & -1 \\ a_1 & 0 & \cdots & & x \end{bmatrix}$$

$$= (-1)^{n+1}a_0(-1)^{n-1} + x\left(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_2x + a_1\right)$$
$$= x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = f(x). \qquad \square$$

5.2 INVARIANT SUBSPACES AND QUOTIENT SPACES

Let V be a vector space and let $\mathcal{T} : V \to V$ be a linear transformation. A $\mathcal{T}$-invariant subspace of V is a subspace W of V such that $\mathcal{T}(W) \subseteq W$. In this section we will see how to obtain invariant subspaces and we will see that if W is an invariant subspace of V, then we can obtain in a natural way the "induced" linear transformation $\overline{\mathcal{T}} : V/W \to V/W$. (Recall that V/W is the quotient of the vector space V by the subspace W. We can form V/W for any subspace W of V, but in order for $\overline{\mathcal{T}}$ to be defined we need W to be an invariant subspace.)

DEFINITION 5.2.1. Let $\mathcal{T} : V \to V$ be a linear transformation. A subspace W of V is $\mathcal{T}$*-invariant* if $\mathcal{T}(W) \subseteq W$, i.e., if $\mathcal{T}(v) \in W$ for every $v \in W$. ◇

REMARK 5.2.2. If W is a $\mathcal{T}$-invariant subspace of V, then for any polynomial $p(x)$, $p(\mathcal{T})(W) \subseteq W$. ◇

Lemma 5.2.4 and Lemma 5.2.6 give two basic ways of obtaining $\mathcal{T}$-invariant subspaces.

DEFINITION 5.2.3. Let $\mathcal{T} : V \to V$ be a linear transformation. Let $\mathcal{B} = \{v_1, \dots, v_k\}$ be a set of vectors in V. The $\mathcal{T}$*-span* of $\mathcal{B}$ is the subspace

$$W = \left\{ \sum_{i=1}^{k} p_i(\mathcal{T})\big(v_i\big) \;\Big|\; p_i(x) \in \mathbb{F}[x] \right\}.$$

In this situation $\mathcal{B}$ is said to $\mathcal{T}$*-generate* W. ◇

Lemma 5.2.4. *In the situation of Definition 5.2.3, the $\mathcal{T}$-span W of $\mathcal{B}$ is a $\mathcal{T}$-invariant subspace of V and is the smallest $\mathcal{T}$-invariant subspace of V containing $\mathcal{B}$.*

In case $\mathcal{B}$ consists of a single vector we have the following:

Lemma 5.2.5. *Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. Let $w \in V$ and let W be the subspace of V $\mathcal{T}$-generated by w. Then the dimension of W is equal to the degree of the $\mathcal{T}$-annihilator $m_{\mathcal{T},w}(x)$ of w.*

Proof. It is easy to check that $m_{\mathcal{T},w}(x)$ has degree k if and only if $\{w, \mathcal{T}(w), \dots, \mathcal{T}^{k-1}(w)\}$ is a basis of W. □

Lemma 5.2.6. *Let $\mathcal{T} : V \to V$ be a linear transformation and let $p(x) \in \mathbb{F}[x]$ be any polynomial. Then*

$$\operatorname{Ker}\big(p(\mathcal{T})\big) = \big\{v \in V \mid p(\mathcal{T})(v) = 0\big\}$$

is a $\mathcal{T}$-invariant subspace of V.

Proof. If $v \in \operatorname{Ker}(p(\mathcal{T}))$, then

$$p(\mathcal{T})(\mathcal{T}(v)) = \mathcal{T}(p(\mathcal{T}))(v) = \mathcal{T}(0) = 0. \qquad \square$$

Now we turn to quotients and induced linear transformations.

Lemma 5.2.7. *Let $\mathcal{T} : V \to V$ be a linear transformation, and let $W \subseteq V$ be a $\mathcal{T}$-invariant subspace. Then $\overline{\mathcal{T}} : V/W \to V/W$ given by $\overline{\mathcal{T}}(v+W) = \mathcal{T}(v) + W$ is a well-defined linear transformation.*

Proof. Recall from Lemma 1.5.11 that V/W is the set of distinct affine subspaces of V parallel to W, and from Proposition 1.5.4 that each such subspace is of the form $v + W$ for some element v of V. We need to check that the above formula gives a well-defined value for $\overline{\mathcal{T}}(v + W)$. Let v and v' be two elements of V with $v+W = v'+W$. Then $v-v' = w \in W$, and then $\mathcal{T}(v) - \mathcal{T}(v') = \mathcal{T}(v - v') = \mathcal{T}(w) = w' \in W$, as we are assuming that W is $\mathcal{T}$-invariant. Hence

$$\overline{\mathcal{T}}(v + W) = \mathcal{T}(v) + W = \mathcal{T}(v') + W = \overline{\mathcal{T}}(v' + W).$$

It is easy to check that $\overline{\mathcal{T}}$ is linear. □

DEFINITION 5.2.8. In the situation of Lemma 5.2.7, we call $\overline{\mathcal{T}} : V/W \to V/W$ the *quotient* linear transformation. ◇

REMARK 5.2.9. If $\pi : V \to V/W$ is the canonical projection (see Definition 1.5.12), then $\overline{\mathcal{T}}$ is given by $\overline{\mathcal{T}}(\pi(v)) = \pi(\mathcal{T}(v))$. ◇

When V is a finite-dimensional vector space, we can recast our discussion in terms of matrices.

Theorem 5.2.10. *Let V be a finite-dimensional vector space and let W be a subspace of V. Let $\mathcal{B}_1 = \{v_1, \dots, v_k\}$ be a basis of W and extend $\mathcal{B}_1$ to $\mathcal{B} = \{v_1, \dots, v_k, v_{k+1}, \dots, v_n\}$, a basis of V. Let $\mathcal{B}_2 = \{v_{k+1}, \dots, v_n\}$. Let $\pi : V \to V/W$ be the quotient map and let $\overline{\mathcal{B}}_2 = \{\pi(v_{k+1}), \dots, \pi(v_n)\}$, a basis of V/W.*

Let $\mathcal{T} : V \to V$ be a linear transformation. Then W is a $\mathcal{T}$-invariant subspace if and only if $[\mathcal{T}]_{\mathcal{B}}$ is a block upper triangular matrix of the form

$$[\mathcal{T}]_{\mathcal{B}} = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix},$$

where A is k-by-k.

In this case, let $\overline{\mathcal{T}} : V/W \to V/W$ be the quotient linear transformation. Then

$$[\overline{\mathcal{T}}]_{\overline{\mathcal{B}}} = D.$$

Lemma 5.2.11. *In the situation of Lemma 5.2.7, let V be finite dimensional, let $\overline{v} \in V/W$ be arbitrary, and let $v \in V$ be any element with $\pi(v) = \overline{v}$. Then $m_{\overline{\mathcal{T}},\overline{v}}(x)$ divides $m_{\mathcal{T},v}(x)$.*

Proof. We have $\overline{v} = v + W$. Then

$$m_{\mathcal{T},v}(\mathcal{T})(\overline{v}) = m_{\mathcal{T},v}(\mathcal{T})(v + W) = m_{\mathcal{T},v}(\mathcal{T})(v) + W = 0 + W = \overline{0},$$

where $\overline{0} = 0 + W$ is the 0 vector in V/W.

Thus $m_{\mathcal{T},v}(x)$ is a polynomial with $m_{\mathcal{T},v}(\overline{v}) = 0$. But $m_{\overline{\mathcal{T}},\overline{v}}(x)$ divides any such polynomial. □

Corollary 5.2.12. *In the situation of Lemma 5.2.11, the minimum polynomial $m_{\overline{\mathcal{T}}}(x)$ of $\overline{\mathcal{T}}$ divides the minimum polynomial $m_{\mathcal{T}}(x)$ of $\mathcal{T}$.*

Proof. It easily follows from Remark 5.2.9 that for any polynomial $p(x)$, $p(\overline{\mathcal{T}})(\pi(v)) = \pi(p(\mathcal{T})(v))$. In particular, this is true for $p(x) = m_{\mathcal{T}}(x)$. Any $\overline{v} \in V/W$ is $\overline{v} = \pi(v)$ for some $v \in V$, so

$$m_{\mathcal{T}}(\overline{\mathcal{T}})(\overline{v}) = \pi(m_{\mathcal{T}}(\mathcal{T})(v)) = \pi(0) = 0.$$

Thus $m_{\mathcal{T}}(\overline{\mathcal{T}})(\overline{v}) = 0$ for every $\overline{v} \in V/W$, i.e., $m_{\mathcal{T}}(\overline{\mathcal{T}}) = 0$. But $m_{\overline{\mathcal{T}}}(x)$ divides any such polynomial. □

5.3 The relationship between the characteristic and minimum polynomials

In this section we derive the very important Theorem 5.3.1, which gives the relationship between the minimum polynomial $m_{\mathcal{T}}(x)$ and the characteristic polynomial $c_{\mathcal{T}}(x)$ of a linear transformation $\mathcal{T} : V \to V$, where V is a finite-dimensional vector space over a general field $\mathbb{F}$. (We did this in the last chapter for $\mathbb{F}$ algebraically closed.) The key result used in proving this theorem is Theorem 5.1.11. As an immediate consequence of Theorem 5.3.1 we have Corollary 5.3.4, the Cayley-Hamilton theorem: For any such $\mathcal{T}$, $c_{\mathcal{T}}(\mathcal{T}) = 0$.

Theorem 5.3.1. *Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. Let $m_{\mathcal{T}}(x)$ be the minimum polynomial of $\mathcal{T}$ and let $c_{\mathcal{T}}(x)$ be the characteristic polynomial of $\mathcal{T}$. Then*

(1) $m_{\mathcal{T}}(x)$ divides $c_{\mathcal{T}}(x)$.

(2) Every irreducible factor of $c_{\mathcal{T}}(x)$ is an irreducible factor of $m_{\mathcal{T}}(x)$.

Proof. We proceed by induction on $n = \dim(V)$. Let $m_{\mathcal{T}}(x)$ have degree $k \le n$. Let $v \in V$ be a vector with $m_{\mathcal{T},v}(x) = m_{\mathcal{T}}(x)$. (Such a vector v exists by Theorem 5.1.11.) Let W_1 be the $\mathcal{T}$-span of v. If we let $v_k = v$ and $v_{k-i} = \mathcal{T}^i(v)$ for $i \le k-1$ then, as in the proof of Theorem 5.1.17, $\mathcal{B}_1 = \{v_1, \ldots, v_k\}$ is a basis for W_1 and $[\mathcal{T}|W_1]_{\mathcal{B}_1} = C(m_{\mathcal{T}}(x))$, the companion matrix of $m_{\mathcal{T}}(x)$.

If $k = n$ then $W_1 = V$, so $[\mathcal{T}]_{\mathcal{B}_1} = C(m_{\mathcal{T}}(x))$ has characteristic polynomial $m_{\mathcal{T}}(x)$. Thus $c_{\mathcal{T}}(x) = m_{\mathcal{T}}(x)$ and we are done.

Suppose $k < n$. Then W_1 has a complement V_2, so $V = W_1 \oplus V_2$. Let $\mathcal{B}_2$ be a basis for V_2 and $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ a basis for V. Then $[\mathcal{T}]_{\mathcal{B}}$ is a matrix of the form

$$[\mathcal{T}]_{\mathcal{B}} = \begin{bmatrix} A & B \\ 0 & D \end{bmatrix}$$

where $A = C(m_{\mathcal{T}}(x))$. (The 0 block in the lower left is due to the fact that W_1 is $\mathcal{T}$-invariant. If V_2 were $\mathcal{T}$-invariant then we would have $B = 0$, but that is not necessarily the case.) We use the basis $\mathcal{B}$ to compute $c_{\mathcal{T}}(x)$.

$$\begin{aligned} c_{\mathcal{T}}(x) &= \det\left(xI - [\mathcal{T}]_{\mathcal{B}}\right) = \det \begin{bmatrix} xI - A & -B \\ 0 & xI - D \end{bmatrix} \\ &= \det(xI - A)\det(xI - D) \\ &= m_{\mathcal{T}}(x)\det(xI - D), \end{aligned}$$

so $m_{\mathcal{T}}(x)$ divides $c_{\mathcal{T}}(x)$.

Now we must show that $m_{\mathcal{T}}(x)$ and $c_{\mathcal{T}}(x)$ have the same irreducible factors. We proceed similarly by induction. If $m_{\mathcal{T}}(x)$ has degree n then $m_{\mathcal{T}}(x) = c_{\mathcal{T}}(x)$ and we are done. Otherwise we again have a direct sum decomposition $V = W_1 \oplus V_2$ and a basis $\mathcal{B}$ with

$$[\mathcal{T}]_{\mathcal{B}} = \begin{bmatrix} A & B \\ 0 & D \end{bmatrix}.$$

In general we cannot consider the restriction $\mathcal{T}|V_2$, as V_2 may not be invariant. But we can (and will) consider $\overline{\mathcal{T}} : V/W_1 \to V/W_1$. If we let $\overline{\mathcal{B}} = \pi(\mathcal{B})$, then by Theorem 5.2.10,

$$\left[\,\overline{\mathcal{T}}\,\right]_{\overline{\mathcal{B}}} = [D].$$

By the inductive hypothesis, $m_{\overline{\mathcal{T}}}(x)$ and $c_{\overline{\mathcal{T}}}(x)$ have the same irreducible factors. Since $m_{\mathcal{T}}(x)$ divides $c_{\mathcal{T}}(x)$, every irreducible factor of $m_{\mathcal{T}}(x)$ is certainly an irreducible factor of $c_{\mathcal{T}}(x)$. We must show the other direction. Let $p(x)$ be an irreducible factor of $c_{\mathcal{T}}(x)$. As in the first part of the proof,

$$c_{\mathcal{T}}(x) = \det(xI - A)\det(xI - D) = m_{\mathcal{T}}(x)c_{\overline{\mathcal{T}}}(x).$$

Since $p(x)$ is irreducible, it divides one of the factors. If $p(x)$ divides the first factor $m_{\mathcal{T}}(x)$, we are done. Suppose $p(x)$ divides the second factor. By the inductive hypothesis, $p(x)$ divides $m_{\overline{\mathcal{T}}}(x)$. By Corollary 5.2.12, $m_{\overline{\mathcal{T}}}(x)$ divides $m_{\mathcal{T}}(x)$. Thus $p(x)$ divides $m_{\mathcal{T}}(x)$, and we are done. □

Corollary 5.3.2. *In the situation of Theorem 5.3.1, let* $m_{\mathcal{T}}(x) = p_1(x)^{e_1} \cdots p_k(x)^{e_k}$ *for distinct irreducible polynomials* $p_1(x), \dots, p_k(x)$*, and positive integers* $e_1, \dots, e_k$*. Then* $c_{\mathcal{T}}(x) = p_1(x)^{f_1} \cdots p_k(x)^{f_k}$ *for integers* $f_1, \dots, f_k$ *with* $f_i \geq e_i$ *for each* i*.*

Proof. This is just a concrete restatement of Theorem 5.3.1. □

The following special case is worth pointing out explicitly.

Corollary 5.3.3. *Let* V *be an* n *dimensional vector space and let* $\mathcal{T} : V \to V$ *be a linear transformation. Then* V *is* $\mathcal{T}$*-generated by a single element if and only if* $m_{\mathcal{T}}(x)$ *is a polynomial of degree* n*, or, equivalently, if and only if* $m_{\mathcal{T}}(x) = c_{\mathcal{T}}(x)$*.*

Proof. For $w \in V$, let W be the subspace of V $\mathcal{T}$-generated by w. Then the dimension of W is equal to the degree of $m_{\mathcal{T},w}(x)$, and $m_{\mathcal{T},w}(x)$ divides $m_{\mathcal{T}}(x)$. Thus if $m_{\mathcal{T}}(x)$ has degree less than n, W has dimension less than n and so $W \subset V$.

By Theorem 5.1.11, there is a vector $v_0 \in V$ with $m_{\mathcal{T},v_0}(x) = m_{\mathcal{T}}(x)$. Thus if $m_{\mathcal{T}}(x)$ has degree n, the subspace V_0 of V generated by v_0 has dimension n and so $V_0 = V$.

Since $m_{\mathcal{T}}(x)$ and $c_{\mathcal{T}}(x)$ are both monic polynomials, and $m_{\mathcal{T}}(x)$ divides $c_{\mathcal{T}}(x)$ by Theorem 5.3.1, then $m_{\mathcal{T}}(x) = c_{\mathcal{T}}(x)$ if and only if they have the same degree. But $c_{\mathcal{T}}(x)$ has degree n. □

Theorem 5.3.1 has a famous corollary, originally proved by completely different methods.

Corollary 5.3.4 (Cayley-Hamilton Theorem). *(1) Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation with characteristic polynomial $c_{\mathcal{T}}(x)$. Then $c_{\mathcal{T}}(\mathcal{T}) = 0$.*

(2) Let A be an n-by-n matrix and let $c_A(x)$ be its characteristic polynomial $c_A(x) = \det(xI - A)$. Then $c_A(A) = 0$.

Proof. (1) $m_{\mathcal{T}}(\mathcal{T}) = 0$ and $m_{\mathcal{T}}(x)$ divides $c_{\mathcal{T}}(x)$, so $c_{\mathcal{T}}(\mathcal{T}) = 0$.

(2) This is a translation of (1) into matrix language. (Let $\mathcal{T} = \mathcal{T}_A$.) □

REMARK 5.3.5. The minimum polynomial $m_{\mathcal{T}}(x)$ has appeared more prominently than the characteristic polynomial $c_{\mathcal{T}}(x)$ so far. As we shall see, $m_{\mathcal{T}}(x)$ plays a more important role in analyzing the structure of $\mathcal{T}$ than $c_{\mathcal{T}}(x)$ does. However, $c_{\mathcal{T}}(x)$ has the very important advantage that it can be calculated without having to consider the structure of $\mathcal{T}$. It is a determinant, and we have methods for calculating determinants. ◇

5.4 INVARIANT SUBSPACES AND INVARIANT COMPLEMENTS

We have stressed the difference between subspaces and quotient spaces. If V is a vector space and W is a subspace, then the quotient space V/W is not a subspace of V. But W always has a complement W' (though except in trivial cases, W' is not unique), $V = W \oplus W'$, and if $\pi : V \to V/W$ is the canonical projection, then the restriction π/W gives an isomorphism from W' to V/W. (On the one hand this can be very useful, but on the other hand it makes it easy to confuse the quotient space V/W with the subspace W'.)

Once we consider $\mathcal{T}$-invariant subspaces, the situation changes markedly. Given a vector space V, a linear transformation $\mathcal{T} : V \to V$, and a $\mathcal{T}$-invariant subspace W, then, as we have seen in Lemma 5.2.7, we obtain from $\mathcal{T}$ in a natural way a linear transformation $\overline{\mathcal{T}}$ on the quotient space V/W. However, it is *not* in general the case that W has a $\mathcal{T}$-invariant complement W'.

This section will be devoted investigating the question of when a $\mathcal{T}$-invariant subspace W has a $\mathcal{T}$-invariant complement W'. We will see two situations in which this is always the case—Theorem 5.4.6, whose proof is relatively simple, and Theorem 5.4.10, whose proof is more involved. Theorem 5.4.10 is the key result we will need in order to develop rational canonical form, and Theorem 5.4.6 is the key result we will need in order to further develop Jordan canonical form.

DEFINITION 5.4.1. Let $\mathcal{T} : V \to V$ be a linear transformation. Then $V = W_1 \oplus \cdots \oplus W_k$ is a *$\mathcal{T}$-invariant direct sum* if $V = W_1 \oplus \cdots \oplus W_k$ is the direct sum of $W_1, \dots, W_k$ and each W_i is a $\mathcal{T}$-invariant subspace. If $V = W_1 \oplus W_2$ is a $\mathcal{T}$-invariant direct sum decomposition, then W_2 is a *$\mathcal{T}$-invariant complement* of W_1. ◇

EXAMPLE 5.4.2. (1) Let V be a 2-dimensional vector space with basis $\{v_1, v_2\}$ and let $\mathcal{T} : V \to V$ be defined by $\mathcal{T}(v_1) = 0$, $\mathcal{T}(v_2) = v_2$. Then $W_1 = \operatorname{Ker}(\mathcal{T}) = \{c_1 v_1 \mid c_1 \in \mathbb{F}\}$ is a $\mathcal{T}$-invariant subspace, and it has $\mathcal{T}$-invariant complement $W_2 = \operatorname{Ker}(\mathcal{T} - \mathcal{I}) = \{c_2 v_2 \mid c_2 \in \mathbb{F}\}$.

(2) Let V be as in part (1) and let $\mathcal{T} : V \to V$ be defined by $\mathcal{T}(v_1) = 0$, $\mathcal{T}(v_2) = v_1$. Then $W_1 = \operatorname{Ker}(\mathcal{T}) = \{c_1 v_1 \mid c_1 \in \mathbb{F}\}$ is again a $\mathcal{T}$-invariant subspace, but it does not have a $\mathcal{T}$-invariant complement. Suppose W_2 is any $\mathcal{T}$-invariant subspace with $V = W_1 + W_2$. Then W_2 has a vector of the form $c_1 v_1 + c_2 v_2$ for some $c_2 \neq 0$. Then $\mathcal{T}(c_1 v_1 + c_2 v_2) = c_2 v_1 \in W_2$, so W_2 contains the subspace spanned by $\{c_2 v_1, c_1 v_1 + c_2 v_2\}$, i.e., $W_2 = V$, and then V is not the direct sum of W_1 and W_2. (Instead of $W_1 \cap W_2 = \{0\}$, as required for a direct sum, $W_1 \cap W_2 = W_1$.) ◇

We now consider a more elaborate situation and investigate invariant subspaces, complements, and induced linear transformations.

EXAMPLE 5.4.3. Let $g(x)$ and $h(x)$ be two monic polynomials that are not relatively prime and let $f(x) = g(x)h(x)$. (For example, we could choose an irreducible polynomial $p(x)$ and let $g(x) = p(x)^i$ and $h(x) = p(x)^j$ for positive integers i and j, in which case $f(x) = p(x)^k$ where $k = i + j$.)

Let V be a vector space and $\mathcal{T} : V \to V$ a linear transformation with $m_{\mathcal{T}}(x) = c_{\mathcal{T}}(x) = f(x)$.

Let $v_0 \in V$ be an element with $m_{\mathcal{T}, v_0}(x) = f(x)$, so that V is $\mathcal{T}$-generated by the single element v_0. Let $W_1 = h(\mathcal{T})(V)$. We claim that W_1 does not have a $\mathcal{T}$-invariant complement. We prove this by contradiction.

Suppose that $V = W_1 \oplus W_2$ where W_2 is also $\mathcal{T}$-invariant. Denote the restrictions of $\mathcal{T}$ to W_1 and W_2 by $\mathcal{T}_1$ and $\mathcal{T}_2$ respectively. First we claim that $m_{\mathcal{T}_1}(x) = g(x)$.

If $w_1 \in W_1$, then $w_1 = h(\mathcal{T})(v_1)$ for some $v_1 \in V$. But v_0 $\mathcal{T}$-generates V, so $v_1 = k(\mathcal{T})(v_0)$ for some polynomial $k(\mathcal{T})$, and then

$$\begin{aligned} g(\mathcal{T})(w_1) &= g(\mathcal{T})\big(h(\mathcal{T})(v_1)\big) = g(\mathcal{T})\big(h(\mathcal{T})\big(k(\mathcal{T})(v_0)\big)\big) \\ &= k(\mathcal{T})\big(g(\mathcal{T})\big(h(\mathcal{T})(v_0)\big)\big) \\ &= k(\mathcal{T})\big(f(\mathcal{T})(v_0)\big) = k(\mathcal{T})(0) = 0. \end{aligned}$$

Thus $g(\mathcal{T})(w_1) = 0$ for every $w_1 \in W_1$, so $m_{\mathcal{T}_1}(x)$ divides $g(x)$. If we let $w_0 = h(\mathcal{T})(v_0)$ and set $k(x) = m_{\mathcal{T}_1,w_0}(x)$, then $0 = k(\mathcal{T})(w_0) = k(\mathcal{T})h(\mathcal{T})(v_0)$, so $m_{\mathcal{T},v_0}(x) = g(x)h(x)$ divides $k(x)h(x)$. Thus $g(x)$ divides $k(x) = m_{\mathcal{T}_1,w_0}(x)$, which divides $m_{\mathcal{T}_1}(x)$.

Next we claim that $m_{\mathcal{T}_2}(x)$ divides $h(x)$. Let $w_2 \in W_2$. Then $h(\mathcal{T})(w_2) \in W_1$ (as $h(\mathcal{T})(v) \in W_1$ for every $v \in V$). Since W_2 is $\mathcal{T}$-invariant, $h(\mathcal{T})(w_2) \in W_2$, so $h(\mathcal{T})(w_2) \in W_1 \cap W_2$. But $W_1 \cap W_2 = \{0\}$ by the definition of a direct sum, so $h(\mathcal{T})(w_2) = 0$ for every $w_2 \in W_2$, and hence $m_{\mathcal{T}_2}(x)$ divides $h(x)$. Set $h_1(x) = m_{\mathcal{T}_2}(x)$.

If $V = W_1 \oplus W_2$, then $v_0 = w_1 + w_2$ for some $w_1 \in W_1$, $w_2 \in W_2$. Let $k(x)$ be the least common multiple of $g(x)$ and $h(x)$. Then $k(\mathcal{T})(v_0) = k(\mathcal{T})(w_1 + w_2) = k(\mathcal{T})(w_1) + k(\mathcal{T})(w_2) = 0 + 0$ as $m_{\mathcal{T}_1}(x) = g(x)$ divides $k(x)$ and $m_{\mathcal{T}_2}(x) = h_1(x)$ divides $h(x)$, which divides $k(x)$. Thus $k(x)$ is divisible by $f(x) = m_{\mathcal{T},v_0}(x)$. But we chose $g(x)$ and $h(x)$ to not be relatively prime, so their least common multiple $k(x)$ is a proper factor of their product $f(x)$, a contradiction. $\Diamond$

EXAMPLE 5.4.4. Suppose that $g(x)$ and $h(x)$ are relatively prime, and let $f(x) = g(x)h(x)$. Let V be a vector space and let $\mathcal{T} : V \to V$ a linear transformation with $m_{\mathcal{T}}(x) = c_{\mathcal{T}}(x) = f(x)$. Let $v_0 \in V$ with $m_{\mathcal{T},v_0}(x) = m_{\mathcal{T}}(x)$, so that V is $\mathcal{T}$-generated by v_0. Let $W_1 = h(\mathcal{T})(V)$. We claim that $W_2 = g(\mathcal{T})(V)$ is a $\mathcal{T}$-invariant complement of W_1.

First we check that $W_1 \cap W_2 = \{0\}$. An argument similar to that in the previous example shows that if $w \in W_1$, then $m_{\mathcal{T}_1,w}(x)$ divides $g(x)$, and that if $w \in W_2$, then $m_{\mathcal{T}_2,w}(x)$ divides $h(x)$. Hence if $w \in W_1 \cap W_2$, $m_{\mathcal{T},w}(x)$ divides both $g(x)$ and $h(x)$, and thus divides their gcd. These two polynomials were assumed to be relatively prime, so their gcd is 1. Hence $1w = 0$, i.e., $w = 0$.

Next we show that we can write any vector in V as a sum of a vector in W_1 and a vector in W_2. Since v_0 $\mathcal{T}$-generates V, it suffices to show that we can write v_0 in this way. Now $g(x)$ and $h(x)$ are relatively prime, so there are polynomials $r(x)$ and $s(x)$ with $g(x)r(x) + s(x)h(x) = 1$. Then

$$\begin{aligned} v_0 = 1v_0 &= \big(h(\mathcal{T})s(\mathcal{T}) + g(\mathcal{T})r(\mathcal{T})\big)\big(v_0\big) \\ &= h(\mathcal{T})\big(s(\mathcal{T})\big(v_0\big)\big) + g(\mathcal{T})\big(r(\mathcal{T})\big(v_0\big)\big) = w_1 + w_2 \end{aligned}$$

where

$$w_1 = h(\mathcal{T})(s(\mathcal{T})(v_0)) \in h(\mathcal{T})(V) = W_1$$

and

$$w_2 = g(\mathcal{T})(r(\mathcal{T})(v_0)) \in g(\mathcal{T})(V) = W_2. \qquad \Diamond$$

EXAMPLE 5.4.5. Let $g(x)$ and $h(x)$ be arbitrary polynomials and let $f(x) = g(x)h(x)$. Let V be a vector space and $\mathcal{T} : V \to V$ a linear transformation with $m_{\mathcal{T}}(x) = c_{\mathcal{T}}(x) = f(x)$. Let $v_0 \in V$ with $m_{\mathcal{T},v_0}(x) = m_{\mathcal{T}}(x)$ so that V is $\mathcal{T}$-generated by v_0.

Let $W_1 = h(\mathcal{T})(V)$. Then we may form the quotient space $\overline{V}_1 = V/W_1$, with the quotient linear transformation $\overline{\mathcal{T}} : \overline{V}_1 \to \overline{V}_1$, and $\pi_1 : V \to \overline{V}_1$. Clearly $\overline{V}_1$ is $\overline{\mathcal{T}}$-generated by the single element $\overline{v}_1 = \pi_1(v_0)$. (Since any $v \in V$ can be written as $v = k(\mathcal{T})(v_0)$ for some polynomial $k(x)$, then $v + W_1 = k(\mathcal{T})(v_0) + W_1$.) We claim that $m_{\overline{\mathcal{T}},\overline{v}_1}(x) = c_{\overline{\mathcal{T}},\overline{v}_1}(x) = h(x)$. We see that $h(\overline{\mathcal{T}})(\overline{v}_1) = h(\mathcal{T})(v_0) + W_1 = 0 + W_1$ as $h(\mathcal{T})(v_0) \in W_1$. Hence $m_{\overline{\mathcal{T}},\overline{v}_1}(x) = k(x)$ divides $h(x)$. Now $k(\overline{\mathcal{T}})(\overline{v}_1) = 0 + W_1$, i.e., $k(\mathcal{T})(v_0) \in W_1 = h(\mathcal{T})(V)$, so $k(\mathcal{T})(v_0) = h(\mathcal{T})(u_1)$ for some $u_1 \in V$. Then $g(\mathcal{T})k(\mathcal{T})(v_0) = g(\mathcal{T})h(\mathcal{T})(v_1) = f(\mathcal{T})(u_1) = 0$ since $m_{\mathcal{T}}(x) = f(x)$. Then $f(x) = g(x)h(x)$ divides $g(x)k(x)$, so $h(x)$ divides $k(x)$. Hence $m_{\overline{\mathcal{T}},\overline{v}_1}(x) = k(x) = h(x)$.

The same argument shows that if $W_2 = g(\mathcal{T})(V)$ and $\overline{V}_2 = V/W_2$ with $\overline{\mathcal{T}} : \overline{V}_2 \to \overline{V}_2$ the induced linear transformation then $\overline{V}_2$ is $\mathcal{T}$-generated by the single element $\overline{v}_2 = \pi_2(v_0)$ with $m_{\overline{\mathcal{T}},\overline{v}_2}(x) = g(x)$. $\diamond$

We now come to the two most important ways we can obtain $\mathcal{T}$-invariant complements (or direct sum decompositions). Here is the first.

Theorem 5.4.6. *Let V be a vector space and let $\mathcal{T} : V \to V$ be a linear transformation. Let $\mathcal{T}$ have minimum polynomial $m_{\mathcal{T}}(x)$ and let $m_{\mathcal{T}}(x)$ factor as a product of pairwise relatively prime polynomials, $m_{\mathcal{T}}(x) = p_1(x) \cdots p_k(x)$. For $i = 1, \dots, k$, let $W_i = \operatorname{Ker}(p_i(\mathcal{T}))$. Then each W_i is a $\mathcal{T}$-invariant subspace and $V = W_1 \oplus \cdots \oplus W_k$.*

Proof. For any i, let $w_i \in W_i$. Then

$$p_i(\mathcal{T})(\mathcal{T}(w_i)) = \mathcal{T}(p_i(\mathcal{T})(w_i)) = \mathcal{T}(0) = 0$$

so $\mathcal{T}(w_i) \in W_i$ and W_i is $\mathcal{T}$-invariant.

For each i, let $q_i(x) = m_{\mathcal{T}}(x)/p_i(x)$. Then $\{q_1(x), \dots, q_k(x)\}$ is relatively prime, so there are polynomials $r_1(x), \dots, r_k(x)$ with $q_1(x)r_1(x) + \cdots + q_k(x)r_k(x) = 1$.

Let $v \in V$. Then

$$\begin{aligned} v = \mathcal{I}v &= \big(q_1(\mathcal{T})r_1(\mathcal{T}) + \cdots + q_k(\mathcal{T})r_k(\mathcal{T})\big)(v) \\ &= w_1 + \cdots + w_k \end{aligned}$$

with $w_i = q_i(\mathcal{T})r_i(\mathcal{T})(v)$. Furthermore,

$$\begin{aligned} p_i(\mathcal{T})\big(w_i\big) &= p_i(\mathcal{T})q_i(\mathcal{T})r_i(\mathcal{T})(v) \\ &= m_{\mathcal{T}}(\mathcal{T})r_i(\mathcal{T})(v) = 0 \qquad \text{as } m_{\mathcal{T}}(\mathcal{T}) = 0 \end{aligned}$$

by the definition of the minimum polynomial $m_{\mathcal{T}}(x)$, and so $w_i \in W_i$.

To complete the proof we show that if $0 = w_1 + \cdots + w_k$ with $w_i \in W_i$ for each i, then $w_1 = \cdots = w_k = 0$. Suppose $i = 1$. Then $0 = w_1 + \cdots + w_k$ so

$$\begin{aligned} 0 = q_1(\mathcal{T})(0) &= q_1(\mathcal{T})(w_1 + \cdots + w_k) \\ &= q_1(\mathcal{T})(w_1) + 0 + \cdots + 0 = q_1(\mathcal{T})(w_1) \end{aligned}$$

as $p_i(x)$ divides $q_1(x)$ for every $i > 1$. Also $p_1(\mathcal{T})(w_1) = 0$ by definition. Now $p_1(x)$ and $q_1(x)$ are relatively prime, so there exist polynomials $f(x)$ and $g(x)$ with $f(x)p_1(x) + g(x)q_1(x) = 1$. Then

$$\begin{aligned} w_1 = \mathcal{I}w_1 &= (f(\mathcal{T})p_1(\mathcal{T}) + g(\mathcal{T})q_1(\mathcal{T}))(w_1) \\ &= f(\mathcal{T})(p_1(\mathcal{T})(w_1)) + g(\mathcal{T})(q_1(\mathcal{T})(w_1)) \\ &= f(\mathcal{T})(0) + g(\mathcal{T})(0) = 0 + 0 = 0. \end{aligned}$$

Similarly, $w_i = 0$ for each i. □

As a consequence, we obtain the $\mathcal{T}$-invariant subspaces of a linear transformation $\mathcal{T} : V \to V$.

Theorem 5.4.7. *Let $\mathcal{T} : V \to V$ be a linear transformation and let $m_{\mathcal{T}}(x) = p_1(x)^{e_1} \cdots p_k(x)^{e_k}$ be a factorization of the minimum polynomial of $\mathcal{T}$ into powers of distinct irreducible polynomials. Let $W_i = \operatorname{Ker}(p_i(\mathcal{T})^{e_i})$, so that $V = W_1 \oplus \cdots \oplus W_k$, a $\mathcal{T}$-invariant direct sum decomposition. For $i = 1, \ldots, k$, let U_i be a $\mathcal{T}$-invariant subspace of W_i (perhaps $U_i = \{0\}$). Then $U = U_1 \oplus \cdots \oplus U_k$ is a $\mathcal{T}$-invariant subspace of V, and every $\mathcal{T}$-invariant subspace of V arises in this way.*

Proof. We have $V = W_1 \oplus \cdots \oplus W_k$, by Theorem 5.4.6. It is easy to check that any such U is $\mathcal{T}$-invariant. We show that these are all the $\mathcal{T}$-invariant subspaces.

Let U be any $\mathcal{T}$-invariant subspace of V. Let $\pi_i : V \to W_i$ be the projection and let $U_i = \pi_i(U)$. We claim that $U = U_1 \oplus \cdots \oplus U_k$. To show that it suffices to show that $U_i \subseteq U$ for each i. Let $u_i \in U_i$. Then, by the definition of U_i, there is an element u of U of the form $u = u_1 + \cdots + u_i + \cdots + u_k$, for some elements $u_j \in U_j$, $j \neq i$. Let $q_i(x) = m_{\mathcal{T}}(x)/p_i(x)^{e_i}$.

Since $p_i(x)^{e_i}$ and $q_i(x)$ are relatively prime, there are polynomials $r_i(x)$ and $s_i(x)$ with $r_i(x)p_i(x)^{e_i} + s_i(x)q_i(x) = 1$. We have $q_i(\mathcal{T})(u_j) = 0$ for $j \neq i$ and $p_i(\mathcal{T})^{e_i}(u_i) = 0$. Then

$$\begin{aligned} u_i &= 1u_i = \big(1 - r_i(\mathcal{T})p_i(\mathcal{T})^{e_i}\big)\big(u_i\big) \\ &= s_i(\mathcal{T})q_i(\mathcal{T})\big(u_i\big) \\ &= 0 + \ldots + s_i(\mathcal{T})q_i(\mathcal{T})\big(u_i\big) + \ldots + 0 \\ &= s_i(\mathcal{T})q_i(\mathcal{T})\big(u_1\big) + \ldots + s_i(\mathcal{T})q_i(\mathcal{T})(u_i) + \ldots + s_k(\mathcal{T})q_k(\mathcal{T})(u_i) \\ &= s_i(\mathcal{T})q_i(\mathcal{T})\big(u_1 + \ldots + u_i + \ldots + u_k\big) = s_i(\mathcal{T})q_i(\mathcal{T})(u). \end{aligned}$$

Since U is $\mathcal{T}$-invariant, $s_i(\mathcal{T})q_i(\mathcal{T})(u) \in U$, i.e., $u_i \in U$, as claimed. □

Now we come to the second way in which we can obtain $\mathcal{T}$-invariant complements. The proof here is complicated, so we separate it into two stages.

Lemma 5.4.8. *Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. Let $w_1 \in V$ be any vector with $m_{\mathcal{T},w_1}(x) = m_{\mathcal{T}}(x)$ and let W_1 be the subspace of V $\mathcal{T}$-generated by w_1. Suppose that W_1 is a proper subspace of V and that there is a vector $v_2 \in V$ such that V is $\mathcal{T}$-generated by $\{w_1, v_2\}$. Then there is a vector $w_2 \in V$ such that $V = W_1 \oplus W_2$, where W_2 is the subspace of V $\mathcal{T}$-generated by w_2.*

Proof. Observe that if V_2 is the subspace of V that is $\mathcal{T}$-generated by v_2, then V_2 is a $\mathcal{T}$-invariant subspace and, by hypothesis, every $v \in V$ can be written as $v = w_1' + v_2''$ for some $w_1' \in W_1$ and some $v_2'' \in V_2$. Thus $V = W_1 + V_2$. However, there is no reason to conclude that W_1 and V_2 are independent subspaces of V, and that may not be the case.

Our proof will consist of showing how to "modify" v_2 to obtain a vector w_2 such that we can still write every $v \in V$ as $v = w_1' + w_2'$ with $w_1' \in W_1$ and $w_2' \in W_2$, the subspace of V $\mathcal{T}$-generated by w_2, and with $W_1 \cap W_2 = \{0\}$. We consider the vector $v_2' = v_2 + w$ where w is any element of W_1. Then we observe that $\{w_1, v_2'\}$ also $\mathcal{T}$-generates V. Our proof will consist of showing that for the proper choice of w, $w_2 = v_2' = v_2 + w$ is an element of V with $W_1 \cap W_2 = \{0\}$. Let V have dimension n and let $m_{\mathcal{T}}(x)$ be a polynomial of degree k. Set $j = n - k$. Then W_1 has basis

$$\mathcal{B}_1 = \{u_1, \ldots, u_k\} = \{\mathcal{T}^{k-1}(w_1), \ldots, \mathcal{T}(w_1), w_1\}.$$

By hypothesis, V is spanned by

$$\{w_1, \mathcal{T}(w_1), \ldots\} \cup \{v_2', \mathcal{T}(v_2'), \ldots\},$$

so V is also spanned by

$$\{w_1, \mathcal{T}(w_1), \ldots, \mathcal{T}^{k-1}(w_1)\} \cup \{v_2', \mathcal{T}(v_2'), \ldots\}.$$

We claim that

$$\{w_1, \mathcal{T}(w_1), \ldots, \mathcal{T}^{k-1}(w_1)\} \cup \{v_2', \mathcal{T}(v_2'), \ldots, \mathcal{T}^{j-1}(v_2')\}$$

is a basis for V. We see this as follows: We begin with the linearly independent set $\{w_1, \ldots, \mathcal{T}^{k-1}(w_1)\}$ and add $v_2', \mathcal{T}(v_2'), \ldots$ as long as we can do so and still obtain a linearly independent set. The furthest we can go is through $\mathcal{T}^{j-1}(v_2')$, as then we have $k + j = n$ vectors in an n-dimensional vector space. But we need to go that far, as once some $\mathcal{T}^i(v_2')$ is a linear combination of $\mathcal{B}_1$ and $\{v_2', \ldots, \mathcal{T}^{i-1}(v_2')\}$, this latter set, consisting of $k + i$ vectors, spans V, so $i \geq j$. (The argument for this uses the fact that W_1 is $\mathcal{T}$-invariant.) We then let

$$\mathcal{B}_2' = \{u_{k+1}', \ldots, u_n'\} = \{\mathcal{T}^{j-1}(v_2'), \ldots, v_2'\} \text{ and } \mathcal{B}' = \mathcal{B}_1 \cup \mathcal{B}_2'.$$

Then $\mathcal{B}'$ is a basis of V.

Consider $\mathcal{T}^j(u_n')$. It has a unique expression in terms of basis elements:

$$\mathcal{T}^j\big(u_n'\big) = \sum_{i=1}^{k} b_i u_i + \sum_{i=0}^{j-1} \big(-c_i\big) u_{n-i}'.$$

If we let $p(x) = x^j + c_{j-1}x^{j-1} + \cdots + c_0$, we have that

$$u = p(\mathcal{T})\big(v_2'\big) = p(\mathcal{T})\big(u_n'\big) = \sum_{i=1}^{k} b_i u_i \in W_1.$$

Case I (incredibly lucky): $u = 0$. Then $\mathcal{T}^j(v_2') \in V_2'$, the subspace $\mathcal{T}$-spanned by v_2', which implies that $\mathcal{T}^i(v_2') \in V_2'$ for every i, so V_2' is $\mathcal{T}$-invariant. Thus in this case we choose $w_2 = v_2'$, so $W_2 = V_2$, $\mathcal{T} = W_1 \oplus W_2$, and we are done.

Case II (what we expect): $u \neq 0$. We have to do some work.

The key observation is that the coefficients $b_k, b_{k-1}, \ldots, b_{k-j+1}$ are all 0, and hence $u = \sum_{i=1}^{k-j} b_i u_i$. Here is where we *crucially* use the hypothesis that $m_{\mathcal{T},w_1}(x) = m_{\mathcal{T}}(x)$. We argue by contradiction. Suppose $b_m \neq 0$ for some $m \geq k - j + 1$, and let m be the largest such index. Then

$$\mathcal{T}^{m-1}(u) = b_m u_1, \quad \mathcal{T}^{m-2}(u) = b_m u_2 + b_{m-1} u_1, \quad \ldots.$$

Thus we see that

$$\{\mathcal{T}^{m-1}p(\mathcal{T})\big(v_2'\big), \mathcal{T}^{m-2}p(\mathcal{T})\big(v_2'\big), \dots, p(\mathcal{T})\big(v_2'\big),$$
$$\mathcal{T}^{j-1}\big(v_2'\big), \mathcal{T}^{j-2}\big(v_2'\big), \dots, v_2'\}$$

is a linearly independent subset of V_2', the subspace of V $\mathcal{T}$-generated by v_2', and hence V_2' has dimension at least $m + j \geq k + 1$. That implies that $m_{\mathcal{T},v_2'}(x)$ has degree at least $k + 1$. But $m_{\mathcal{T},v_2'}(x)$ divides $m_{\mathcal{T}}(x) = m_{\mathcal{T},w_1}(x)$, which has degree k, and that is impossible.

We now set

$$w = -\sum_{i=1}^{k-1} b_i u_{i+j}$$

and $w_2 = v_2' + w$,

$$\mathcal{B}_1 = \{u_1, \dots, u_k\} = \{\mathcal{T}^{k-1}(w_1), \dots, w_1\} \quad \text{(as before)},$$
$$\mathcal{B}_2 = \{u_{k+1}, \dots, u_n\} = \{\mathcal{T}^{j-1}(w_2), \dots, w_2\}, \text{ and } \mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2.$$

We then have

$$\begin{aligned}\mathcal{T}^j\big(u_n\big) &= \mathcal{T}^j\big(v_2' + w\big) = \mathcal{T}^j\big(v_2'\big) + \mathcal{T}^j\big(w\big)\\ &= \sum_{i=1}^{k-j} b_i u_i + \mathcal{T}^j\left(-\sum_{i=1}^{k-j} b_i u_{i+j}\right)\\ &= \sum_{i=1}^{k-j} b_i u_i + \sum_{i=1}^{k-j}\big(-b_i u_i\big) = 0\end{aligned}$$

and we are back in Case I (through skill, rather than luck) and we are done. □

Corollary 5.4.9. *In the situation of Lemma 5.4.8, let $n = \dim V$ and let $k = \deg m_{\mathcal{T}}(x)$. Then $n \leq 2k$. Suppose that $n = 2k$. If V_2 is the subspace of V $\mathcal{T}$-generated by v_2, then $V = W_1 \oplus V_2$.*

Proof. From the proof of Lemma 5.4.8 we see that $j = n - k \leq k$. Also, if $n = 2k$, then $j = k$, so $b_k, b_{k-1}, \dots, b_1$ are all zero. Then $u = 0$, and we are Case I. □

Theorem 5.4.10. *Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. Let $w_1 \in V$ be any vector with*

$m_{\mathcal{T},w_1}(x) = m_{\mathcal{T}}(x)$ and let W_1 be the subspace of V $\mathcal{T}$-generated by w_1. Then W_1 has a $\mathcal{T}$-invariant complement W_2, i.e., there is a $\mathcal{T}$-invariant subspace W_2 of V with $V = W_1 \oplus W_2$.

Proof. If $W_1 = V$ then $W_2 = \{0\}$ and we are done.

Suppose not. $W_2 = \{0\}$ is a $\mathcal{T}$-invariant subspace of V with $W_1 \cap W_2 = \{0\}$. Then there exists a maximal $\mathcal{T}$-invariant subspace W_2 of V with $W_1 \cap W_2 = \{0\}$, either by using Zorn's Lemma, or more simply by taking such a subspace of maximal dimension. We claim that $W_1 \oplus W_2 = V$.

We prove this by contradiction, so assume $W_1 \oplus W_2 \subset V$.

Choose an element v_2 of V with $v_2 \notin W_1 \oplus W_2$. Let V_2 be the subspace $\mathcal{T}$-spanned by v_2 and let $U_2 = W_2 + V_2$. If $W_1 \cap U_2 = \{0\}$ then U_2 is a $\mathcal{T}$-invariant subspace of V with $W_1 \cap U_2 = \{0\}$ and with $U_2 \supset W_2$, contradicting the maximality of W_2.

Otherwise, let $V' = W_1 + U_2$. Then V' is a $\mathcal{T}$-invariant subspace of V so we may consider the restriction $\mathcal{T}'$ of $\mathcal{T}$ to V', $\mathcal{T}' : V' \to V'$. Now W_2 is a $\mathcal{T}'$-invariant subspace of V', so we may consider the quotient linear transformation $\overline{\mathcal{T}'} : V'/W_2 \to V'/W_2$. Set $X = V'/W_2$ and $\mathcal{S} = \overline{\mathcal{T}'}$. Let $\pi : V' \to X$ be the quotient map. Let $\overline{w}_1 = \pi(w_1)$ and let $\overline{v}_2 = \pi(v_2)$. Let $Y_1 = \pi(W_1) \subset X$ and let $Z_2 = \pi(U_2) \subset X$. We make several observations: First, Y_1 and Z_2 are $\mathcal{S}$-invariant subspaces of X. Second, Y_1 is $\mathcal{T}$-spanned by $\overline{w}_1$ and Z_2 is $\mathcal{T}$-spanned by $\overline{v}_2$, so that X is $\mathcal{T}$-spanned by $\{\overline{w}_1, \overline{v}_2\}$. Third, since $W_1 \cap W_2 = \{0\}$, the restriction of π to W_1, $\pi : W_1 \to Y_1$, is 1-1.

Certainly $m_{\mathcal{T}'}(x)$ divides $m_{\mathcal{T}}(x)$ (as if $p(\mathcal{T})(v) = 0$ for every $v \in V$, then $p(\mathcal{T})(v) = 0$ for every $v \in V'$) and we know that $m_{\mathcal{S}}(x)$ divides $m_{\mathcal{T}'}(x)$ by Corollary 5.2.12. By hypothesis $m_{\mathcal{T},w_1}(x) = m_{\mathcal{T}}(x)$, and, since $\pi : W_1 \to Y_1$ is 1-1, $m_{\mathcal{S},\overline{w}_1}(x) = m_{\mathcal{T},w_1}(x)$. Since $w_1 \in V'$, $m_{\mathcal{T},w_1}(x)$ divides $m_{\mathcal{T}'}(x)$. Finally, $m_{\mathcal{S},\overline{w}_1}(x)$ divides $m_{\mathcal{S}}(x)$. Putting these together, we see that

$$m_{\mathcal{S},\overline{w}_1}(x) = m_{\mathcal{S}}(x) = m_{\mathcal{T}'}(x) = m_{\mathcal{T}}(x) = m_{\mathcal{T},w_1}(x).$$

We now apply Lemma 5.4.8 with $\mathcal{T} = \mathcal{S}$, $V = X$, $w_1 = \overline{w}_1$, and $v_2 = \overline{v}_2$. We conclude that there is a vector, which we denote by $\overline{w}_2$, such that $X = Y_1 \oplus Y_2$, where Y_2 is the subspace of X generated by $\overline{w}_2$. Let w_2' be any element of V' with $\pi(w_2') = \overline{w}_2$, and let V_2' be the subspace of V' $\mathcal{T}'$-spanned by w_2', or, equivalently, the subspace of V $\mathcal{T}$-spanned by w_2'. Then $\pi(V_2') = Y_2$.

To finish the proof, we observe that

$$V'/W_2 = X = Y_1 + Z_2 = Y_1 \oplus Y_2,$$

so, setting $U_2' = W_2 + V_2'$,

$$V = W_1 + V_2' + W_2 = W_1 + \left(W_2 + V_2'\right) = W_1 + U_2'.$$

Also, $W_1 \cap U_2' = \{0\}$. For if $x \in W_1 \cap U_2'$, $\pi(x) \in \pi(W_1) \cap \pi(U_2') = Y_1 \cap Y_2 = \{0\}$ (as $\pi(w_2) = \{0\}$). But if $x \in W_1 \cap U_2'$, then $x \in W_1$, and the restriction of π to W_1 is 1-1, so $\pi(x) = 0$ implies $x = 0$.

Hence $V' = W_1 \oplus U_2'$ and $U_2' \supset W_2$, contradicting the maximality of W_2. □

We will only need Theorem 5.4.10 but we can generalize it.

Corollary 5.4.11. *Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. Let $w_1, \dots, w_k \in V$ and let W_i be the subspace $\mathcal{T}$-spanned by w_i, $i = 1, \dots, k$. Suppose that $m_{\mathcal{T},w_i}(x) = m_{\mathcal{T}}(x)$ for $i = 1, \dots, k$, and that $\{W_1, \dots, W_k\}$ is independent. Then $W_1 \oplus \cdots \oplus W_k$ has a $\mathcal{T}$-invariant complement, i.e., there is a $\mathcal{T}$-invariant subspace W' of V with $V = W_1 \oplus \cdots \oplus W_k \oplus W'$.*

Proof. We proceed by induction on k. The $k = 1$ case is Theorem 5.4.10. For the induction step, consider $\overline{\mathcal{T}} : \overline{V} \to \overline{V}$ where $\overline{V} = V/W_1$.

We outline the proof.

Let W_{k+1} be a maximal $\mathcal{T}$-invariant subspace of V with

$$(W_1 \oplus \cdots \oplus W_k) \cap W_{k+1} = \{0\}.$$

We claim that $W_1 \oplus \cdots \oplus W_{k+1} = V$. Assume not. Let $\overline{W}_i = T(W_i)$ for $i = 2, \dots, k$. By the inductive hypothesis, $\overline{W}_2 \oplus \cdots \oplus \overline{W}_k$ has a $\mathcal{T}$-invariant complement $\overline{Y}_{k+1}$ containing $\pi(W_{k+1})$. (This requires a slight modification of the statement and proof of Theorem 5.4.10. We used our original formulation for the sake of simplicity.) Let Y_{k+1} be a subspace of V with $Y_{k+1} \supseteq W_{k+1}$ and $\pi(Y_{k+1}) = \overline{Y}_{k+1}$. Certainly $(W_2 \oplus \cdots \oplus W_k) \cap Y_{k+1} = \{0\}$. Choose any vector $y \in Y_{k+1}$, $y \notin W_{k+1}$. If the subspace Y $\mathcal{T}$-generated by y is disjoint from W_1, set $x = y$ and $X = Y$. Otherwise, "modify" Y as in the proof of Lemma 5.4.8 to obtain x with X, the subspace $\mathcal{T}$-generated by x, disjoint from W_1. Set $W' = W_{k+1} \oplus X$. Then $W' \supset W_{k+1}$ and W' is disjoint from $W_1 \oplus \cdots \oplus W_k$, contradicting the maximality of W_{k+1}. □

5.5 RATIONAL CANONICAL FORM

Let V be a finite-dimensional vector space over an arbitrary field $\mathbb{F}$ and let $\mathcal{T} : V \to V$ be a linear transformation. In this section we prove that $\mathcal{T}$ has a unique rational canonical form.

The basic idea of the proof is one we have seen already in a much simpler context. Recall the theorem that any linearly independent subset of a vector space extends to a basis of that vector space. We think of that as saying that any partial good set extends to a complete good set. We would like to do the same thing in the presence of a linear transformation $\mathcal{T}$: Define a partial $\mathcal{T}$-good set and show that any partial $\mathcal{T}$-good set extends to a complete $\mathcal{T}$-good set. But we have to be careful to define a $\mathcal{T}$-good set in the right way. We will see that the right kind of way to define a partial $\mathcal{T}$-good set is to define it as the right kind of basis for the right kind of $\mathcal{T}$-invariant subspace W. Then we will be able extend this to the right kind of basis for all of V by using Theorem 5.4.10.

DEFINITION 5.5.1. Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. An ordered set $\mathcal{C} = \{w_1, \ldots, w_k\}$ is a *rational canonical $\mathcal{T}$-generating set* of V if the following conditions are satisfied:

(1) $V = W_1 \oplus \cdots \oplus W_k$ where W_i is the subspace of V that is $\mathcal{T}$-generated by w_i

(2) $p_i(x)$ is divisible by $p_{i+1}(x)$ for $i = 1, \ldots, k-1$, where $p_i(x) = m_{\mathcal{T},w_i}(x)$ is the $\mathcal{T}$-annihilator of w_i. $\diamond$

When $\mathcal{T} = \mathcal{I}$, any basis of V is a rational canonical $\mathcal{T}$-generating set and vice-versa, with $p_i(x) = x - 1$ for every i. Of course, every V has a basis. A basis for V is never unique, but any two bases of V have the same number of elements, namely the dimension of V.

Here is the appropriate generalization of these two facts. For the second fact, we have not only that any two rational canonical $\mathcal{T}$-generating sets have the same number of elements, but also the same number of elements of each "type", where the type of an element is its $\mathcal{T}$-annihilator.

Theorem 5.5.2. *Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. Then V has a rational canonical $\mathcal{T}$-generating set $\mathcal{C} = \{w_1, \ldots, w_k\}$. If $\mathcal{C}' = \{w_1', \ldots, w_l'\}$ is any rational canonical $\mathcal{T}$-generating set of V, then $k = l$ and $p_i'(x) = p_i(x)$ for $i = 1, \ldots, k$, where $p_i'(x) = m_{\mathcal{T},w_i'}(x)$ and $p_i(x) = m_{\mathcal{T},w_i}(x)$.*

Proof. First we prove existence and then we prove uniqueness.

For existence we proceed by induction on $n = \dim(V)$. Choose an element w_1 of V with $m_{\mathcal{T},w_1}(x) = m_{\mathcal{T}}(x)$ and let W_1 be the subspace of V $\mathcal{T}$-generated by w_1. If $W_1 = V$ we are done.

Otherwise, let W' be a $\mathcal{T}$-invariant complement of W in V, which exists by Theorem 5.4.10. Then $V = W \oplus W'$. Let $\mathcal{T}'$ be the restriction of $\mathcal{T}$ to W', $\mathcal{T}' : W' \to W'$. Then $m_{\mathcal{T}'}(x)$ divides $m_{\mathcal{T}}(x)$. (Since $m_{\mathcal{T}}(\mathcal{T})(v) = 0$ for all $v \in V$, $m_{\mathcal{T}}(\mathcal{T})(v) = 0$ for all v in W'.) By induction, W' has a rational canonical $\mathcal{T}'$-generating set that we write as $\{w_2, \dots, w_k\}$. Then $\{w_1, \dots, w_k\}$ is a rational canonical $\mathcal{T}$-generating set of V.

For uniqueness, suppose V has rational canonical $\mathcal{T}$-generating sets $\mathcal{C} = \{w_1, \dots, w_k\}$ and $\mathcal{C}' = \{w_1', \dots, w_l'\}$ with corresponding $\mathcal{T}$-invariant direct sum decompositions $V = W_1 \oplus \cdots \oplus W_k$ and $V = W_1' \oplus \cdots \oplus W_l'$ and corresponding $\mathcal{T}$-annihilators $p_i(x) = m_{\mathcal{T},w_i}(x)$ and $p_i'(x) = m_{\mathcal{T},w_i'}(x)$. Let these polynomials have degree d_i and d_i' respectively, and let V have dimension n. We proceed by induction on k.

Now $p_1(x) = m_{\mathcal{T}}(x)$ and $p_1'(x) = m_{\mathcal{T}}(x)$, so $p_1'(x) = p_1(x)$. If $k = 1$, $V = W_1$, $\dim(V) = \dim(W_1)$, $n = d_1$. But then $n = d_1' = \dim(W_1')$ so $V = W_1'$. Then $l = 1$, $p_1'(x) = p_1(x)$, and we are done.

Suppose for some $k \geq 1$ we have $p_i'(x) = p_i(x)$ for $i = 1, \dots, k$. If $V = W_1 \oplus \cdots \oplus W_k$ then $n = d_1 + \cdots + d_k = d_1' + \cdots + d_k'$ so $V = W_1' \oplus \cdots \oplus W_k'$ as well, $l = k$, $p_i'(x) = p_i(x)$ and we are done, and similarly if $V = W_1' \oplus \cdots \oplus W_l'$. Otherwise consider the vector space $p_{k+1}(\mathcal{T})(V)$, a $\mathcal{T}$-invariant subspace of V. Since $V = W_1 \oplus \cdots \oplus W_k \oplus W_{k+1} \oplus \cdots$ we have that

$$\begin{aligned} p_{k+1}(\mathcal{T})(V) = p_{k+1}(\mathcal{T})\big(W_1\big) \oplus \cdots \oplus p_{k+1}(\mathcal{T})\big(W_k\big) \\ \oplus\, p_{k+1}(\mathcal{T})\big(W_{k+1}\big) \oplus \cdots . \end{aligned}$$

Let us identify this subspace further. Since $p_{k+1}(x) = m_{\mathcal{T},w_{k+1}}(x)$, we have that $p_{k+1}(\mathcal{T})(w_{k+1}) = 0$, and hence $p_{k+1}(\mathcal{T})(W_{k+1}) = 0$. Since $p_{k+i}(x)$ divides $p_{k+1}(x)$ for $i \geq 1$, we also have that $p_{k+1}(\mathcal{T})(w_{k+i}) = 0$ and hence $p_{k+1}(\mathcal{T})(W_{k+i}) = 0$ for $i \geq 1$. Thus

$$p_{k+1}(\mathcal{T})(V) = p_{k+1}(\mathcal{T})\big(W_1\big) \oplus \cdots \oplus p_{k+1}(\mathcal{T})\big(W_k\big).$$

Now $p_{k+1}(x)$ divides $p_i(x)$ for $i < k$, so $p_{k+1}(\mathcal{T})(W_i)$ has dimension $d_i - d_{k+1}$, and hence $p_{k+1}(\mathcal{T})(V)$ is a vector space of dimension $d = (d_1 - d_{k+1}) + (d_2 - d_{k+1}) + \cdots + (d_k - d_{k+1})$. (Some or all of these differences of dimensions may be zero, which does not affect the argument.)

Apply the same argument to the decomposition $V = W_1' \oplus \cdots \oplus W_l'$ to obtain

$$p_{k+1}(\mathcal{T})(V) = p_{k+1}(\mathcal{T})\big(W_1'\big) \oplus \cdots \oplus p_{k+1}(\mathcal{T})\big(W_k'\big) \oplus p_{k+1}(\mathcal{T})\big(W_{k+1}'\big) \oplus \cdots$$

which has the subspace $p_{k+1}(\mathcal{T})(W_1') \oplus \cdots \oplus p_{k+1}(\mathcal{T})(W_k')$ of dimension d as well (since $p_i'(x) = p_i(x)$ for $i \leq k$). Thus this subspace must be the entire space, and in particular $p_{k+1}(\mathcal{T})(W_{k+1}') = 0$, or, equivalently, $p_{k+1}(\mathcal{T})(W_{k+1}') = 0$. But w_{k+1}' has $\mathcal{T}$-annihilator $p_{k+1}'(x)$, so $p_{k+1}'(x)$ divides $p_{k+1}(x)$. The same argument using $p_{k+1}'(\mathcal{T})(V)$ instead of $p_{k+1}(\mathcal{T})(V)$ shows that $p_{k+1}(x)$ divides $p_{k+1}'(x)$, so we see that $p_{k+1}'(x) = p_k(x)$. Proceeding in this way we obtain $p_i'(x) = p_i(x)$ for every i, and $l = k$, and we are done. □

We translate this theorem into matrix language.

DEFINITION 5.5.3. An n-by-n matrix M is in *rational canonical form* if M is a block diagonal matrix

$$M = \begin{bmatrix} C\big(p_1(x)\big) & & & \\ & C\big(p_2(x)\big) & & \\ & & \ddots & \\ & & & C\big(p_k(x)\big) \end{bmatrix}$$

where $C(p_i(x))$ denotes the companion matrix of $p_i(x)$, for some sequence of polynomials $p_1(x), p_2(x), \ldots, p_k(x)$ with $p_i(x)$ divisible by $p_{i+1}(x)$ for $i = 1, \ldots, k-1$. ◇

Theorem 5.5.4 (Rational Canonical Form)**.** *(1) Let V be a finite-dimensional vector space, and let $\mathcal{T} : V \to V$ be a linear transformation. Then V has a basis $\mathcal{B}$ such that $[\mathcal{T}]_{\mathcal{B}} = M$ is in rational canonical form. Furthermore, M is unique.*

(2) Let A be an n-by-n matrix. Then A is similar to a unique matrix M in rational canonical form.

Proof. (1) Let $\mathcal{C} = \{w_1, \ldots, w_k\}$ be a rational canonical $\mathcal{T}$-generating set for V, where $p_i(x) = m_{T,w_i}(x)$ has dimension d_i. Then

$$\mathcal{B} = \big\{\mathcal{T}^{d_1-1}\big(w_1\big), \ldots, w_1, \mathcal{T}^{d_2-1}\big(w_2\big), \ldots, w_2, \ldots, \mathcal{T}^{d_k-1}\big(w_k\big), \ldots, w_k\big\}$$

is the desired basis.

(2) Apply part (1) to the linear transformation $\mathcal{T} = \mathcal{T}_A$. □

DEFINITION 5.5.5. If $\mathcal{T}$ has rational canonical form with diagonal blocks $C(p_1(x)), C(p_2(x)), \ldots, C(p_k(x))$ with $p_i(x)$ divisible by $p_{i+1}(x)$ for $i = 1, \ldots, k-1$, then $p_1(x), \ldots, p_k(x)$ is the sequence of *elementary divisors* of $\mathcal{T}$. $\diamond$

Corollary 5.5.6. *(1) $\mathcal{T}$ is determined up to similarity by its sequence of elementary divisors $p_1(x), \ldots, p_k(x)$*

(2) The sequence of elementary divisors $p_1(x), \ldots, p_k(x)$ is determined recursively as follows: $p_1(x) = m_{\mathcal{T}}(x)$. Let w_1 be any element of V with $m_{\mathcal{T},w_1}(x) = m_{\mathcal{T}}(x)$ and let W_1 be the subspace $\mathcal{T}$-generated by w_1. Let $\overline{\mathcal{T}} : V/W_1 \to V/W_1$. Then $p_2(x) = m_{\overline{\mathcal{T}}}(x)$, etc.

Corollary 5.5.7. *Let $\mathcal{T}$ have elementary divisors $\{p_1(x), \ldots, p_k(x)\}$. Then*

(1) $m_{\mathcal{T}}(x) = p_1(x)$

(2) $c_{\mathcal{T}}(x) = p_1(x)p_2(x)\cdots p_k(x)$.

Proof. We already know (1). As for (2),

$$c_{\mathcal{T}}(x) = \det(C(p_1(x)))\det(C(p_2(x)))\cdots = p_1(x)p_2(x)\cdots p_k(x). \quad \square$$

REMARK 5.5.8. In the next section we will develop Jordan canonical form, and in the following section we will develop an algorithm for finding the Jordan canonical form of a linear transformation $\mathcal{T} : V \to V$, and for finding a Jordan basis of V, providing we can factor the characteristic polynomial of $\mathcal{T}$.

There is an unconditional algorithm for finding a rational canonical $\mathcal{T}$-generating set for a linear transformation $\mathcal{T} : V \to V$, and hence the rational canonical form of $\mathcal{T}$. Since it can be tedious to apply, and the result is not so important, we will merely sketch the argument.

First observe that for any nonzero vector $v \in V$, we can find its $\mathcal{T}$-annihilator $m_{\mathcal{T},x}(x)$ as follows: Successively check whether the sets $\{v\}, \{v, \mathcal{T}(v)\}, \{v, \mathcal{T}(v), \mathcal{T}^2(v)\}, \ldots,$ are linearly independent. When we come to a linearly dependent set $\{v, \mathcal{T}(v), \ldots, \mathcal{T}^k(v)\}$, stop. From the linear dependence we obtain the $\mathcal{T}$-annihilator $m_{\mathcal{T}}(x)$ of v, a polynomial of degree k.

Next observe that using Euclid's algorithm we may find the gcd and lcm of any finite set of polynomials (without having to factor them).

Given these observations we proceed as follows: Pick a basis $\{v_1, \ldots, v_n\}$ of V. Find the $\mathcal{T}$-annihilators $m_{\mathcal{T},v_1}(x), \ldots, m_{\mathcal{T},v_n}(x)$. Knowing these, we can find the minimum polynomial $m_{\mathcal{T}}(x)$ by using Theorem 5.1.5. Then we can find a vector $w_1 \in V$ with $m_{\mathcal{T},w_1}(x) = m_{\mathcal{T}}(x)$ by using Theorem 5.1.11.

Let W_1 be the subspace of V $\mathcal{T}$-generated by w_1. Choose any complement V_2 of V, so that $V = W_1 \oplus V_2$, and choose any basis $\{v_2, \ldots, v_m\}$ of V_2. Successively "modify" $v_2, \ldots, v_m$ to $u_2, \ldots, u_m$ as in the proof of Lemma 5.4.8. The subspace U_2 spanned by $\{u_2, \ldots, u_m\}$ is a $\mathcal{T}$-invariant complement of W_1, $V = W_1 \oplus U_2$. Let $\mathcal{T}'$ be the restriction of $\mathcal{T}$ to U_2, so that $\mathcal{T}' : U_2 \to U_2$. Repeat the argument for U_2, etc.

In this way we obtain vectors $w_1, w_2, \ldots, w_k$, with $\mathcal{C} = \{w_1, \ldots, w_k\}$ being a rational canonical $\mathcal{T}$-generating set for V, and from $\mathcal{C}$ we obtain a basis $\mathcal{B}$ of V with $[\mathcal{T}]_{\mathcal{B}}$ the block diagonal matrix whose diagonal blocks are the companion matrices $C(m_{\mathcal{T},w_1}(x)), \ldots, C(m_{\mathcal{T},w_k}(x))$, a matrix in rational canonical form. ◇

5.6 JORDAN CANONICAL FORM

Now let $\mathbb{F}$ be an algebraically closed field, let V be a finite-dimensional vector space over $\mathbb{F}$, and let $\mathcal{T} : V \to V$ be a linear transformation. In this section we show in Theorem 5.6.5 that $\mathcal{T}$ has an essentially unique Jordan canonical form. If $\mathbb{F}$ is not algebraically closed that may or may not be the case. In Theorem 5.6.6 we see the condition on $\mathcal{T}$ that will guarantee that it does. At the end of this section we discuss, though without full proofs, a generalization of Jordan canonical form that always exists (Theorem 5.6.13).

These results in this section are easy to obtain given the hard work we have already done. We begin with some preliminary work, apply Theorem 5.4.6, use rational canonical form, and out pops Jordan canonical form with no further ado!

Lemma 5.6.1. *Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. Suppose that $m_{\mathcal{T}}(x) = c_{\mathcal{T}}(x) = (x-a)^k$. Then V is $\mathcal{T}$-generated by a single element w_1 and V has a basis $\mathcal{B} = \{v_1, \ldots, v_k\}$ where $v_k = w$ and $v_i = (\mathcal{T} - a\mathcal{I})(v_{i+1})$ for $i = 1, \ldots, k-1$.*

Proof. We know that there is an element w of V with $m_{\mathcal{T},w}(x) = m_{\mathcal{T}}(x)$. Then w $\mathcal{T}$-generates a subspace W_1 of V whose dimension is the degree k of $m_{\mathcal{T}}(x)$. By hypothesis $m_{\mathcal{T}}(x) = c_{\mathcal{T}}(x)$, so $c_{\mathcal{T}}(x)$ also has degree k. But the degree $c_{\mathcal{T}}(x)$ is equal to the dimension of V, so $\dim(W_1) = \dim(V)$ and hence $W_1 = V$.

Set $v_k = w$ and for $1 \le i < k$, set $v_i = (\mathcal{T} - a\mathcal{I})^{k-i}(v_k)$. Then $v_i = (\mathcal{T} - a\mathcal{I})^{k-i}(v_k) = (\mathcal{T} - a\mathcal{I})(\mathcal{T} - a\mathcal{I})^{k-i-1}(v_k) = (\mathcal{T} - a\mathcal{I})(v_{i+1})$.

It remains to show that $\mathcal{B} = \{v_1, \ldots, v_k\}$ is a basis. It suffices to show that this set is linearly independent. Suppose that $c_1 v_1 + \cdots + c_k v_k = 0$, i.e., $c_1(\mathcal{T} - a\mathcal{I})^{k-1} v_k + \cdots + c_k v_k = 0$. Then $p(\mathcal{T})(v_k) = 0$ where $p(x) = c_1(x-a)^{k-1} + c_2(x-a)^{k-2} + \cdots + c_k$. Now $p(x)$ is a polynomial of degree at most $k-1$, and $m_{\mathcal{T},v_k}(x) = (x-a)^k$ is of degree k, so $p(x)$ is the zero polynomial. The coefficient of x^{k-1} in $p(x)$ is c_1, so $c_1 = 0$; then the coefficient of x^{k-2} in $p(x)$ is c_2, so $c_2 = 0$, etc. Thus $c_1 = c_2 = \cdots = c_k = 0$ and $\mathcal{B}$ is linearly independent. □

Corollary 5.6.2. *Let $\mathcal{T}$ and $\mathcal{B}$ be as in Lemma 5.6.1. Then*

$$[\mathcal{T}]_{\mathcal{B}} = \begin{bmatrix} a & 1 & & & \\ & a & 1 & & \\ & & \ddots & & \\ & & & & 1 \\ & & & & a \end{bmatrix},$$

a k-by-k matrix with diagonal entries a, entries immediately above the diagonal 1, *and all other entries* 0.

Proof. $(\mathcal{T} - a\mathcal{I})(v_1) = 0$ so $\mathcal{T}(v_1) = v_1$; $(\mathcal{T} - a\mathcal{I})(v_{i+1}) = v_i$ so $\mathcal{T}(v_{i+1}) = v_i + av_{i+1}$, and the result follows from Remark 2.2.8. □

DEFINITION 5.6.3. A basis $\mathcal{B}$ of V as in Corollary 5.6.2 is called a *Jordan basis* of V.

If $V = V_1 \oplus \cdots \oplus V_l$ and V_i has a Jordan basis $\mathcal{B}_i$, then $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_l$ is called a Jordan basis of V. ◇

DEFINITION 5.6.4. (1) A k-by-k matrix

$$\begin{bmatrix} a & 1 & & & \\ & a & 1 & & \\ & & \ddots & & \\ & & & & 1 \\ & & & & a \end{bmatrix}$$

as in Corollary 5.6.2 is called a k-by-k *Jordan block* associated to the eigenvalue a.

(2) A matrix J is said to be in Jordan canonical form if J is a block diagonal matrix

$$J = \begin{bmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_l \end{bmatrix}$$

with each J_i a Jordan block. $\diamond$

Theorem 5.6.5 (Jordan canonical form)**.** *(1) Let $\mathbb{F}$ be an algebraically closed field and let V be a finite-dimensional $\mathbb{F}$-vector space. Let $\mathcal{T} : V \to V$ be a linear transformation. Then V has a basis $\mathcal{B}$ with $[\mathcal{T}]_{\mathcal{B}} = J$ a matrix in Jordan canonical form. J is unique up to the order of the blocks.*

(2) Let $\mathbb{F}$ be an algebraically closed field and let A be an n-by-n matrix with entries in $\mathbb{F}$. Then A is similar to a matrix J in Jordan canonical form. J is unique up to the order of the blocks.

Proof. Let $\mathcal{T}$ have characteristic polynomial

$$c_{\mathcal{T}}(x) = (x - a_1)^{e_1} \cdots (x - a_m)^{e_m}.$$

Then, by Theorem 5.4.6, we have a $\mathcal{T}$-invariant direct sum decomposition $V = V^1 \oplus \cdots \oplus V^m$ where $V^i = \operatorname{Ker}(\mathcal{T} - a_i \mathcal{I})^{e_i}$. Let $\mathcal{T}_i$ be the restriction of $\mathcal{T}$ to V^i. Then, by Theorem 5.5.2, V^i has a rational canonical $\mathcal{T}$-basis $C = \{w_1^i, \ldots, w_{k_i}^i\}$ and a corresponding direct sum decomposition $V^i = W_1^i \oplus \cdots \oplus W_{k_i}^i$. Then each W_j^i satisfies the hypothesis of Lemma 5.6.1, so W_j^i has a Jordan basis $\mathcal{B}_j^i$. Then

$$\mathcal{B} = \mathcal{B}_1^1 \cup \cdots \cup \mathcal{B}_{k_1}^1 \cup \cdots \cup \mathcal{B}_1^m \cup \cdots \cup \mathcal{B}_{k_m}^m$$

is a Jordan basis of V. To see uniqueness, note that there is unique factorization for the characteristic polynomial, and then the uniqueness of each of the block sizes is an immediate consequence of the uniqueness of rational canonical form.

(2) Apply part (1) to the linear transformation $\mathcal{T} = \mathcal{T}_A$. $\square$

We stated Theorem 5.6.5 as we did for emphasis. We have a more general result.

Theorem 5.6.6 (Jordan canonical form)**.** *(1) Let V be a finite-dimensional vector space over a field $\mathbb{F}$ and let $\mathcal{T} : V \to V$ be a linear transformation. Suppose that $c_{\mathcal{T}}(x)$, the characteristic polynomial of $\mathcal{T}$, factors into a* *product of linear factors, $c_{\mathcal{T}}(x) = (x - a_1)^{e_1} \cdots (x - a_m)^{e_m}$. Then V has a basis $\mathcal{B}$ with $[v]_{\mathcal{B}} = J$ a matrix in Jordan canonical form. J is unique up to the order of the blocks.*

(2) Let A be an n-by-n matrix with entries in a field $\mathbb{F}$. Suppose that $c_A(x)$, the characteristic polynomial of A, factors into a product of linear factors, $c_A(x) = (x - a_1)^{e_1} \cdots (x - a_m)^{e_m}$. Then A is similar to a matrix J in Jordan canonical form. J is unique up to the order of the blocks.

Proof. Identical to the proof of Theorem 5.6.5. □

REMARK 5.6.7. Let us look at a couple of small examples. Let $A_1 = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$. Then A_1 is already in Jordan canonical form, but its rational canonical form is $M_1 = \begin{bmatrix} 3 & 1 \\ -2 & 0 \end{bmatrix}$. Let $A_2 = \begin{bmatrix} 3 & 1 \\ 0 & 3 \end{bmatrix}$. Then A_2 is already in Jordan canonical form, but its rational canonical form is $M_2 = \begin{bmatrix} 6 & 1 \\ -9 & 0 \end{bmatrix}$. In both of these two (one diagonalizable, one not) we see that the rational canonical form is more complicated and less informative than the Jordan canonical form, and indeed in most applications it is the Jordan canonical form we are interested in. But, as we have seen, the path to Jordan canonical form goes through rational canonical form. ◇

The question now naturally arises as to what we can say for a linear transformation $\mathcal{T} : V \to V$ where V is a vector space over $\mathbb{F}$ and $c_{\mathcal{T}}(x)$ may not factor into a product of linear factors over $\mathbb{F}$. Note that this makes no difference in the rational canonical form. Although there is not a Jordan canonical form in this case, there is an appropriate generalization. Since it is not so useful, we will only state the results. The proofs are not so different, and we leave them for the reader.

Lemma 5.6.8. *Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. Suppose that $m_{\mathcal{T}}(x) = c_{\mathcal{T}}(x) = p(x)^k$, where $p(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ is an irreducible polynomial of degree d. Then V is $\mathcal{T}$-generated by a single element w, and V has a basis $\mathcal{B} = \{v_1^1, \dots, v_1^d, v_2^1, \dots, v_2^d, \dots, v_k^1, \dots, v_k^d\}$ where $v_k^d = w$ and $\mathcal{T}$ is given as follows: For any j, and for $i > 1$, $\mathcal{T}(v_j^i) = v_j^{i-1}$. For $j = 1$, and for $i = 1$, $\mathcal{T}(v_1^1) = -a_0v_1^1 - a_1v_1^2 - \cdots - a_{d-1}v_1^d$. For $j > 1$, and for $i = 1$, $\mathcal{T}(v_j^1) = -a_0v_j^1 - a_1v_j^2 - \cdots - a_{d-1}v_j^d + v_{j-1}^d$.*

REMARK 5.6.9. This is a direct generalization of Lemma 5.6.1, as if $m_{\mathcal{T}}(x) = c_{\mathcal{T}}(x) = (x - a)^k$, then $d = 1$ so we are in the case $i = 1$. the companion matrix of $p(x) = x - a$ is the 1-by-1 matrix $[a_0] = [-a]$, and then $\mathcal{T}(v_1^1) = av_1^1$ and $\mathcal{T}(v_j^1) = av_j^1 + v_{j-1}^1$ for $j > 1$. ◇

Corollary 5.6.10. *In the situation of Lemma 5.6.8,*

$$[\mathcal{T}]_{\mathcal{B}} = \begin{bmatrix} C & N & & \\ & C & N & \\ & & \ddots & N \\ & & & C \end{bmatrix},$$

where there are k identical d-by-d blocks $C = C(c_{\mathcal{T}}(x))$ along the diagonal, and $(k-1)$ identical d-by-d blocks N immediately above the diagonal, where N is a matrix with an entry of 1 *in row d, column* 1 *and all other entries* 0.

REMARK 5.6.11. If $p(x) = (x - a)$ this is just a k-by-k Jordan block. $\diamond$

DEFINITION 5.6.12. A matrix as in Corollary 5.6.10 is said to be a *generalized Jordan block.* A block diagonal matrix whose diagonal blocks are generalized Jordan blocks is said to be in *generalized Jordan canonical form.* $\diamond$

Theorem 5.6.13 (Generalized Jordan canonical form). *(1) Let V be a finite-dimensional vector space over the field $\mathbb{F}$ and let $c_T(x)$ factor as $c_{\mathcal{T}}(x) = p_1(x)^{e_1} \cdots p_m(x)^{e_m}$ for irreducible polynomials $p_1(x), \dots, p_m(x)$. Then V has a basis $\mathcal{B}$ with $[V]_{\mathcal{B}}$ a matrix in generalized Jordan canonical form. $[V]_{\mathcal{B}}$ is unique up to the order of the generalized Jordan blocks.*

(2) Let A be an n-by-n matrix with entries in $\mathbb{F}$ and let $c_A(x)$ factor as $c_A(x) = p_1(x)^{e_1} \cdots p_m(x)^{e_m}$ for irreducible polynomials $p_1(x), \dots,$ $p_m(x)$. Then A is similar to a matrix in generalized Jordan canonical form. This matrix is unique up to the order of the generalized Jordan blocks.

5.7 An algorithm for Jordan canonical form and Jordan basis

In this section we develop an algorithm to find the Jordan canonical form of a linear transformation, and a Jordan basis, assuming that we can factor the characteristic polynomial into a product of linear factors. (As is well known, there is no general method for doing this.)

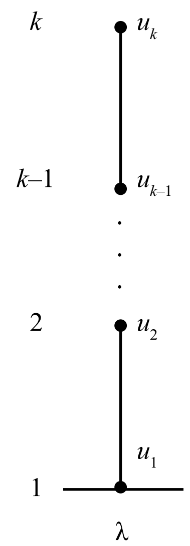
We will proceed by first developing a pictorial encoding of the information we are trying to find. We call this picture the *labelled eigenstructure picture* or *ℓESP,* of the linear transformation.

DEFINITION 5.7.1. Let u_k be a generalized eigenvector of index k corresponding to an eigenvalue λ of a linear transformation $\mathcal{T} : V \to V$. Set $u_{k-1} = (\mathcal{T} - \lambda\mathcal{I})(u_k), u_{k-2} = (\mathcal{T} - \lambda\mathcal{I})(u_{k-1}), \ldots, u_1 = (\mathcal{T} - \lambda\mathcal{I})(u_2)$. Then $\{u_1, \ldots, u_k\}$ is a *chain* of generalized eigenvectors. The vector u_k is the *top* of the chain. $\diamond$

REMARK 5.7.2. If $\{u_1, \ldots, u_k\}$ is a chain as in Definition 5.7.1, then for each $1 \leq i \leq k$, u_i is a generalized eigenvector of index i associated to the eigenvalue λ of $\mathcal{T}$. $\diamond$

REMARK 5.7.3. A chain is entirely determined by the vector u_k at the top. (We will use this observation later: To find a chain, it suffices to find the vector at the top of the chain.) $\diamond$

We now pictorially represent a chain as in Definition 5.7.1 as follows:



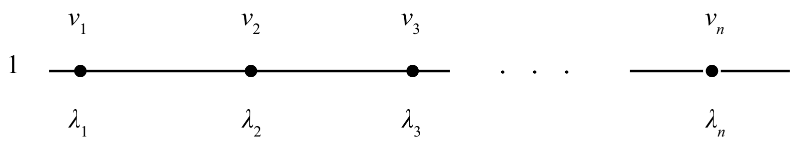
If $\{u_1, \ldots, u_k\}$ forms a Jordan basis for a k-by-k Jordan block for the eigenvalue λ of $\mathcal{T}$, the vectors in this basis form a chain. Conversely, from a chain we can construct a Jordan block, and a Jordan basis.

A general linear transformation will have more than one Jordan block. The ℓESP of a linear transformation is the picture we obtain by putting its chains side by side.

The *eigenstructure picture*, or *ESP*, of a linear transformation, is obtained from the ℓESP by erasing the labels. We will usually think about this the other way: We will think of obtaining the ℓESP from the *ESP* by putting the labels in. From the Jordan canonical form of a linear transformation we can determine its *ESP*, and conversely. Although the *ESP* has less information than the ℓESP, it is easier to determine.

The opposite extreme from the situation of a linear transformation whose Jordan canonical form has a single Jordan block is a diagonalizable linear transformation.

Suppose $\mathcal{T}$ is diagonalizable with eigenvalues $\lambda_1, \ldots, \lambda_n$ (not necessarily distinct) and a basis $\{v_1, \ldots, v_n\}$ of associated eigenvectors. Then $\mathcal{T}$ has ℓESP



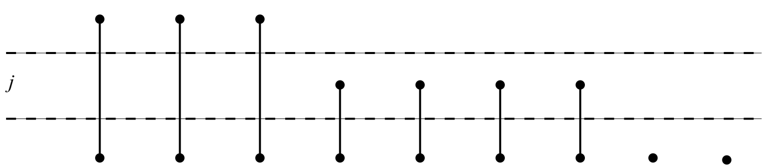
We have shown that the Jordan canonical form of a linear transformation is unique up to the order of the blocks, so we see that the *ESP* of a linear transformation is unique up to the order of the chains. As Jordan bases are not unique, neither is the ℓESP.

The ℓESP is easier to illustrate by example than to define formally. We have just given two general examples. For a concrete example we advise the reader to look at the beginning of Example 5.7.7.

We now present our algorithm for determining the Jordan canonical form of a linear transformation. Actually, the algorithm we present will be an algorithm for *ESP*.

To find the *ESP* of $\mathcal{T}$ what we need to find is the positions of the nodes at the top of chains. We envision starting at the top, i.e., the highest index, and working our way down. From this point of view, the nodes we encounter at the top of chains are "new" nodes, while nodes that are not at the top of chains come from nodes we have already seen, and we regard them as "old" nodes.

Let us now imagine ourselves in the middle of this process, say at height (= index) j, and suppose we see part of the *ESP* of $\mathcal{T}$ for the eigenvalue λ:



Each node in the ESP represents a vector in the generalized eigenspace E_λ^∞, and together these vectors are a basis for E_λ^∞. More precisely, the vectors corresponding to the nodes at height j or less form a basis for E_λ^j, the subspace of E_λ^∞ consisting of eigenvectors of index at most j (as well as the 0 vector). Thus if we let $d_j(\lambda)$ be the number of nodes at height at most j, then

$$d_j(\lambda) = \dim E_\lambda^j.$$

As a first step toward finding the number of new nodes at index j, we want to find the number of all nodes at this index. If we let $d_j^{\text{ex}}(\lambda)$ denote the number of nodes exactly at level j, then

$$d_j^{\text{ex}}(\lambda) = d_j(\lambda) - d_{j-1}(\lambda).$$

(That is, the number of nodes at height exactly j is the number of nodes at height at most j minus the number of nodes at height at most $j-1$.)

We want to find $d_j^{\text{new}}(\lambda)$, the number of new nodes at height j. Every node at height j is either new or old, so the number of new nodes at height j is

$$d_j^{\text{new}}(\lambda) = d_j^{\text{ex}}(\lambda) - d_{j+1}^{\text{ex}}(\lambda)$$

as every old node at height j comes from a node at height $j+1$, and there are exactly $d_{j+1}^{\text{ex}}(\lambda)$ of those.

This gives our algorithm:

Algorithm 5.7.4. *Let λ be an eigenvalue of $\mathcal{T} : V \to V$.*

Step 1. *For $j = 1, 2, \ldots,$ compute*

$$d_j(\lambda) = \dim E_\lambda^j = \dim(\operatorname{Ker}(\mathcal{T} - \lambda\mathcal{I})^j).$$

Stop when $d_j(\lambda) = d_\infty(\lambda) = \dim E_\lambda^\infty$. Recall from Lemma 4.2.4 that $d_\infty(\lambda) = \text{alg-mult}(\lambda)$. Denote this value of j by $j_{\max}(\lambda)$. (Note also that $j_{\max}(\lambda)$ is the smallest value of j for which $d_j(\lambda) = d_{j-1}(\lambda)$.)

Step 2. *For $j = 1, \ldots, j_{\max}(\lambda)$ compute $d_j^{\text{ex}}(\lambda)$ by*

$$d_1^{\text{ex}}(\lambda) = d_1(\lambda),$$
$$d_j^{\text{ex}}(\lambda) = d_j(\lambda) - d_{j-1}(\lambda) \quad \textit{for } j > 1.$$

Step 3. *For* $j = 1, \ldots, j_{\max}(\lambda)$ *compute* $d_j^{\mathrm{new}}(\lambda)$ *by*

$$d_j^{\mathrm{new}}(\lambda) = d_j^{\mathrm{ex}}(\lambda) - d_{j+1}^{\mathrm{ex}}(\lambda) \qquad \textit{for } j < j_{\max}(\lambda),$$
$$d_j^{\mathrm{new}}(\lambda) = d_j^{\mathrm{ex}}(\lambda) \quad \textit{for} \quad j = j_{\max}(\lambda).$$

We now refine our argument to use it to find a Jordan basis for a linear transformation. The algorithm we present will be an algorithm for ℓ*ESP*, but since we already know how to find the *ESP,* it is now just a matter of finding the labels.

Again we us imagine ourselves in the middle of this process, at height j for the eigenvalue λ. The vectors labelling the nodes at height at most j form a basis for E_λ^j and the vectors labelling the nodes at height at most $j-1$ form a basis for E_λ^{j-1}. Thus the vectors labelling the nodes at height exactly j are a basis for a subspace F_λ^j of E_λ^j that is complementary to E_λ^{j-1}. But cannot be any subspace, as it must contain the old nodes at height j, which come from one level higher, i.e., from a subspace F_λ^{j+1} of E_λ^{j+1} that is complementary to E_λ^j. But that is the only condition on the complement F_λ^j, and since we are working our way down and are at level j, we may assume we have successfully chosen a complement F_λ^{j+1} at level $j+1$.

With a bit more notation we can describe our algorithm. Let us denote the space spanned by the old nodes at height j by A_λ^j. (We use A because it is the initial letter of alt, the German word for old. We cannot use O for typographical reasons.) The nodes in A_λ^j come from nodes at height $j+1$, but we already know what these are: they are in F_λ^{j+1}. Thus we set $A_\lambda^j = (\mathcal{T} - \lambda\mathcal{I})(F_\lambda^{j+1})$. Then A_λ^j and E_λ^{j-1} are both subspaces of E_λ^j, and in fact they are independent subspaces, as any nonzero vector in A_λ^j has height j and any nonzero vector in E_λ^{j-1} has height at most $j-1$. We then choose N_λ^j to be any complement of $E_\lambda^{j-1} \oplus A_\lambda^j$ in E_λ^j. (For $j = 1$ the situation is a little simpler, as we simply choose N_λ^j to be a complement of A_λ^j in E_λ^j.)

This is a space of new (or, in German, neu) vectors at height j and is precisely the space we are looking for. We choose a basis for N_λ^j and label the new nodes at height j with the elements of this basis. In practice, we usually find N_λ^j as follows: We find a basis $\mathcal{B}_1$ of E_λ^{j-1}, a basis $\mathcal{B}_2$ of A_λ^j, and extend $\mathcal{B}_1 \cup \mathcal{B}_2$ to a basis $\mathcal{B}$ of E_λ^j. Then $\mathcal{B} - (\mathcal{B}_1 \cup \mathcal{B}_2)$ is a basis of N_λ^j. So actually we will find the basis of N_λ^j directly, and that is the information we need. Finally, we have just obtained $E_\lambda^j = E_\lambda^{j-1} \oplus A_\lambda^j \oplus N_\lambda^j$

so we set $F_\lambda^j = A_\lambda^j \oplus N_\lambda^j$ and we are finished at height j and ready to drop down to height $j-1$. (When we start at the top, for $j = j_{\max}(\lambda)$, the situation is easier. At the top there can be no old vectors, so for $j = j_{\max}$ we simply have $E_\lambda^j = E_\lambda^{j-1} \oplus N_\lambda^j$ and $F_\lambda^j = N_\lambda^j$.)

We summarize our algorithm as follows:

Algorithm 5.7.5. *Let λ be an eigenvalue of $\mathcal{T} : V \to V$.*

Step 1. *For $j = 1, 2, \ldots, j_{\max}(\lambda)$ find the subspace $E_\lambda^j = \operatorname{Ker}((\mathcal{T} - \lambda \mathcal{I})^j)$.*

Step 2. *For $j = j_{\max}(\lambda), \ldots, 2, 1$:*

(a) If $j = j_{\max}(\lambda)$, let N_λ^j be any complement of E_λ^{j-1} in E_λ^j. If $j < j_{\max}(\lambda)$, let $A_\lambda^j = (\mathcal{T} - \lambda \mathcal{I})(F_\lambda^{j+1})$. Let N_λ^j be any complement of $E_\lambda^{j-1} \oplus A_\lambda^j$ in E_λ^j if $j > 1$, and let N_λ^j be any complement of A_λ^j in E_λ^j if $j = 1$.

(b) Label the new nodes at height j with a basis of N_λ^j.

(c) Let $F_\lambda^j = A_\lambda^j \oplus N_\lambda^j$.

There is one more point we need to clear up to make sure this algorithm works. We know from our results on Jordan canonical form that there is some Jordan basis for A, i.e., some labelling so that the ℓESP is correct. We have made some choices, in choosing our complements N_λ^j, and in choosing our basis for N_λ^j. But we can see that these choices all yield the same *ESP* (and hence one we know is correct.) For the dimensions of the various subspaces are all determined by the Jordan canonical form of A, or equivalently by its *ESP*, and different choices of bases or complements will yield spaces of the same dimension.

REMARK 5.7.6. There are lots of choices here. Complements are almost never unique, and bases are never unique except for the vector space $\{0\}$. But no matter what choice we make, we get labels for the ESP and hence Jordan bases for V. (It is no surprise that a Jordan basis is not unique.) $\diamond$

In finding the ℓESP (or, equivalently, in finding a Jordan basis), it is essential that we work from the top down and not from the bottom up. If we try to work from the bottom up, we have to make arbitrary choices and we have no way of knowing if they are correct. Since they almost certainly won't be, something we would only find out at a later (perhaps much later) stage, we would have to go back and modify them, and this rapidly becomes an unwieldy mess.

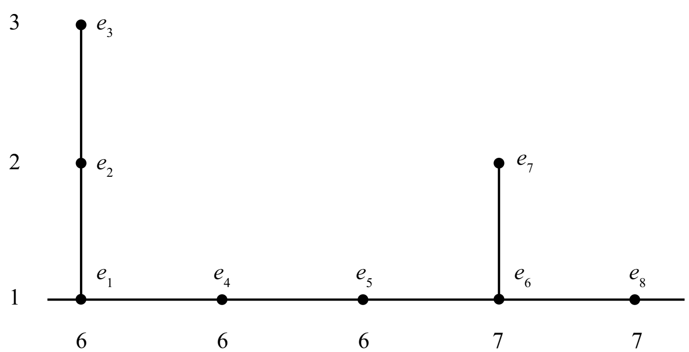
We recall that if A is a matrix and $\mathcal{B}$ is a Jordan basis for V, then $A = PJP^{-1}$ where J is the Jordan canonical form of A and P is the matrix whose columns consist of the vectors in $\mathcal{B}$ (taken in the corresponding order).

EXAMPLE 5.7.7. Here is an example for a matrix that is already in Jordan canonical form. We present it to illustrate all of the various subspaces we have introduced, before we move on to some highly nontrivial examples. Let

$$A = \begin{bmatrix} 6 & 1 & 0 & & & & & \\ 0 & 6 & 1 & & & & & \\ 0 & 0 & 6 & & & & & \\ & & & 6 & & & & \\ & & & & 6 & & & \\ & & & & & 7 & 1 & \\ & & & & & 0 & 7 & \\ & & & & & & & 7 \end{bmatrix},$$

with characteristic polynomial $c_A(x) = (x-6)^5(x-7)^3$.

We can see immediately that A has ℓESP



$E_6^1 = \operatorname{Ker}(A-6I)$ has dimension 3, with basis $\{e_1, e_4, e_5\}$.

$E_6^2 = \operatorname{Ker}(A-6I)^2$ has dimension 4, with basis $\{e_1, e_2, e_4, e_5\}$.

$E_6^3 = \operatorname{Ker}(A-6I)^3$ has dimension 5, with basis $\{e_1, e_2, e_3, e_4, e_5\}$.

$E_7^1 = \operatorname{Ker}(A-7I)$ has dimension 2, with basis $\{e_6, e_8\}$.

$E_7^2 = \operatorname{Ker}(A-7I)^2$ has dimension 3, with basis $\{e_6, e_7, e_8\}$.

Thus

$$d_1(6) = 3, \qquad d_2(6) = 4, \qquad d_3(6) = 5,$$

so

$$d_1^{\mathrm{ex}}(6) = 3, \qquad d_2^{\mathrm{ex}}(6) = 4 - 3 = 1, \qquad d_3^{\mathrm{ex}}(6) = 5 - 4 = 1,$$

and

$$d_1^{\mathrm{new}}(6) = 3 - 1 = 2, \qquad d_2^{\mathrm{new}}(6) = 1 - 1 = 0, \qquad d_3^{\mathrm{new}}(6) = 1.$$

Also

$$d_1(7) = 2, \qquad d_2(7) = 3,$$

so

$$d_1^{\mathrm{ex}}(7) = 2, \qquad d_2^{\mathrm{ex}}(7) = 3 - 2 = 1,$$

and

$$d_1^{\mathrm{new}}(7) = 2 - 1 = 1, \qquad d_2^{\mathrm{new}}(7) = 1,$$

and we recover that A has 1 3-by-3 block and 2 1-by-1 blocks for the eigenvalue 6, and 1 2-by-2 block and 1 1-by-1 block for the eigenvalue 7.

Furthermore,

$$E_6^2 \quad \text{has a complement in } E_6^3 \text{ of } N_6^3 \text{ with basis } \{e_3\}.$$

Set $F_6^3 = N_6^3$ with basis $\{e_3\}$.

$A_6^2 = (A - 6I)(F_6^3)$ has basis $\{e_2\}$, and $E_6^1 \oplus A_6^2$ has complement in E_6^2 of $N_6^2 = \{0\}$ with empty basis. Set

$$F_6^2 = A_6^2 \oplus N_6^2 \text{ with basis } \{e_2\}.$$

$A_6^1 = (A - 6I)(F_6^2)$ has basis $\{e_1\}$, and A_6^1 has complement in E_6^1 of N_6^1 with basis $\{e_4, e_5\}$.

Also

$$E_7^1 \quad \text{has complement in } E_7^2 \text{ of } N_7^2 \text{ with basis } \{e_7\}.$$

Set $F_7^2 = N_7^2$ with basis $\{e_7\}$.

$A_7^1 = (A - 7I)(F_7^2)$ has basis $\{e_6\}$, and A_7^1 has complement in E_7^1 of N_7^1 with basis $\{e_8\}$.

Thus we recover that e_3 is at the top of a chain of height 3 for the eigenvalue 6, e_4 and e_5 are each at the top of a chain of height 1 for the eigenvalue 6, e_7 is at the top of a chain of height 2 for the eigenvalue 7, and e_8 is at the top of a chain of height 1 for the eigenvalue 7.

Finally, since $e_2 = (A - 6I)(e_3)$ and $e_1 = (A - 6I)(e_2)$, and $e_6 = (A-7I)(e_7)$, we recover that $\{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8\}$ is a Jordan basis. $\diamond$

EXAMPLE 5.7.8. We present a pair of (rather elaborate) examples to illustrate our algorithm.

(1) Let A be the 8-by-8 matrix

$$A = \begin{bmatrix} 3 & 3 & 0 & 0 & 0 & -1 & 0 & 2 \\ -3 & 4 & 1 & -1 & -1 & 0 & 1 & -1 \\ 0 & 6 & 3 & 0 & 0 & -2 & 0 & -4 \\ -2 & 4 & 0 & 1 & -1 & 0 & 2 & -5 \\ -3 & 2 & 1 & -1 & 2 & 0 & 1 & -2 \\ -1 & 1 & 0 & -1 & -1 & 3 & 1 & -1 \\ -5 & 10 & 1 & -3 & -2 & -1 & 6 & -10 \\ -3 & 2 & 1 & -1 & -1 & 0 & 1 & 1 \end{bmatrix}$$

with characteristic polynomial $c_A(x) = (x-3)^7(x-2)$.

The eigenvalue $\lambda = 2$ is easy to deal with. We know without any further computation that $d_1(2) = d_\infty(2) = 1$ and that $\operatorname{Ker}(A - 2I)$ is 1-dimensional.

For the eigenvalue $\lambda = 3$, computation shows that $A - 3I$ has rank 5, so $\operatorname{Ker}(A - 3I)$ has dimension 3 and $d_1(3) = 3$. Further computation shows that $(A - 3I)^2$ has rank 2, so $\operatorname{Ker}(A - 3I)^2$ has dimension 6 and $d_2(3) = 6$. Finally, $(A - 3I)^3$ has rank 1, so $\operatorname{Ker}(A - 3I)^3$ has dimension 7 and $d_3(3) = d_\infty(3) = 7$.

At this point we can conclude that A has minimum polynomial $m_A(x) = (x-3)^3(x-2)$.

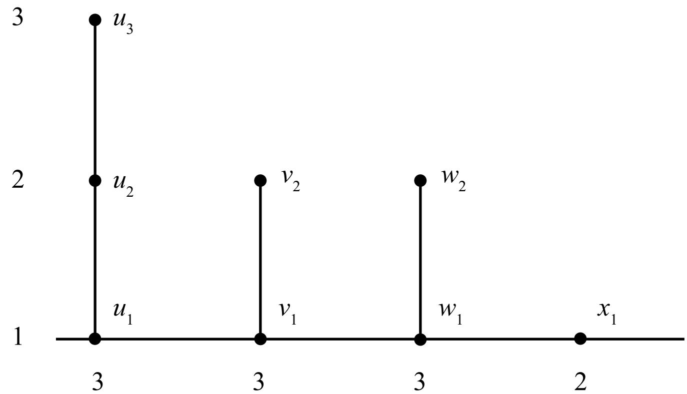
We can also determine the ESP of A. We have

$$\begin{aligned} d_1^{\text{ex}}(3) &= d_1(3) = 3 \\ d_2^{\text{ex}}(3) &= d_2(3) - d_1(3) = 6 - 3 = 3 \\ d_3^{\text{ex}}(3) &= d_3(3) - d_2(3) = 7 - 6 = 1 \end{aligned}$$

and then

$$\begin{aligned} d_3^{\text{new}}(3) &= d_3^{\text{ex}}(3) = 1 \\ d_2^{\text{new}}(3) &= d_2^{\text{ex}}(3) - d_3^{\text{ex}}(3) = 3 - 1 = 2 \\ d_1^{\text{new}}(3) &= d_1^{\text{ex}}(3) - d_2^{\text{ex}}(3) = 3 - 3 = 0. \end{aligned}$$

Thus we see that for the eigenvalue 3, we have one new node at level 3, two new nodes at level 2, and no new nodes at level 1. Hence A has ℓESP



with the labels yet to be determined, and thus A has Jordan canonical form

$$J = \begin{bmatrix} 3 & 1 & 0 & & & & & \\ 0 & 3 & 1 & & & & & \\ 0 & 0 & 3 & & & & & \\ & & & 3 & 1 & & & \\ & & & 0 & 3 & & & \\ & & & & & 3 & 1 & \\ & & & & & 0 & 3 & \\ & & & & & & & 2 \end{bmatrix}.$$

Now we find a Jordan basis.

Equivalently, we find the values of the labels. Once we have the labels u_3, v_2, w_2, and x_1 on the new nodes, the others are determined.

The vector x_1 is easy to find. It is any eigenvector corresponding to the eigenvalue 2. Computation reveals that we may choose

$$x_1 = \begin{bmatrix} 30 \\ -12 \\ 68 \\ 18 \\ 1 \\ -4 \\ 66 \\ 1 \end{bmatrix}.$$

The situation for the eigenvalue 3 is more interesting. We compute that

$$\mathrm{Ker}(A-3I)^3 \text{ has basis } \left\{ \begin{bmatrix}1\\0\\0\\0\\0\\0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\\0\\0\\0\\0\\1\end{bmatrix}, \begin{bmatrix}0\\0\\1\\0\\0\\0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\0\\1\\0\\0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\0\\0\\1\\0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\0\\0\\0\\1\\0\\0\end{bmatrix} \begin{bmatrix}0\\0\\0\\0\\0\\0\\1\\0\end{bmatrix} \right\},$$

$$\mathrm{Ker}(A-3I)^2 \text{ has basis } \left\{ \begin{bmatrix}1\\0\\2\\0\\0\\0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\\0\\0\\0\\0\\1\end{bmatrix}, \begin{bmatrix}0\\0\\0\\1\\0\\0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\0\\0\\1\\0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\0\\0\\0\\1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\0\\0\\0\\0\\1\\0\end{bmatrix} \right\},$$

$$\text{and } \mathrm{Ker}(A-3I) \text{ has basis } \left\{ \begin{bmatrix}1\\0\\2\\0\\0\\0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\\0\\1\\1\\1\\1\end{bmatrix}, \begin{bmatrix}0\\0\\0\\1\\0\\0\\1\\0\end{bmatrix} \right\}.$$

For u_3 we may choose any vector $u_3 \in \mathrm{Ker}(A-3I)^3$, $u_3 \notin \mathrm{Ker}(A-3I)^2$. Inspection reveals that we may choose

$$u_3 = \begin{bmatrix}1\\0\\0\\0\\0\\0\\0\\0\end{bmatrix}.$$

Then

$$u_2 = (A - 3I)u_3 = \begin{bmatrix} 0 \\ -3 \\ 0 \\ -2 \\ -3 \\ -1 \\ -5 \\ -3 \end{bmatrix} \quad \text{and} \quad u_1 = (A - 3I)u_2 = \begin{bmatrix} -2 \\ 0 \\ -4 \\ 0 \\ 0 \\ 0 \\ -2 \\ 0 \end{bmatrix}.$$

For v_2, w_2 we may choose any two vectors in $\operatorname{Ker}(A - 3I)^2$ such that the set of six vectors consisting of these two vectors, u_2, and the given three vectors in our basis of $\operatorname{Ker}(A - 3I)$ are linearly independent. Computation reveals that we may choose

$$v_2 = \begin{bmatrix} 1 \\ 0 \\ 2 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad \text{and} \quad w_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

Then

$$v_1 = (A - 3I)v_2 = \begin{bmatrix} 0 \\ -1 \\ 0 \\ -2 \\ -1 \\ -1 \\ -3 \\ -1 \end{bmatrix} \quad \text{and} \quad w_1 = (A - 3I)w_2 = \begin{bmatrix} 1 \\ 0 \\ 2 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Then

$$\{u_1, u_2, u_3, v_1, v_2, w_1, w_2, x_1\}$$
$$= \left\{ \begin{bmatrix} -2 \\ 0 \\ -4 \\ 0 \\ 0 \\ 0 \\ -2 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ -3 \\ 0 \\ -2 \\ -3 \\ -1 \\ -5 \\ -3 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ -1 \\ 0 \\ -2 \\ -1 \\ -1 \\ -3 \\ -1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 2 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 2 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 30 \\ -12 \\ 68 \\ 18 \\ 1 \\ -4 \\ 66 \\ 1 \end{bmatrix} \right\}$$

is a Jordan basis. $\diamond$

(2) Let A be the 8-by-8 matrix

$$A = \begin{bmatrix} 3 & 1 & 0 & 0 & 0 & 0 & 0 & -1 \\ 3 & 4 & 1 & -1 & -1 & 1 & -3 & 3 \\ -1 & 0 & 3 & 1 & 2 & -2 & 6 & -1 \\ 6 & 0 & 0 & 2 & 0 & 0 & 0 & 6 \\ 1 & -1 & 0 & 0 & 4 & 0 & 0 & 1 \\ 3 & -1 & -2 & 0 & 4 & 0 & 12 & 3 \\ 1 & 0 & -1 & 0 & 2 & -2 & 10 & 1 \\ 4 & -1 & 0 & -1 & 0 & 0 & 0 & 8 \end{bmatrix}$$

with characteristic polynomial $c_A(x) = (x-4)^6(x-5)^2$.

For the eigenvalue $\lambda = 5$, we compute that $A - 5I$ has rank 7, so $\operatorname{Ker}(A - 5I)$ has dimension 1 and hence $d_1(5) = 1$, and also that $\operatorname{Ker}(A - 5I)^2$ has dimension 2 and hence $d_2(5) = d_\infty(5) = 2$.

For the eigenvalue $\lambda = 4$, we compute that $A - 4I$ has rank 5, so $\operatorname{Ker}(A-4I)$ has dimension 3 and hence $d_1(4) = 3$, that $(A-4I)^2$ has rank 4, so $\operatorname{Ker}(A-4I)^2$ has dimension 4 and hence $d_2(4) = 4$, that $(A-4I)^3$ has rank 3, so $\operatorname{Ker}(A-4I)^3$ has dimension 5 and hence that $d_3(4) = 5$ and that $(A-4I)^4$ has rank 2, so $\operatorname{Ker}(A-4I)^4$ has dimension 6 and hence that $d_4(4) = d_\infty(4) = 6$.

Thus we may conclude that $m_A(x) = (x-4)^4(x-5)^2$.

Furthermore

$$\begin{aligned}
d_1^{\text{ex}}(4) &= d_1(4) = 3\\
d_2^{\text{ex}}(4) &= d_2(4) - d_1(4) = 4 - 3 = 1\\
d_3^{\text{ex}}(4) &= d_3(4) - d_2(4) = 5 - 4 = 1\\
d_4^{\text{ex}}(4) &= d_4(4) - d_3(4) = 6 - 5 = 1
\end{aligned}$$

and then

$$\begin{aligned}
d_4^{\text{new}}(4) &= d_4^{\text{ex}} = 1\\
d_3^{\text{new}}(4) &= d_3^{\text{ex}}(4) - d_4^{\text{ex}}(4) = 1 - 1 = 0\\
d_2^{\text{new}}(4) &= d_2^{\text{ex}}(4) - d_3^{\text{ex}}(4) = 1 - 1 = 0\\
d_1^{\text{new}}(4) &= d_1^{\text{ex}}(4) - d_2^{\text{ex}}(4) = 3 - 1 = 2.
\end{aligned}$$

Also

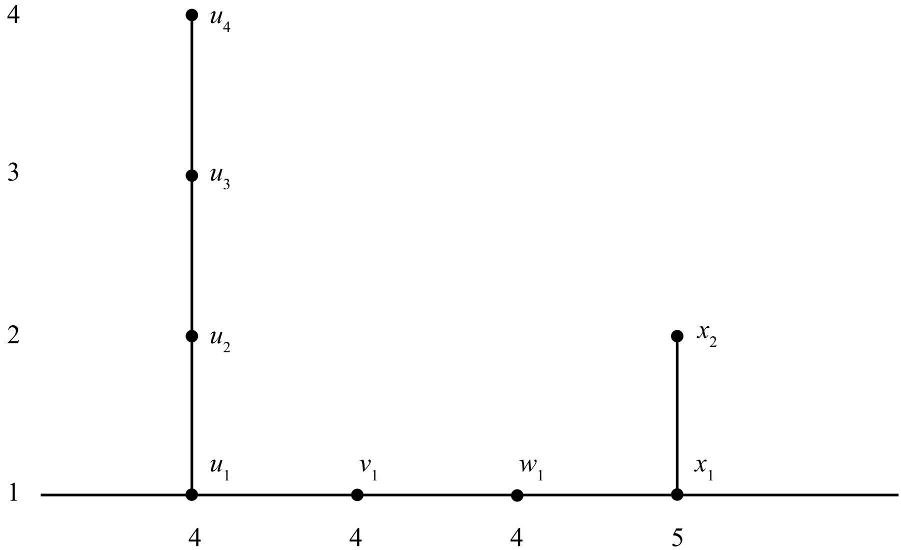
$$\begin{aligned}
d_1^{\text{ex}}(5) &= d_1(5) = 1\\
d_2^{\text{ex}}(5) &= d_2(5) - d_1(5) = 2 - 1 = 1
\end{aligned}$$

and then

$$\begin{aligned}
d_2^{\text{new}}(5) &= d_2^{\text{ex}}(5) = 1\\
d_1^{\text{new}}(5) &= d_1^{\text{ex}}(5) - d_2^{\text{ex}}(5) = 1 - 1 = 0.
\end{aligned}$$

Hence A has ℓESP as on the next page with the labels yet to be determined. In any case A has Jordan canonical form

$$\begin{bmatrix}
4 & 1 & 0 & 0 & & & & \\
0 & 4 & 1 & 0 & & & & \\
0 & 0 & 4 & 1 & & & & \\
0 & 0 & 0 & 4 & & & & \\
 & & & & 4 & & & \\
 & & & & & 4 & & \\
 & & & & & & 5 & 1\\
 & & & & & & 0 & 5
\end{bmatrix}.$$



Now we find the labels. $\operatorname{Ker}(A-4I)^4$ has basis

$$\left\{\begin{bmatrix}1\\0\\0\\0\\0\\0\\0\\-1\end{bmatrix},\begin{bmatrix}0\\1\\0\\0\\0\\0\\0\\0\end{bmatrix},\begin{bmatrix}0\\0\\0\\3\\0\\0\\0\\1\end{bmatrix},\begin{bmatrix}0\\0\\6\\0\\0\\0\\1\\0\end{bmatrix},\begin{bmatrix}0\\0\\0\\0\\3\\0\\-1\\0\end{bmatrix},\begin{bmatrix}0\\0\\0\\0\\0\\3\\1\\0\end{bmatrix}\right\},$$

$\operatorname{Ker}(A-4I)^3$ has basis

$$\left\{\begin{bmatrix}1\\0\\0\\0\\0\\0\\0\\-1\end{bmatrix},\begin{bmatrix}0\\1\\0\\0\\0\\0\\0\\0\end{bmatrix},\begin{bmatrix}0\\0\\6\\0\\0\\0\\1\\0\end{bmatrix},\begin{bmatrix}0\\0\\0\\0\\3\\0\\-1\\0\end{bmatrix},\begin{bmatrix}0\\0\\0\\0\\0\\3\\1\\0\end{bmatrix}\right\},$$

$\mathrm{Ker}(A-4I)^2$ has basis

$$\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 3 \\ 1 \\ 0 \end{bmatrix} \right\},$$

and $\mathrm{Ker}(A-4I)$ has basis

$$\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 3 \\ 1 \\ 0 \end{bmatrix} \right\}.$$

Also, $A-5I^2$ has basis

$$\left\{ \begin{bmatrix} 0 \\ 1 \\ 0 \\ 2 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 2 \\ 1 \\ 0 \end{bmatrix} \right\},$$

and $\mathrm{Ker}(A-5I)$ has basis

$$\left\{ \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 2 \\ 1 \\ 0 \end{bmatrix} \right\}.$$

We may choose for u_4 any vector in $\mathrm{Ker}(A - 4I)^4$ that is not in $\mathrm{Ker}(A - 4I)^3$. We choose

$$u_4 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 3 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \qquad \text{so } u_3 = (A - 4I)u_4 = \begin{bmatrix} -1 \\ 0 \\ 2 \\ 0 \\ 1 \\ 3 \\ 1 \\ 1 \end{bmatrix},$$

$$u_2 = (A - 4I)u_3 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad u_1 = (A - 4I)u_2 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ -1 \\ -1 \\ 0 \\ -1 \end{bmatrix}.$$

Then we may choose v_1 and w_1 to be any two vectors such that u_1, v_1, and w_1 form a basis for $\mathrm{Ker}(A - 4I)$. We choose

$$v_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -1 \end{bmatrix} \quad \text{and} \quad w_1 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 3 \\ 1 \\ 0 \end{bmatrix}.$$

We may choose x_2 to be any vector in $\mathrm{Ker}(A - 5I)^2$ that is not in $\mathrm{Ker}(A - 5I)$. We choose

$$x_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 2 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \quad \text{so} \quad x_1 = (A - 5I)x_2 = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 2 \\ 1 \\ 0 \end{bmatrix}.$$

Thus we obtain a Jordan basis

$$\{u_1, u_2, u_3, u_4, v_1, w_1, x_1, x_2\} = \left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ -1 \\ -1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} -1 \\ 0 \\ 2 \\ 0 \\ 1 \\ 3 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 3 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 3 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 2 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 2 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \right\}.$$

5.8 FIELD EXTENSIONS

Suppose we have an n-by-n matrix A with entries in $\mathbb{F}$ and suppose we have an extension field $\mathbb{E}$ of $\mathbb{F}$. An extension field is a field $\mathbb{E} \supseteq \mathbb{F}$. For example, we might have $\mathbb{E} = \mathbb{C}$ and $\mathbb{F} = \mathbb{R}$. If A is similar over $\mathbb{F}$ to another matrix B, i.e., $B = PAP^{-1}$ where P has entries in $\mathbb{F}$, then A is similar to B over $\mathbb{E}$ by the same equation $B = PAP^{-1}$, since the entries of P, being in $\mathbb{F}$, are certainly in $\mathbb{E}$. (Furthermore, P is invertible over $\mathbb{F}$ if and only if it is invertible over $\mathbb{E}$, as we see from the condition that P is invertible if and only if $\det(P) \neq 0$.) But a priori, the converse may not be true. A priori, A might be similar to B over $\mathbb{E}$, i.e., there may be a matrix Q with entries in $\mathbb{E}$ with $B = QAQ^{-1}$, though there may be no matrix P with entries in $\mathbb{F}$ with $B = PAP^{-1}$. In fact, this does not occur: A and B are similar over $\mathbb{F}$ if and only if they are similar over some (and hence over any) extension field $\mathbb{E}$ of $\mathbb{F}$.

Lemma 5.8.1. *Let $\{v_1, \ldots, v_k\}$ be vectors in $\mathbb{F}^n$ and let $\mathbb{E}$ be an extension of $\mathbb{F}$. Then $\{v_1, \ldots, v_k\}$ is linearly independent over $\mathbb{F}$ (i.e., the equation $c_1v_1 + \cdots + c_kv_k = 0$ with each $c_i \in \mathbb{F}$ only has the solution $c_1 = \cdots = c_k = 0$) if and only if it is linearly independent over $\mathbb{E}$ (i.e., the equation $c_1v_1 + \cdots + c_kv_k = 0$ with each $c_i \in \mathbb{E}$ only has the solution $c_1 = \cdots = c_k = 0$).*

Proof. Certainly if $\{v_1, \ldots, v_k\}$ is linearly independent over $\mathbb{E}$, it is linearly independent over $\mathbb{F}$.

Suppose now that $\{v_1, \ldots, v_k\}$ is linearly independent over $\mathbb{F}$. Then $\{v_1, \ldots, v_k\}$ extends to a basis $\{v_1, \ldots, v_n\}$ of $\mathbb{F}^n$. Let $\mathcal{E} = \{e_1, \ldots, e_n\}$ be the standard basis of $\mathbb{F}^n$. It is the standard basis of $\mathbb{E}^n$ as well. Since

$\{v_1, \ldots, v_n\}$ is a basis, the matrix $P = [[v_1]_{\mathcal{E}}|\cdots|[v_n]_{\mathcal{E}}]$ is nonsingular when viewed as a matrix over $\mathbb{F}$. That means $\det(P) \neq 0$. If we view P as a matrix over $\mathbb{E}$, P remains nonsingular as $\det(P) \neq 0$. ($\det(P)$ is computed purely from the entries of P.) Then $\{v_1, \ldots, v_n\}$ is a basis for V over $\mathbb{E}$, so $\{v_1, \ldots, v_k\}$ is linearly independent over $\mathbb{E}$. $\square$

Lemma 5.8.2. *Let A be an n-by-n matrix over $\mathbb{F}$, and let $\mathbb{E}$ be an extension of $\mathbb{F}$.*

(1) For any $v \in \mathbb{F}^n$, $m_{A,v}(x) = \widetilde{m}_{A,v}(x)$ where $m_{A,v}(x)$ (respectively $\widetilde{m}_{A,v}(x)$) is the A-annihilator of v regarded as an element of $\mathbb{F}^n$ (respectively of $\mathbb{E}^n$).

(2) $m_A(x) = \widetilde{m}_A(x)$ where $m_A(x)$ (respectively $\widetilde{m}_A(x)$) is the minimum polynomial of A regarded as a matrix over $\mathbb{F}$ (respectively over $\mathbb{E}$).

(3) $c_A(x) = \widetilde{c}_A(x)$ where $c_A(x)$ (resp. $\widetilde{c}_A(x)$) is the characteristic polynomial of A regarded as a matrix over $\mathbb{F}$ (resp. over $\mathbb{E}$).

Proof. (1) $\widetilde{m}_{A,v}(x)$ divides any polynomial $p(x)$ with coefficients in $\mathbb{E}$ for which $p(A)(v) = 0$ and $m_{A,v}(x)$ is such a polynomial (as its coefficients lie in $\mathbb{F} \subseteq \mathbb{E}$). Thus $\widetilde{m}_{A,v}(x)$ divides $m_{A,v}(x)$.

Let $m_{A,v}(x)$ have degree d. Then $\{v, Av, \ldots, A^{d-1}v\}$ is linearly independent over $\mathbb{F}$, and hence, by Lemma 5.8.1, over $\mathbb{E}$ as well, so $\widetilde{m}_{A,v}(x)$ has degree at least d. But then $\widetilde{m}_{A,v}(x) = \widetilde{m}_{A,v}(x)$.

(2) Again, $\widetilde{m}_A(x)$ divides $m_A(x)$. There is a vector v in $\mathbb{F}^n$ with $m_A(x) = m_{A,v}(x)$. By (1), $\widetilde{m}_{A,v}(x) = m_{A,v}(x)$. But $\widetilde{m}_{A,v}(x)$ divides $\widetilde{m}_A(x)$, so they are equal.

(3) $c_A(x) = \det(xI - A) = \widetilde{c}_A(x)$ as the determinant is computed purely from the entries of A. $\square$

Theorem 5.8.3. *Let A and B be n-by-n matrices over $\mathbb{F}$ and let $\mathbb{E}$ be an extension field of $\mathbb{F}$. Then A and B are similar over $\mathbb{E}$ if and only if they are similar over $\mathbb{F}$.*

Proof. If A and B are similar over $\mathbb{F}$, they are certainly similar over $\mathbb{E}$. Suppose A and B are not similar over $\mathbb{F}$. Then A has a sequence of elementary divisors $p_1(x), \ldots, p_k(x)$ and B has a sequence of elementary divisors $q_1(x), \ldots, p_l(x)$ that are not the same. Let us find the elementary divisors of A over $\mathbb{E}$. We follow the proof of rational canonical form, still working over $\mathbb{F}$, and note that the sequence of elementary divisors we obtain over $\mathbb{F}$ is still a sequence of elementary divisors over $\mathbb{E}$. (If $\{w_1, \ldots, w_k\}$ is a rational canonical $\mathcal{T}$-generating set over $\mathbb{F}$, it is a rational canonical $\mathcal{T}$-generating set over $\mathbb{E}$; this follows from Lemma 5.8.2.) But the sequence of elementary divisors is unique. In other words, $p_1(x), \ldots, p_k(x)$ is the sequence of elementary divisors of A over $\mathbb{E}$, and similarly $q_1(x), \ldots, q_l(x)$ is the sequence of elementary divisors of B over $\mathbb{E}$. Since these are different, A and B are not similar over $\mathbb{E}$. □

We have stated the theorem in terms of matrices rather than linear transformation so as not to presume any extra background. But it is equivalent to the following one, stated in terms of tensor products.

Theorem 5.8.4. *Let V be a finite-dimensional $\mathbb{F}$-vector space and let $\mathcal{S} : V \to V$ and $\mathcal{T} : V \to V$ be two linear transformations. Then $\mathcal{S}$ and $\mathcal{T}$ are conjugate if and only if for some, and hence for any, extension field $\mathbb{E}$ of $\mathbb{F}$, $\mathcal{S} \otimes 1 : V \otimes_{\mathbb{F}} \mathbb{E} \to V \otimes_{\mathbb{F}} \mathbb{E}$ and $\mathcal{T} \otimes 1 : V \otimes_{\mathbb{F}} \mathbb{E} \to V \otimes_{\mathbb{F}} \mathbb{E}$ are conjugate.*

5.9 More than one linear transformation

Hitherto we have examined the structure of a single linear transformation. In the last section of this chapter, we derive three results that have a common theme: They deal with questions that arise when we consider more than one linear transformation.

To begin, let $\mathcal{T} : V \to W$ and $\mathcal{S} : W \to V$ be linear transformations, with V and W finite-dimensional vector spaces. We examine the relationship between $\mathcal{S}\mathcal{T} : V \to V$ and $\mathcal{T}\mathcal{S} : W \to W$.

If $V = W$ and at least one of $\mathcal{S}$ and $\mathcal{T}$ are invertible, then $\mathcal{S}\mathcal{T}$ and $\mathcal{T}\mathcal{S}$ are conjugate: $\mathcal{S}\mathcal{T} = \mathcal{T}^{-1}(\mathcal{T}\mathcal{S})\mathcal{T}$ or $\mathcal{T}\mathcal{S} = \mathcal{S}^{-1}(\mathcal{S}\mathcal{T})\mathcal{S}$. In general we have

Lemma 5.9.1. *Let $\mathcal{T} : V \to W$ and $\mathcal{S} : W \to V$ be linear transformations between finite-dimensional vector spaces.*

Let $p(x) = a_t x^t + \cdots + a_0 \in \mathbb{F}[x]$ be any polynomial with constant term $a_0 \neq 0$. Then

$$\dim\bigl(\operatorname{Ker}\bigl(p(\mathcal{S}\mathcal{T})\bigr)\bigr) = \dim\bigl(\operatorname{Ker}\bigl(p(\mathcal{T}\mathcal{S})\bigr)\bigr).$$

Proof. Let $\{v_1, \ldots, v_k\}$ be a basis for $\operatorname{Ker}(p(\mathcal{S}\mathcal{T}))$. We claim that $\{\mathcal{T}(v_1), \ldots, \mathcal{T}(v_k)\}$ is linearly independent. To see this, suppose

$$c_1\mathcal{T}(v_1) + \cdots + c_k\mathcal{T}(v_k) = 0.$$

Then $\mathcal{T}(c_1v_1 + \cdots + c_kv_k) = 0$, so $\mathcal{S}\mathcal{T}(c_1v_1 + \cdots + c_kv_k) = 0$. Let $v = c_1v_1 + \cdots + c_kv_k$, so $\mathcal{S}\mathcal{T}(v) = 0$. But $v \in \text{Ker}(p(\mathcal{S}\mathcal{T}))$, so $0 = (a_t(\mathcal{S}\mathcal{T})^t + \cdots + a_1(\mathcal{S}\mathcal{T}) + a_0I)(v) = 0 + \cdots + 0 + a_0v = a_0v$ and hence, since $a_0 \neq 0$, $v = 0$. Thus $c_1v_1 + \cdots + c_kv_k = 0$. But $\{v_1, \ldots, v_k\}$ is linearly independent, so $c_i = 0$ for all i, and hence $\{\mathcal{T}(v_1), \ldots, \mathcal{T}(v_k)\}$ is linearly independent.

Next we claim that $\mathcal{T}(v_i) \in \text{Ker}(p(\mathcal{T}\mathcal{S}))$ for each i. To see this, note that

$$(\mathcal{T}\mathcal{S})^s\mathcal{T} = (\mathcal{T}\mathcal{S})\cdots(\mathcal{T}\mathcal{S})\mathcal{T} = \mathcal{T}(\mathcal{S}\mathcal{T})\cdots(\mathcal{S}\mathcal{T}) = \mathcal{T}(\mathcal{S}\mathcal{T})^s$$

for any s. Then

$$\begin{aligned} p(\mathcal{T}\mathcal{S})(\mathcal{T}(v_i)) &= (a_t(\mathcal{T}\mathcal{S})^t + \cdots + a_0\mathcal{I})(\mathcal{T}(v_i)) \\ &= (\mathcal{T}(a_t(\mathcal{S}\mathcal{T})^t + \cdots + a_0\mathcal{I}))(v_i) \\ &= \mathcal{T}(p(\mathcal{S}\mathcal{T})(v_i)) = \mathcal{T}(0) = 0. \end{aligned}$$

Hence $\{\mathcal{T}(v_1), \ldots, \mathcal{T}(v_k)\}$ is a linearly independent subset of $\text{Ker}(p(\mathcal{T}\mathcal{S}))$, so $\dim(\text{Ker}(p(\mathcal{T}\mathcal{S}))) \geq \dim(\text{Ker}(p(\mathcal{S}\mathcal{T})))$. Interchanging $\mathcal{S}$ and $\mathcal{T}$ shows that the dimensions are equal. □

Theorem 5.9.2. *Let $\mathcal{T} : V \to W$ and $\mathcal{S} : W \to V$ be linear transformations between finite-dimensional vector spaces over an algebraically closed field $\mathbb{F}$. Then $\mathcal{S}\mathcal{T}$ and $\mathcal{T}\mathcal{S}$ have the same nonzero eigenvalues, and for each common eigenvalue $\lambda \neq 0$ $\mathcal{S}\mathcal{T}$ and $\mathcal{T}\mathcal{S}$ have the same* ESP *at λ and hence the same Jordan block structure at λ (i.e., the same number of blocks of the same sizes).*

Proof. Apply Lemma 5.9.1 to the polynomials $p_{t,\lambda}(x) = (x - \lambda)^t$ for $t = 1, 2, \ldots$, noting that the sequence of integers $\{\dim(\text{Ker}(p_{t,\lambda}(\mathcal{R}))) \mid t = 1, 2, \ldots\}$ determines the *ESP* of a linear transformation $\mathcal{R}$ at λ, or, equivalently, its Jordan block structure at λ. □

Corollary 5.9.3. *Let $\mathcal{T} : V \to V$ and $\mathcal{S} : V \to V$ be linear transformations on a finite-dimensional vector space over an arbitrary field $\mathbb{F}$. Then $\mathcal{S}\mathcal{T}$ and $\mathcal{T}\mathcal{S}$ have the same characteristic polynomial.*

Proof. First suppose that that $\mathbb{F}$ is algebraically closed. If $\dim(V) = n$ and $\mathcal{S}\mathcal{T}$, and hence $\mathcal{T}\mathcal{S}$, has distinct nonzero eigenvalues $\lambda_1, \ldots, \lambda_k$ of multiplicities $e_1, \ldots, e_k$ respectively, then they each have characteristic polynomial $x^{e_0}(x - \lambda_1)^{e_1} \cdots (x - \lambda_k)^{e_k}$ where $e_0 = n - (e_1 + \cdots + e_k)$.

In the general case, choose an arbitrary basis for V and represent $\mathcal{S}$ and $\mathcal{T}$ by matrices A and B with entries in $\mathbb{F}$. Then regard A and B as having entries in $\overline{\mathbb{F}}$, the algebraic closure of $\mathbb{F}$, and apply the algebraically closed case. $\square$

Theorem 5.9.2 and Corollary 5.9.3 are the strongest results that hold in general. It is not necessarily the case that $\mathcal{S}\mathcal{T}$ and $\mathcal{T}\mathcal{S}$ are conjugate, if $\mathcal{S}$ and $\mathcal{T}$ are both singular linear transformations.

EXAMPLE 5.9.4. (1) Let $A = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right]$ and $B = \left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right]$. Then $AB = \left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right]$ and $BA = \left[\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right]$ are not similar, so $\mathcal{T}_A\mathcal{T}_B = \mathcal{T}_{AB}$ and $\mathcal{T}_B\mathcal{T}_A = \mathcal{T}_{BA}$ are not conjugate, though they both have characteristic polynomial x^2.

(2) Let $A = \left[\begin{smallmatrix} 1 & 0 \\ -1 & 0 \end{smallmatrix}\right]$ and $B = \left[\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right]$. Then $AB = \left[\begin{smallmatrix} 1 & 1 \\ -1 & -1 \end{smallmatrix}\right]$ and $BA = \left[\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right]$ are not similar, so $\mathcal{T}_A\mathcal{T}_B = \mathcal{T}_{AB}$ and $\mathcal{T}_B\mathcal{T}_A = \mathcal{T}_{BA}$ are not conjugate, though they both have characteristic polynomial x^2. (In this case $\mathcal{T}_A$ and $\mathcal{T}_B$ are both diagonalizable.) $\diamond$

Let $\mathcal{T} : V \to V$ be a linear transformation, let $p(x)$ be a polynomial, and set $\mathcal{S} = p(\mathcal{T})$. Then $\mathcal{S}$ and $\mathcal{T}$ commute. We now investigate the question of under what circumstances any linear transformation that commutes with $\mathcal{T}$ must be of this form.

Theorem 5.9.5. *Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. The following are equivalent:*

(1) V is $\mathcal{T}$-generated by a single element, or, equivalently, the rational canonical form of $\mathcal{T}$ consists of a single block.

(2) Every linear transformation $\mathcal{S} : V \to V$ that commutes with $\mathcal{T}$ can be expressed as a polynomial in $\mathcal{T}$.

Proof. Suppose (1) is true, and let v_0 be a $\mathcal{T}$-generator of V. Then every element of V can be expressed as $p(\mathcal{T})(v_0)$ for some polynomial $p(x)$. In particular, there is a polynomial $p_0(x)$ such that $\mathcal{S}(v_0) = p_0(\mathcal{T})(v_0)$.

For any $v \in V$, let $v = p(\mathcal{T})(v_0)$. If $\mathcal{S}$ commutes with $\mathcal{T}$,

$$\begin{aligned}\mathcal{S}(v) &= \mathcal{S}\big(p(\mathcal{T})(v_0)\big) = p(\mathcal{T})\big(\mathcal{S}(v_0)\big) = p(\mathcal{T})\big(p_0(\mathcal{T})(v_0)\big)\\ &= p_0(\mathcal{T})\big(p(\mathcal{T})(v_0)\big) = p_0(\mathcal{T})(v);\end{aligned}$$

so $\mathcal{S} = p_0(\mathcal{T})$. (We have used the fact that if $\mathcal{S}$ commutes with $\mathcal{T}$, it commutes with any polynomial in $\mathcal{T}$. Also, any two polynomials in $\mathcal{T}$ commute with each other.) Thus (2) is true.

Suppose (1) is false, so that V has a rational canonical $\mathcal{T}$-generating set $\{v_1, \dots, v_k\}$ with $k > 1$. Let $p_i(x)$ be the $\mathcal{T}$-annihilator of v_i, so $p_1(x)$ is divisible by $p_i(x)$ for $i > 1$. Then we have a $\mathcal{T}$-invariant direct sum decomposition $V = V_1 \oplus \cdots \oplus V_k$. Define $\mathcal{S} : V \to V$ by $\mathcal{S}(v) = 0$ if $v \in V_1$ and $\mathcal{S}(v) = v$ if $v \in V_i$ for $i > 1$. It follows easily from the $\mathcal{T}$-invariance of the direct sum decomposition that $\mathcal{S}$ commutes with $\mathcal{T}$. We claim that $\mathcal{S}$ is not a polynomial in $\mathcal{T}$. Suppose $\mathcal{S} = p(\mathcal{T})$ for some polynomial $p(x)$. Then $0 = s(v_1) = p(\mathcal{T})(v_1)$ so $p(x)$ is divisible by $p_1(x)$, the $\mathcal{T}$-annihilator of v_1. But $p_1(x)$ is divisible by $p_i(x)$ for $i \geq 1$, so $p(x)$ is divisible by $p_i(x)$ for $i > 1$, and hence $\mathcal{S}(v_2) = \cdots = \mathcal{S}(v_k) = 0$. Thus $\mathcal{S}(v) \neq v$ if $0 \neq v \in V_i$ for $i > 1$, a contradiction, and (2) is false. □

REMARK 5.9.6. Equivalent conditions to condition (1) of Theorem 5.9.5 were given in Corollary 5.3.3. ◇

Finally, let $\mathcal{S}$ and $\mathcal{T}$ be diagonalizable linear transformations. We see when $\mathcal{S}$ and $\mathcal{T}$ are simultaneously diagonalizable.

Theorem 5.9.7. *Let V be a finite-dimensional vector space and let $\mathcal{S} : V \to V$ and $\mathcal{T} : V \to V$ be diagonalizable linear transformations. The following are equivalent:*

(1) $\mathcal{S}$ and $\mathcal{T}$ are simultaneously diagonalizable, i.e, there is a basis $\mathcal{B}$ of V with $[\mathcal{S}]_{\mathcal{B}}$ and $[\mathcal{T}]_{\mathcal{B}}$ both diagonal, or equivalently, there is a basis $\mathcal{B}$ of V consisting of common eigenvectors of $\mathcal{S}$ and $\mathcal{T}$.

(2) $\mathcal{S}$ and $\mathcal{T}$ commute.

Proof. Suppose (1) is true. Let $\mathcal{B} = \{v_1, \dots, v_n\}$ where $\mathcal{S}(v_i) = \lambda_i v_i$ and $\mathcal{T}(v_j) = \mu_i v_i$ for some $\lambda_i, \mu_i \in \mathbb{F}$. Then $\mathcal{S}(\mathcal{T}(v_i)) = \mathcal{S}(\mu_i v_i) = \lambda_i \mu_i v_i = \mu_i \lambda_i v_i = \mathcal{T}(\lambda_i(v_i)) = \mathcal{T}(\mathcal{S}(v_i))$ for each i, and since $\mathcal{B}$ is a basis, this implies $\mathcal{S}(\mathcal{T}(v)) = \mathcal{T}(\mathcal{S}(v))$ for every $v \in V$, i.e., that $\mathcal{S}$ and $\mathcal{T}$ commute.

Suppose (2) is true. Since $\mathcal{T}$ is diagonalizable, $V = V_1 \oplus \cdots \oplus V_k$ where V_i is the eigenspace of $\mathcal{T}$ corresponding to the eigenvalue μ_i of $\mathcal{T}$. For $v \in V_i$, $\mathcal{T}(\mathcal{S}(v_i)) = \mathcal{S}(\mathcal{T}(v_i)) = \mathcal{S}(\mu_i v_i) = \mu_i \mathcal{S}(v_i)$, so $\mathcal{S}(v_i) \in V_i$ as well. Thus each subspace V_i is $\mathcal{S}$-invariant. Since $\mathcal{S}$ is diagonalizable, so is its restriction $\mathcal{S}_i : V_i \to V_i$. ($m_{\mathcal{S}_i}(x)$ divides $m_{\mathcal{S}}(x)$, which is a product of distinct linear factors, so $m_{\mathcal{S}_i}(x)$ is a product of distinct linear factors as well.) Thus V_i has a basis $\mathcal{B}_i$ consisting of eigenvectors for $\mathcal{S}$. Since every nonzero vector in V_i is an eigenvector of $\mathcal{T}$, $\mathcal{B}_i$ consists of eigenvectors of $\mathcal{T}$, as well. Set $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_k$. □

Remark 5.9.8. It is easy to see that if $\mathcal{S}$ and $\mathcal{T}$ are both triangularizable linear transformations and $\mathcal{S}$ and $\mathcal{T}$ commute, then they are simultaneously triangularizable, but it is even easier to see that the converse is false. For example, take $\mathcal{S} = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}$ and $\mathcal{T} = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$. $\diamond$

CHAPTER 6

Bilinear, sesquilinear, and quadratic forms

In this chapter we investigate bilinear, sesquilinear, and quadratic forms, or "forms" for short. A form is an additional structure on a vector space. Forms are interesting in their own right, and they have applications throughout mathematics. Many important vector spaces naturally come equipped with a form.

In the first section we introduce forms and derive their basic properties. In the second section we see how to simplify forms on finite-dimensional vector spaces and in some cases completely classify them. In the third section we see how the presence of nonsingular form(s) enables us to define the adjoint of a linear transformation.

6.1 Basic definitions and results

Definition 6.1.1. A conjugation on a field $\mathbb{F}$ is a map $c : \mathbb{F} \to \mathbb{F}$ with the properties (where we denote $c(f)$ by $\overline{f}$):

(1) $\overline{\overline{f}} = f$ for every $f \in \mathbb{F}$,

(2) $\overline{f_1 + f_2} = \overline{f_1} + \overline{f_2}$ for every $f_1, f_2 \in \mathbb{F}$,

(3) $\overline{f_1 f_2} = \overline{f_1}\,\overline{f_2}$ for every $f_1, f_2 \in \mathbb{F}$.

The conjugation c is nontrivial if c is not the identity on $\mathbb{F}$.

A conjugation on a vector space V over $\mathbb{F}$ is a map $c : V \to V$ with the properties (where we denote $c(v)$ by $\overline{v}$):

(1) $\overline{\overline{v}} = v$ for every $v \in V$,

(2) $\overline{v_1 + v_2} = \overline{v_1} + \overline{v_2}$ for every $v_1, v_2 \in V$,

(3) $\overline{fv} = \overline{f}\,\overline{v}$ for every $f \in \mathbb{F}$, $v \in V$.

$\diamond$

REMARK 6.1.2. The archetypical example of a conjugation on a field is complex conjugation on the field $\mathbb{C}$ of complex numbers. $\diamond$

DEFINITION 6.1.3. Let $\mathbb{F}$ be a field with a nontrivial conjugation and let V and W be $\mathbb{F}$-vector spaces. Then $\mathcal{T} : V \to W$ is *conjugate linear* if

(1) $\mathcal{T}(v_1 + v_2) = \mathcal{T}(v_1) + \mathcal{T}(v_2)$ for every $v_1, v_2 \in V$

(2) $\mathcal{T}(cv) = \overline{c}\,\mathcal{T}(v)$ for every $c \in \mathbb{F}$, $v \in V$.

$\diamond$

Now we come to the basic definition. The prefix "sesqui" means "one and a half".

DEFINITION 6.1.4. Let V be an $\mathbb{F}$-vector space. A *bilinear form* is a function $\varphi : V \times V \to \mathbb{F}$, $\varphi(x, y) = \langle x, y\rangle$, that is linear in each entry, i.e., that satisfies

(1) $\langle c_1x_1 + c_2x_2, y\rangle = c_1\langle x_1, y\rangle + c_2\langle x_2, y\rangle$ for every $c_1, c_2 \in \mathbb{F}$, and $x_1, x_2, y \in V$

(2) $\langle x, c_1y_1 + c_2y_2\rangle = c_1\langle x, y_1\rangle + c_2\langle x, y_2\rangle$ for every $c_1, c_2 \in \mathbb{F}$, and $x, y_1, y_2 \in V$.

A *sesquilinear* form is a function $\varphi : V \times V \to \mathbb{F}$, $\varphi(x, y) = \langle x, y\rangle$, that is linear in the first entry and conjugate linear in the second, i.e., that satisfies (1) and $(\overline{2})$:

$(\overline{2})$ $\langle x, c_1y_1 + c_2y_2\rangle = \overline{c}_1\langle x, y_1\rangle + \overline{c}_2\langle x, y_2\rangle$ for every $c_1, c_2 \in \mathbb{F}$, and $x, y_1, y_2 \in V$

for a nontrivial conjugation $c \mapsto \overline{c}$ on $\mathbb{F}$. $\diamond$

EXAMPLE 6.1.5. (1) Let $V = \mathbb{R}^n$. Then $\langle x, y\rangle = {}^t xy$ is a bilinear form. If $V = \mathbb{C}^n$, then $\langle x, y\rangle = {}^t x\overline{y}$ is a sesquilinear form. In both cases this is the familiar "dot product." Indeed for any field $\mathbb{F}$ we can define a bilinear form on $\mathbb{F}^n$ by $\langle x, y\rangle = {}^t xy$ and for any field $\mathbb{F}$ with a nontrivial conjugation we can define a sesquilinear form on $\mathbb{F}^n$ by $\langle x, y\rangle = {}^t x\overline{y}$.

(2) More generally, for an n-by-n matrix A with entries in $\mathbb{F}$, $\langle x, y\rangle = {}^t xAy$ is a bilinear form on $\mathbb{F}^n$, and $\langle x, y\rangle = {}^t xA\overline{y}$ is a sesquilinear form

on $\mathbb{F}^n$. We will see that all bilinear and sesquilinear forms on $\mathbb{F}^n$ arise this way, and, by taking coordinates, that all bilinear and sesquilinear forms on finite-dimensional vector spaces over $\mathbb{F}$ arise in this way.

(3) Let $V = {}^r\mathbb{F}^\infty$ and let $x = (x_1, x_2, \ldots)$, $y = (y_1, y_2, \ldots)$. We define a bilinear form on V by $\langle x, y \rangle = \sum x_i y_i$. If $\mathbb{F}$ has a nontrivial conjugation, we define a sesquilinear form on V by $\langle x, y \rangle = \sum x_i \overline{y}_i$.

(4) Let V be the vector space of real-valued continuous functions on $[0, 1]$. Then V has a bilinear form given by

$$\big\langle f(x), g(x) \big\rangle = \int_0^1 f(x) g(x)\, dx.$$

If V is the vector space of complex-valued continuous functions on $[0, 1]$, then V has a sesquilinear form given by

$$\big\langle f(x), g(x) \big\rangle = \int_0^1 f(x) \overline{g}(x)\, dx.$$

$\diamond$

Let us see the connection between forms and dual spaces.

Lemma 6.1.6. *(1) Let V be a vector space and let $\varphi(x, y) = \langle x, y \rangle$ be a bilinear form on V. Then $\alpha_\varphi : V \to V^*$ defined by $\alpha_\varphi(y)(x) = \langle x, y \rangle$ is a linear transformation.*

(2) Let V be a vector space and let $\varphi(x, y) = \langle x, y \rangle$ be a sesquilinear form on V. Then $\alpha_\varphi : V \to V^*$ defined by $\alpha_\varphi(y)(x) = \langle x, y \rangle$ is a conjugate linear transformation.

REMARK 6.1.7. In the situation of Lemma 6.1.6, $\alpha_\varphi(y)$ is often written as $\langle \cdot, y \rangle$, so with this notation $\alpha_\varphi : y \mapsto \langle \cdot, y \rangle$. $\diamond$

DEFINITION 6.1.8. Let V be a vector space and let φ be a bilinear (respectively sesquilinear) form on V. Then φ is *nonsingular* if the map $\alpha_\varphi : V \to V^*$ is an isomorphism (respectively conjugate isomorphism). $\diamond$

REMARK 6.1.9. In more concrete terms, φ is nonsingular if and only if the following is true: Let $\mathcal{T} : V \to \mathbb{F}$ be any linear transformation. Then there is a unique vector $w \in V$ such that

$$\mathcal{T}(v) = \varphi(v, w) = \langle v, w \rangle \quad \text{for every } v \in V.$$

$\diamond$

In case V is finite dimensional, we have an easy criterion to determine if a form φ is nonsingular.

Lemma 6.1.10. *Let V be a finite-dimensional vector space and let $\varphi(x, y) = \langle x, y\rangle$ be a bilinear or sesquilinear form on V. Then φ is nonsingular if and only if for every $y \in V$, $y \neq 0$, there is an $x \in V$ such that $\langle x, y\rangle = \varphi(x, y) \neq 0$.*

Proof. Since $\dim V^* = \dim V$, α_φ is an (conjugate) isomorphism if and only if it is injective.

Suppose that α_φ is injective, i.e., if $y \neq 0$, then $\alpha_\varphi(y) \neq 0$. This means that there exists an $x \in V$ with $\alpha_\varphi(y)(x) = \varphi(x, y) \neq 0$.

Conversely, suppose that for every $y \in V$, $y \neq 0$, there exists an x with $\alpha_\varphi(y)(x) = \varphi(x, y) \neq 0$. Then for every $y \in V$, $y \neq 0$, $\alpha_\varphi(y)$ is not the zero map. Hence $\mathrm{Ker}(\alpha_\varphi) = \{0\}$ and α_φ is injective. $\square$

Now we see how to use coordinates to associate a matrix to a bilinear or sesquilinear form on a finite-dimensional vector space. Note this is *different* from associating a matrix to a linear transformation.

Theorem 6.1.11. *Let $\varphi(x, y) = \langle x, y\rangle$ be a bilinear (respectively sesquilinear) form on the finite-dimensional vector space V and let $\mathcal{B} = \{v_1, \dots, v_n\}$ be a basis for V. Define a matrix $A = (a_{ij})$ by*

$$a_{ij} = \left\langle v_i, v_j \right\rangle \quad i, j = 1, \dots, n.$$

Then for $x, y \in V$,

$$\langle x, y\rangle =^t [x]_{\mathcal{B}} A [y]_{\mathcal{B}} \quad \left(\textit{respectively } {}^t[x]_{\mathcal{B}} A \overline{[y]}_{\mathcal{B}}\right).$$

Proof. By construction, this is true when $x = v_i$ and $y = v_j$ (as then $[x] = e_i$ and $[y] = e_j$) and by (conjugate) linearity that implies it is true for any vectors x and y in V. $\square$

DEFINITION 6.1.12. The matrix $A = (a_{ij})$ of Theorem 6.1.11 is the *matrix of the form* φ with respect to the basis $\mathcal{B}$. We denote it by $[\varphi]_{\mathcal{B}}$. $\diamond$

Theorem 6.1.13. *The bilinear or sesquilinear form φ on the finite dimensional vector space V is nonsingular if and only if matrix $[\varphi]_{\mathcal{B}}$ in any basis $\mathcal{B}$ of V is nonsingular.*

Proof. We use the criterion of Lemma 6.1.10 for nonsingularity of a form.

Suppose $A = [\varphi]_{\mathcal{B}}$ is a nonsingular matrix. For $x \in V$, $x \neq 0$, let

$$[x]_{\mathcal{B}} = \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}.$$

Then for some i, $c_i \neq 0$. Let $z = A^{-1}e_i \in \mathbb{F}_n$ and let $y \in V$ with $[y]_{\mathcal{B}} = z$ (or $[y]_{\mathcal{B}} = \overline{z}$). Then $\varphi(x, y) = {}^t x A A^{-1} e_i = c_i \neq 0$.

Suppose A is singular. Let $z \in \mathbb{F}^n$, $z \neq 0$, with $Az = 0$. Then if $y \in V$ with $[y]_{\mathcal{B}} = z$ (or $[y]_{\mathcal{B}} = \overline{z}$), then $\varphi(x, y) = {}^t x A z = {}^t x 0 = 0$ for every $x \in V$. □

Now we see the effect of a change of basis on the matrix of a form.

Theorem 6.1.14. *Let V be a finite-dimensional vector space and let φ be a bilinear (respectively sesquilinear) form on V. Let $\mathcal{B}$ and $\mathcal{C}$ be any two bases of V. Then*

$$[\varphi]_{\mathcal{C}} = {}^t P_{\mathcal{B}\leftarrow\mathcal{C}} [\varphi]_{\mathcal{B}} P_{\mathcal{B}\leftarrow\mathcal{C}} \quad (\textit{respectively } {}^t P_{\mathcal{B}\leftarrow\mathcal{C}} [\varphi]_{\mathcal{B}} \overline{P}_{\mathcal{B}\leftarrow\mathcal{C}}).$$

Proof. We do the sesquilinear case; the bilinear case follows by omitting the conjugation.

By the definition of $[\varphi]_{\mathcal{C}}$,

$$\varphi(x, y) = {}^t[x]_{\mathcal{C}} [\varphi]_{\mathcal{C}} \overline{[y]}_{\mathcal{C}}$$

and by the definition of $[\varphi]_{\mathcal{B}}$,

$$\varphi(x, y) = {}^t[x]_{\mathcal{B}} [\varphi]_{\mathcal{B}} \overline{[y]}_{\mathcal{B}}.$$

But $[x]_{\mathcal{B}} = P_{\mathcal{B}\leftarrow\mathcal{C}}[x]_{\mathcal{C}}$ and $\overline{[y]}_{\mathcal{B}} = \overline{P}_{\mathcal{B}\leftarrow\mathcal{C}}\overline{[y]}_{\mathcal{C}}$. Substitution gives

$$\begin{aligned} {}^t[x]_{\mathcal{C}} [\varphi]_{\mathcal{C}} \overline{[y]}_{\mathcal{C}} = \varphi(x, y) &= {}^t[x]_{\mathcal{B}} [\varphi]_{\mathcal{B}} \overline{[y]}_{\mathcal{B}} \\ &= {}^t\big(P_{\mathcal{B}\leftarrow\mathcal{C}}[x]_{\mathcal{C}}\big)[\varphi]_{\mathcal{B}}\big(\overline{P}_{\mathcal{B}\leftarrow\mathcal{C}}\overline{[y]}_{\mathcal{C}}\big) \\ &= {}^t[x]_{\mathcal{C}}\big({}^t P_{\mathcal{B}\leftarrow\mathcal{C}}[\varphi]_{\mathcal{B}}\overline{P}_{\mathcal{B}\leftarrow\mathcal{C}}\big)\overline{[y]}_{\mathcal{C}}. \end{aligned}$$

Since this is true for every $x, y \in V$,

$$[\varphi]_{\mathcal{C}} = {}^t P_{\mathcal{B}\leftarrow\mathcal{C}} [\varphi]_{\mathcal{B}} \overline{P}_{\mathcal{B}\leftarrow\mathcal{C}}.$$ □

This leads us to the following definition.

DEFINITION 6.1.15. Two square matrices A and B with entries in $\mathbb{F}$ are *congruent* if there is an invertible matrix P with ${}^tPAP = B$, and are *conjugate congruent* if there is an invertible matrix P with ${}^tPA\overline{P} = B$. $\diamond$

It is easy to check that (conjugate) congruence is an equivalence relation. We then have:

Corollary 6.1.16. *(1) Let φ be a bilinear (respectively sesquilinear) form on the finite-dimensional vector space V. Let $\mathcal{B}$ and $\mathcal{C}$ be bases of V. Then $[\varphi]_{\mathcal{B}}$ and $[\varphi]_{\mathcal{C}}$ are congruent (respectively conjugate congruent).*

(2) Let A and B be congruent (respectively conjugate congruent) n-by-n matrices. Let V be an n-dimensional vector space over $\mathbb{F}$. Then there is a bilinear form (respectively sesquilinear form) φ on V and bases $\mathcal{B}$ and $\mathcal{C}$ of V with $[\varphi]_{\mathcal{B}} = A$ and $[\varphi]_{\mathcal{C}} = B$.

6.2 CHARACTERIZATION AND CLASSIFICATION THEOREMS

In this section we derive results about the characterization and classification of forms on finite-dimensional vector spaces.

Our discussion so far has been general, but almost all the forms encountered in mathematical practice fall into one of the following classes.

DEFINITION 6.2.1. (1) A bilinear form φ on V is *symmetric* if $\varphi(x, y) = \varphi(y, x)$ for all $x, y \in V$.

(2) A bilinear form φ on V is *skew-symmetric* if $\varphi(x, y) = -\varphi(y, x)$ for all $x, y \in V$, and $\varphi(x, x) = 0$ for all $x \in V$ (this last condition follows automatically if $\operatorname{char}(\mathbb{F}) \neq 2$).

(3) A sesquilinear form φ on V is *Hermitian* if $\varphi(x, y) = \overline{\varphi(y, x)}$ for all $x, y \in V$.

(4) A sesquilinear form φ on V is *skew-Hermitian* if $\operatorname{char}(\mathbb{F}) \neq 2$ and $\varphi(x, y) = -\overline{\varphi(y, x)}$ for all $x, y \in V$. (If $\operatorname{char}(\mathbb{F}) = 2$, skew-Hermitian is not defined.) $\diamond$

Lemma 6.2.2. *Let V be a finite-dimensional vector space over $\mathbb{F}$ and let φ be a form on V. Choose a basis $\mathcal{B}$ of V and let $A = [\varphi]_{\mathcal{B}}$. Then*

(1) φ is symmetric if and only if ${}^tA = A$.

(2) φ is skew-symmetric if and only if ${}^tA = -A$ (and, if $\operatorname{char}(\mathbb{F}) = 2$, *the diagonal entries of A are all 0).*

(3) φ is Hermitian if and only if ${}^tA = \overline{A}$.

(4) φ is skew-Hermitian if and only if ${}^tA = -\overline{A}$ (and $\operatorname{char}(\mathbb{F}) \neq 2$*).*

DEFINITION 6.2.3. Matrices satisfying the conclusion of Lemma 6.2.2 parts (1), (2), (3), or (4) are called *symmetric*, *skew-symmetric*, *Hermitian*, or *skew-Hermitian* respectively. $\diamond$

For the remainder of this section we assume that the forms we consider are one of these types: symmetric, Hermitian, skew-symmetric, or skew-Hermitian, and that the vector spaces they are defined on are finite dimensional.

We will write (V, φ) for the space V equipped with the form φ.

The appropriate notion of equivalence of forms is isometry.

DEFINITION 6.2.4. Let V admit a form φ and W admit a form ψ. Then a linear transformation $\mathcal{T} : V \to W$ is an *isometry* between (V, φ) and (W, ψ) if $\mathcal{T}$ is an isomorphism and furthermore

$$\psi\big(\mathcal{T}(v_1), \mathcal{T}(v_2)\big) = \varphi(v_1, v_2) \quad \text{for every } v_1, v_2 \in V.$$

If there exists an isometry between (V, φ) and (W, ψ) then (V, φ) and (W, ψ) are *isometric*. $\diamond$

Lemma 6.2.5. *In the situation of Definition 6.2.4, let V have basis $\mathcal{B}$ and let W have basis $\mathcal{C}$. Then $\mathcal{T}$ is an isometry if and only if $M = [\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}$ is an invertible matrix with*

$$\begin{aligned} {}^tM[\psi]_{\mathcal{C}}M &= [\varphi]_{\mathcal{B}} \text{ in the bilinear case, or} \\ {}^tM[\psi]_{\mathcal{C}}\overline{M} &= [\varphi]_{\mathcal{B}} \text{ in the sesquilinear case.} \end{aligned}$$

Thus V and W are isometric if and only if $[\psi]_{\mathcal{C}}$ and $[\varphi]_{\mathcal{B}}$ are congruent, in the bilinear case, or conjugate congruent, in the sesquilinear case, in some (or any) pair of bases $\mathcal{B}$ of V and $\mathcal{C}$ of W.

DEFINITION 6.2.6. Let φ be a bilinear or sesquilinear form on the vector space V. Then the isometry group of φ is

$$\begin{aligned} \mathrm{Isom}(\varphi) = \big\{\mathcal{T} : V \to V \text{ isomorphism} \mid \\ \mathcal{T} \text{ is an isometry from } (V, \varphi) \text{ to itself}\big\}. \end{aligned}$$ $\diamond$

Corollary 6.2.7. *In the situation of Definition 6.2.6, let $\mathcal{B}$ be any basis of V. Then $\mathcal{T} \mapsto [\mathcal{T}]_{\mathcal{B}}$ gives an isomorphism*

$$\begin{aligned} \mathrm{Isom}(\varphi) \to \big\{\textit{invertible matrices } M \mid \\ {}^tM[\varphi]_{\mathcal{B}}M = [\varphi]_{\mathcal{B}} \textit{ or } {}^tM[\varphi]_{\mathcal{B}}\overline{M} = [\varphi]_{\mathcal{B}}\big\}. \end{aligned}$$

Now we begin to simplify and classify forms.

DEFINITION 6.2.8. Let V admit the form φ. Then two vectors v_1 and v_2 in V are *orthogonal* (with respect to φ) if

$$\varphi(v_1, v_2) = \varphi(v_2, v_1) = 0.$$

Two subspaces V_1 and V_2 are *orthogonal* (with respect to φ) if

$$\varphi(v_1, v_2) = \varphi(v_2, v_1) = 0 \quad \text{for all } v_1 \in V_1,\ v_2 \in V_2. \qquad \diamond$$

We also have an appropriate notion of direct sum.

DEFINITION 6.2.9. Let V admit a form φ, and let V_1 and V_2 be subspaces of V. Then V is the *orthogonal direct sum* of V_1 and V_2, $V = V_1 \perp V_2$, if $V = V_1 \oplus V_2$ (i.e., V is the direct sum of V_1 and V_2) and V_1 and V_2 are orthogonal with respect to φ. This is equivalent to the condition: Let $v, v' \in V$ and write v uniquely as $v = v_1 + v_2$ with $v_1 \in V_1$ and $v_2 \in V_2$, and similarly $v' = v_1' + v_2'$ with $v_1' \in V_1$ and $v_2' \in V_2$.

Let φ_1 be the restriction of φ to $V_1 \times V_1$, and φ_2 be the restriction of φ to $V_2 \times V_2$. Then

$$\varphi(v, v') = \varphi_1(v_1, v_1') + \varphi_2(v_2, v_2').$$

In this situation we will also write $(V, \varphi) = (V_1, \varphi_1) \perp (V_2, \varphi_2)$. $\diamond$

REMARK 6.2.10. Translated into matrix language, the condition in Definition 6.2.9 is as follows: Let $\mathcal{B}_1$ be a basis for V_1 and $\mathcal{B}_2$ be a basis for V_2. Let $A_1 = [\varphi_1]_{\mathcal{B}_1}$ and $A_2 = [\varphi_2]_{\mathcal{B}_2}$. Let $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ and $A = [\varphi]_{\mathcal{B}}$. Then

$$A = \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix}$$

(a block-diagonal matrix with blocks A_1 and A_2). $\diamond$

First let us note that if φ is not nonsingular, we may "split off" its singular part.

DEFINITION 6.2.11. Let φ be a form on V. The *kernel* of φ is the subspace of V given by

$$\operatorname{Ker}(\varphi) = \{v \in V \mid \varphi(v, w) = \varphi(w, v) = 0 \quad \text{for all } w \in V\}. \qquad \diamond$$

REMARK 6.2.12. By Lemma 6.1.10, φ is nonsingular if and only if $\operatorname{Ker}(\varphi) = 0$. $\diamond$

Lemma 6.2.13. *Let φ be a form on V. Then V is the orthogonal direct sum*

$$V = \operatorname{Ker}(\varphi) \perp V_1$$

for some subspace V_1, with $\varphi_1 = \varphi|V_1$ a nonsingular form on V_1, and (V_1, φ_1) is well-defined up to isometry.

Proof. Let V_1 be any complement of $\operatorname{Ker}(\varphi)$, so that $V = \operatorname{Ker}(\varphi) \oplus V_1$, and let $\varphi_1 = \varphi|V_1$. Certainly $V = \operatorname{Ker}(\varphi) \perp V_1$. To see that φ_1 is nonsingular, suppose that $v_1 \in V_1$ with $\varphi(v_1, w_1) = 0$ for every $w_1 \in V_1$. Then $\varphi(v_1, w) = 0$ for every $w \in V$, so $v_1 \in \operatorname{Ker}(\varphi)$, i.e., $v \in \operatorname{Ker}(\varphi) \cap V_1 = \{0\}$.

There was a choice of V_1, but we claim that all choices yield isometric forms. To see this, let V' be the quotient space $V/\operatorname{Ker}(\varphi)$. There is a well-defined form φ' on V' defined as follows: Let $\pi : V \to V/\operatorname{Ker}(\varphi)$ be the canonical projection. Let $v', w' \in V'$, choose $v, w \in V$ with $v' = \pi(v)$ and $w' = \pi(w)$. Then $\varphi'(v', w') = \varphi(v, w)$. It is then easy to check that π/V_1 gives an isometry from (V_1, φ_1) to (V', φ'). □

In light of this lemma, we usually concentrate on nonsingular forms. But we also have the following well-defined invariant of forms in general.

DEFINITION 6.2.14. Let V be finite dimensional and let V admit the form φ. Then the *rank* of φ is the dimension of V_1, where V_1 is the subspace given in Lemma 6.2.13. ◇

DEFINITION 6.2.15. Let W be a subspace of V. Then its *orthogonal subspace* is the subspace

$$W^\perp = \{v \in V \mid \varphi(w, v) = 0 \text{ for all } w \in W\}. \qquad \diamond$$

Lemma 6.2.16. *Let V be a finite-dimensional vector space. Let W be a subspace of V and let $\psi = \varphi|W$. If ψ is nonsingular, then $V = W \perp W^\perp$. If φ is nonsingular as well, then $\psi^\perp = \varphi|W^\perp$ is nonsingular.*

Proof. Clearly W and $W^\perp$ are orthogonal, so to show that $V = W \perp W^\perp$ it suffices to show that $V = W \oplus W^\perp$.

Let $v_0 \in W \cap W^\perp$. Then $v_0 \in W^\perp$, so $\varphi(w, v_0) = 0$ for all $w \in W$. But $v_0 \in W$ as well, so $\psi(w, v_0) = \varphi(w, v_0)$ and then the nonsingularity of ψ implies $v_0 = 0$.

Let $v_0 \in V$. Then $\mathcal{T}(w) = \varphi(w, v_0)$ is a linear transformation $\mathcal{T} : W \to \mathbb{F}$, and we are assuming ψ is nonsingular so by Remark 6.1.9 there is a $w_0 \in W$ with $\mathcal{T}(w) = \psi(w, w_0) = \varphi(w, w_0)$ for every $w \in W$. Then $\varphi(w, v_0 - w_0) = 0$ for every $w \in W$, so $v_0 - w_0 \in W^\perp$, and $v_0 = w_0 + (v_0 - w_0)$.

Suppose φ is nonsingular and let $v_0 \in W^\perp$. Then there is a vector $v \in V$ with $\varphi(v, v_0) \neq 0$. Write $v = w_1 + w_2$ with $w_1 \in W$, $w_2 \in W^\perp$. Then

$$0 \neq \varphi(v, v_0) = \varphi(w_1 + w_2, v_0) = \varphi(w_1, v_1) + \varphi(w_2, v_0) = \varphi(w_2, v_0),$$

so $\varphi|W^\perp$ is nonsingular. □

REMARK 6.2.17. The condition that $\varphi|W$ be nonsingular is necessary. For example, if φ is the form on $\mathbb{F}^2$ defined by

$$\varphi(v, w) = {}^t v \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} w$$

and W is the subspace

$$W = \left\{ \begin{bmatrix} x \\ 0 \end{bmatrix} \right\},$$

then $W = W^\perp$. ◇

Corollary 6.2.18. *Let V be a finite-dimensional vector space and let W be a subspace of V with $\varphi|W$ and $\varphi|W^\perp$ both nonsingular. Then $(W^\perp)^\perp = W$.*

Proof. We have $V = W \perp W^\perp = W^\perp \perp (W^\perp)^\perp$. It is easy to check that $(W^\perp)^\perp \supseteq W$, so they are equal. □

Our goal now is to "simplify", and in favorable cases classify, forms on finite-dimensional vector spaces. Lemma 6.2.16 is an important tool that enables to apply inductive arguments. Here is another important tool, and a result interesting in its own right.

Lemma 6.2.19. *Let V be a vector space over $\mathbb{F}$, and let V admit the nonsingular form φ. If* $\mathrm{char}(\mathbb{F}) \neq 2$, *assume φ is symmetric or Hermitian. If* $\mathrm{char}(\mathbb{F}) = 2$, *assume φ is Hermitian. Then there is a vector $v \in V$ with* $\varphi(v, v) \neq 0$.

Proof. Pick a nonzero vector $v_1 \in V$. If $\varphi(v_1, v_1) \neq 0$, then set $v = v_1$. If $\varphi(v_1, v_1) = 0$, then, by the nonsingularity of φ, there is a vector v_2

with $b = \varphi(v_1, v_2) \neq 0$. If $\varphi(v_2, v_2) \neq 0$, set $v = v_2$. Otherwise, let $v_3 = av_1 + v_2$ where $a \in \mathbb{F}$ is an arbitrary scalar. Then

$$\begin{aligned}
\varphi(v_3, v_3) &= \varphi(av_1 + v_2, av_1 + v_2) \\
&= \varphi(av_1, av_1) + \varphi(av_1, v_2) + \varphi(v_2, av_1) + \varphi(v_2, v_2) \\
&= \varphi(av_1, v_2) + \varphi(v_2, av_1) \\
&= 2ab \qquad \text{if } \varphi \text{ is symmetric} \\
&= ab + \overline{ab} \qquad \text{if } \varphi \text{ is Hermitian.}
\end{aligned}$$

In the symmetric case, choose $a \neq 0$ arbitrarily. In the Hermitian case, let a be any element of $\mathbb{F}$ with $ab \neq -\overline{ab}$. (If $\operatorname{char}(\mathbb{F}) \neq 2$ we may choose $a = b^{-1}$. If $\operatorname{char}(\mathbb{F}) = 2$ we may choose $a = b^{-1}c$ where $c \in \mathbb{F}$ with $\overline{c} \neq c$.) Then set $v = v_3$ for this choice of a. □

REMARK 6.2.20. The conclusion of this lemma does not hold if $\operatorname{char}(\mathbb{F}) = 2$. For example, let $\mathbb{F}$ be a field of characteristic 2, let $V = \mathbb{F}^2$, and let φ be the form defined on V by

$$\varphi(v, w) = {}^t v \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} w.$$

Then it is easy to check that $\varphi(v, v) = 0$ for every $v \in V$. ◇

Thus we make the following definition.

DEFINITION 6.2.21. Let V be a vector space over a field $\mathbb{F}$ of characteristic 2 and let φ be a symmetric bilinear form on V. Then φ is *even* if $\varphi(v, v) = 0$ for every $v \in V$, and *odd* otherwise. ◇

Lemma 6.2.22. *Let V be a vector space over a field $\mathbb{F}$ of characteristic 2 and let φ be a symmetric bilinear form on V. Then V is even if and only if for some (and hence for every) basis $\mathcal{B} = \{v_1, v_2, \ldots\}$ of V, $\varphi(v_i, v_i) = 0$ for every $v_i \in \mathcal{B}$.*

Proof. This follows immediately from the identity

$$\begin{aligned}
\varphi(v + w, v + w) &= \varphi(v, v) + \varphi(v, w) + \varphi(w, v) + \varphi(w, w) \\
&= \varphi(v, v) + 2\varphi(v, w) + \varphi(w, w) \\
&= \varphi(v, v) + \varphi(w, w).
\end{aligned}$$

□

Here is our first simplification.

DEFINITION 6.2.23. Let V be a finite-dimensional vector space and let φ be a symmetric bilinear or a Hermitian form on V. Then φ is diagonalizable if there are 1-dimensional subspaces $V_1, V_2, \ldots, V_n$ of V such that

$$V = V_1 \perp V_2 \perp \cdots \perp V_n. \qquad \diamond$$

REMARK 6.2.24. Let us see where the name comes from. Choose a nonzero vector v_i in V_i for each i (so $\{v_i\}$ is a basis for V_i) and let $a_i = \varphi(v_i, v_i)$. Let $\mathcal{B}$ be the basis of V given by $\mathcal{B} = \{v_1, \ldots, v_n\}$. Then

$$[\varphi]_{\mathcal{B}} = \begin{bmatrix} a_1 & & & \\ & a_2 & & 0 \\ & 0 & \ddots & \\ & & & a_n \end{bmatrix}$$

is a diagonal matrix. Conversely if V has a basis $\mathcal{B} = \{v_1, \ldots, v_n\}$ with $[\varphi]_{\mathcal{B}}$ diagonal, then $V = V_1 \perp \cdots \perp V_n$ where V_i is the subspace spanned by v_i. $\diamond$

REMARK 6.2.25. We will let $[a]$ denote the bilinear or Hermitian form on $\mathbb{F}$ (an $\mathbb{F}$-vector space) with matrix $[a]$, i.e., the bilinear form given by $\varphi(x, y) = xay$, or the Hermitian form given by $\varphi(x, y) = xa\overline{y}$. In this notation a form φ on V is diagonalizable if and only if it is isometric to $[a_1] \perp \cdots \perp [a_n]$ for some $a_1, \ldots, a_n \in \mathbb{F}$. $\diamond$

Theorem 6.2.26. *Let V be a finite-dimensional vector space over a field $\mathbb{F}$ of characteristic $\neq 2$, and let φ be a symmetric or Hermitian form on V. Then φ is diagonalizable. If* $\operatorname{char}(\mathbb{F}) = 2$ *and φ is Hermitian, then φ is diagonalizable.*

Proof. We only prove the case $\operatorname{char}(\mathbb{F}) \neq 2$.

By Lemma 6.2.13, it suffices to consider the case where φ is nonsingular. We proceed by induction on the dimension of V.

If V is 1-dimensional, there is nothing to prove. Suppose the theorem is true for all vector spaces of dimension less than n, and let V have dimension n.

By Lemma 6.2.19, there is an element v_1 of V with $\varphi(v_1, v_1) = a_1 \neq 0$. Let $V_1 = \operatorname{Span}(v_1)$. Then, by Lemma 6.2.16, $V = V_1 \perp V_1^{\perp}$ and $\varphi|V_1^{\perp}$ is nonsingular. Then by induction $V_1^{\perp} = V_2 \perp \cdots \perp V_n$ for 1-dimensional subspaces $V_2, \ldots, V_n$, so $V = V_1 \perp V_2 \perp \cdots \perp V_n$ as required. $\square$

The theorem immediately gives us a classification of forms on complex vector spaces.

Corollary 6.2.27. *Let φ be a nonsingular symmetric bilinear form on V, where V is an n-dimensional vector space over $\mathbb{C}$. Then φ is isometric to $[1] \perp \cdots \perp [1]$. In particular, any two such forms are isometric.*

Proof. By Theorem 6.2.26, $V = V_1 \perp \cdots \perp V_n$ where V_i has basis $\{v_i\}$. Let $a_i = \varphi(v_i, v_i)$. If b_i is a complex number with $b_i^2 = 1/a_i$ and $\mathcal{B}$ is the basis $\mathcal{B} = \{b_1 v_1, \ldots, b_n v_n\}$ of V, then

$$[\varphi]_{\mathcal{B}} = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}. \qquad \square$$

The classification of symmetric forms over $\mathbb{R}$, or Hermitian forms over $\mathbb{C}$, is more interesting. Whether we can solve $b_i^2 = 1/a_i$ over $\mathbb{R}$, or $b_i \overline{b_i} = 1/a_i$ over $\mathbb{C}$, comes down to the sign of a_i. (Recall that in the Hermitian case a_i must be real.)

Before developing this classification, we introduce a notion interesting and important in itself.

DEFINITION 6.2.28. Let φ be a symmetric bilinear form on the real vector space V, or a Hermitian form on the complex vector space V. Then φ is *positive definite* if $\varphi(v, v) > 0$ for every $v \in V$, $v \neq 0$, and φ is *negative definite* if $\varphi(v, v) < 0$ for every $v \in V$, $v \neq 0$. It is *indefinite* if there are vectors $v_1, v_2 \in V$ with $\varphi(v_1, v_1) > 0$ and $\varphi(v_2, v_2) < 0$. $\diamond$

Theorem 6.2.29 (Sylvester's law of inertia)**.** *Let V be a finite-dimensional real vector space and let φ be a nonsingular symmetric bilinear form on V, or let V be a finite-dimensional complex vector space and let φ be a nonsingular Hermitian form on V. Then φ is isometric to $p[1] \perp q[-1]$ for well-defined integers p and q with $p + q = n = \dim(V)$.*

Proof. As in the proof of Corollary 6.2.27, we have that φ is isometric to $p[1] \perp q[-1]$ for some integers p and q with $p + q = n$. We must show that p and q are well-defined.

To do so, let V_+ be a subspace of V of largest dimension with $\varphi|V_+$ positive definite and let V_- be a subspace of V of largest dimension with $\varphi|V_-$ negative definite. Let $p_0 = \dim(V_+)$ and $q_0 = \dim(V_-)$. Clearly p_0 and q_0 are well-defined. We shall show that $p = p_0$ and $q = q_0$. We argue by contradiction.

Let $\mathcal{B}$ be a basis of V with $[\varphi]_{\mathcal{B}} = p[1] \perp q[-1]$. If $\mathcal{B} = \{v_1, \ldots, v_n\}$, let $\mathcal{B}_+ = \{v_1, \ldots, v_p\}$ and $\mathcal{B}_- = \{v_{p+1}, \ldots, v_n\}$. If W_+ is the space spanned by $\mathcal{B}_+$, then $\varphi|W_+$ is positive definite, so $p_0 \geq p$. If W_- is the space spanned by $\mathcal{B}_-$, then $\varphi|W_-$ is negative definite, so $q_0 \geq q$. Now $p + q = n$, so $p_0 + q_0 \geq n$. Suppose it is not the case that $p = p_0$ and $q = q_0$. Then $p_0 + q_0 > n$, i.e., $\dim(V_+) + \dim(V_-) > n$. Then $V_+ \cap V_-$ has dimension at least one, so contains a nonzero vector v. Then $\varphi(v, v) > 0$ as $v \in V_+$, but $\varphi(v, v) < 0$ as $v \in V_-$, which is impossible. □

We make part of the proof explicit.

Corollary 6.2.30. *Let V and φ be as in Theorem 6.2.29. Let p_0 be the largest dimension of a subspace V_+ of V with $\varphi|V_+$ positive definite and let q_0 be the largest dimension of a subspace V_- of V with $\varphi|V_-$ negative definite. If φ is isometric to $p[1] \perp q[-1]$, then $p = p_0$ and $q = q_0$. In particular, φ is positive definite if and only if φ is isometric to $n[1]$.*

We can now define a very important invariant of these forms.

DEFINITION 6.2.31. Let V, φ, p, and q be as in Theorem 6.2.29. Then the *signature* of φ is $p - q$. ◇

Corollary 6.2.32. *A nonsingular symmetric bilinear form on a finite-dimensional vector space V over $\mathbb{R}$, or a nonsingular Hermitian form on a finite-dimensional vector space V over $\mathbb{C}$, is classified up to isometry by its rank and signature.*

REMARK 6.2.33. Here is one way in which these notions appear. Let $f : \mathbb{R}^n \to \mathbb{R}$ be a C^2 function and let x_0 be a critical point of f. Let H be the Hessian matrix of f at x_0. Then f has a local minimum at x_0 if H is positive definite and a local maximum at x_0 if H is negative definite. If H is indefinite, then x_0 is neither a local maximum nor a local minimum for f. ◇

We have the following useful criterion.

Theorem 6.2.34 (Hurwitz's criterion)**.** *Let φ be a nonsingular symmetric bilinear form on the n-dimensional complex vector space V. Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be an arbitrary basis of V and let $A = [\varphi]_{\mathcal{B}}$. Let $\delta_0(A) = 1$ and for $1 \leq k \leq n$ let $\delta_k(A) = \det(A_k)$ where A_k is the k-by-k submatrix in the upper left corner of A. Then*

(1) φ is positive definite if and only if $\delta_k(A) > 0$ for $k = 1, \ldots, n$.

(2) φ is negative definite if and only if $(-1)^k \delta_k(A) > 0$ for $k = 1, \ldots, n$.

(3) If $\delta_k(A) \neq 0$ for $k = 1, \ldots, n$, then the signature of φ is $r - s$, where

$$r = \#\{k \mid \delta_k(A) \text{ and } \delta_{k-1}(A) \text{ have the same sign}\}$$
$$s = \#\{k \mid \delta_k(A) \text{ and } \delta_{k-1}(A) \text{ have opposite signs}\}.$$

Proof. We prove (1). Then (2) follows immediately by considering the form $-\varphi$. We leave (3) to the reader; it can be proved using the ideas of the proof of (1).

We prove the theorem by induction on $n = \dim(V)$. If $n = 1$, the theorem is clear: φ is positive definite if and only if $[\varphi]_{\mathcal{B}} = [a_1]$ with $a_1 > 0$. Suppose the theorem is true for all forms on vector spaces of dimension $n - 1$ and let V have dimension n. Let V_{n-1} be the subspace of V spanned by $\mathcal{B}_{n-1} = \{v_1, \ldots, v_{n-1}\}$, so that $A_{n-1} = [\varphi | V_{n-1}]_{\mathcal{B}_{n-1}}$.

Suppose φ is positive definite. Then $\varphi | V_{n-1}$ is also positive definite (if $\varphi(v, v) > 0$ for all $v \neq 0$ in V, then $\varphi(v, v) > 0$ for all $v \in V_{n-1}$). By the inductive hypothesis $\delta_1(A), \ldots, \delta_{n-1}(A)$ are all positive. Also, since $\delta_{n-1}(A) \neq 0$, $\varphi | V_{n-1}$ is nonsingular. Hence $V = V_{n-1} \perp V_{n-1}^{\perp}$, where $V_{n-1}^{\perp}$ is a 1-dimensional subspace generated by a vector w_n. Let $b_{nn} = \varphi(w_n, w_n)$, so $b_{nn} > 0$.

Let $\mathcal{B}'$ be the basis $\{v_1, \ldots, v_{n-1}, w_n\}$. Then

$$\det([\varphi]_{\mathcal{B}'}) = \delta_{n-1}(A) b_{nn} > 0.$$

By Theorem 6.1.14, if P is the change of basis matrix $P_{\mathcal{B}' \leftarrow \mathcal{B}}$, then

$$\begin{aligned} \det\big([\varphi]_{\mathcal{B}'}\big) &= \det(P)^2 \det(A) = \det(P)^2 \delta_n(A) \quad \text{if } \varphi \text{ is symmetric} \\ &= \det(P)\overline{\det(P)} \det(A) = \big|\det(P)\big|^2 \delta_n(A) \quad \text{if } \varphi \text{ is Hermitian} \end{aligned}$$

and in any case $\delta_n(A)$ has the same sign as $\det([\varphi]_{\mathcal{B}'})$, so $\delta_n(A) > 0$.

Suppose that $\delta_1(A), \ldots, \delta_{n-1}(A)$ are all positive. By the inductive hypothesis $\varphi | V_{n-1}$ is positive definite. Again let $V = V_{n-1} \perp V_{n-1}^{\perp}$ with w_n as above. If $b_{nn} = \varphi(w_n, w_n) > 0$ then φ is positive definite. The same argument shows that $\delta_{n-1}(A) b_{nn}$ has the same sign as $\delta_n(A)$. But $\delta_{n-1}(A)$ and $\delta_n(A)$ are both positive, so $b_{nn} > 0$. □

Here is a general formula for the signature of φ.

Theorem 6.2.35. *Let φ be a nonsingular symmetric bilinear form on the n-dimensional real vector space V or a nonsingular Hermitian form on the n-dimensional complex vector space V. Let $\mathcal{B}$ be a basis for φ and let $A = [\varphi]_{\mathcal{B}}$. Then*

(1) A has n real eigenvalues (counting multiplicity), and

(2) the signature of φ is $r-s$, where r is the number of positive eigenvalues and s is the number of negative eigenvalues of A.

Proof. To prove this we need a result from the next chapter, Corollary 7.3.20, that states that every symmetric matrix is orthogonally diagonalizable and that every Hermitian matrix is unitarily diagonalizable. In other words, if A is symmetric then there is an orthogonal matrix P, i.e., a matrix with ${}^tP = P^{-1}$, such that $D = PAP^{-1}$ is diagonal, and if A is Hermitian there is a unitary matrix P, i.e., a matrix with ${}^t\overline{P} = P^{-1}$, such that $D = PAP^{-1}$ is diagonal (necessarily with real entries). In both cases the diagonal entries of D are the eigenvalues of A and $D = [\varphi]_{\mathcal{C}}$ for some basis $\mathcal{C}$.

Thus we see that $r-s$ is the number of positive entries on the diagonal of D minus the number of negative entries on the diagonal of D.

Let $\mathcal{C} = \{v_1, \dots, v_n\}$. Reordering the elements of $\mathcal{C}$ if necessary, we may assume that the first r diagonal entries of D are positive and the remaining $s = n-r$ diagonal entries of D are negative. Then $V = W_1 \perp W_2$ where W_1 is the subspace spanned by $\{v_1, \dots, v_r\}$ and W_2 is the subspace spanned by $\{v_{r+1}, \dots, v_n\}$. Then $\varphi|W_1$ is positive definite and $\varphi|W_2$ is negative definite, so the signature of φ is equal to $\dim(W_1) - \dim(W_2) = r-s$. □

Closely related to symmetric bilinear forms are quadratic forms.

DEFINITION 6.2.36. Let V be a vector space over $\mathbb{F}$. A *quadratic form* on V is a function $\Phi : V \to \mathbb{F}$ satisfying

(1) $\Phi(av) = a^2\Phi(v)$ for any $a \in \mathbb{F}$, $v \in V$

(2) the function $\varphi : V \times V \to \mathbb{F}$ defined by

$$\varphi(x, y) = \Phi(x+y) - \Phi(x) - \Phi(y)$$

is a (necessarily symmetric) bilinear form on V. We say that Φ and φ are *associated.* ◇

Lemma 6.2.37. *Let V be a vector space over $\mathbb{F}$ with $\mathrm{char}(\mathbb{F}) \neq 2$. Then every quadratic form Φ is associated to a unique symmetric bilinear form, and conversely.*

Proof. Clearly Φ determines φ. On the other hand, suppose that φ is associated to Φ. Then $4\Phi(x) = \Phi(2x) = \Phi(x+x) = 2\Phi(x) + \varphi(x, x)$

so

$$\Phi(x) = \frac{1}{2}\varphi(x, x)$$

and φ determines Φ as well. $\square$

In characteristic 2 the situation is considerably more subtle and we simply state the results without proof. For an integer m let $e(m) = 2^{m-1}(2^m + 1)$ and $o(m) = 2^{m-1}(2^m - 1)$.

Theorem 6.2.38. *(1) Let φ be a symmetric bilinear form on a vector space V of dimension n over the field $\mathbb{F}$ of 2 elements. Then φ is associated to a quadratic form Φ if and only if φ is even (in the sense of Definition 6.2.21). In this case there are 2^n quadratic forms associated to φ. Each such quadratic form Φ is called a quadratic refinement of φ.*

(2) Let φ be a nonsingular even symmetric bilinear form on a vector space V of necessarily even dimension $n = 2m$ over $\mathbb{F}$, and let Φ be a quadratic refinement of φ.

The Arf *invariant of Φ is defined as follows: Let $|\cdot|$ denote the cardinality of a set. Then either*

$$\left|\Phi^{-1}(0)\right| = e(m) \quad \textit{and} \quad \left|\Phi^{-1}(1)\right| = o(m), \quad \textit{in which case } \operatorname{Arf}(\Phi) = 0,$$

or

$$\left|\Phi^{-1}(0)\right| = o(m) \quad \textit{and} \quad \left|\Phi^{-1}(1)\right| = e(m), \quad \textit{in which case } \operatorname{Arf}(\Phi) = 1.$$

Then there are $e(m)$ quadratic refinements Φ of φ with $\operatorname{Arf}(\Phi) = 0$ and $o(m)$ quadratic refinements Φ of φ with $\operatorname{Arf}(\Phi) = 1$.

(3) Quadratic refinements of a nonsingular even symmetric bilinear form on a finite-dimensional vector space V are classified up to isometry by their rank $(= \dim(V))$ and Arf *invariant.*

Proof. Omitted. $\square$

EXAMPLE 6.2.39. We now give a classical application of our earlier results. Let

$$V = \mathbb{F}^n = \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \right\},$$

$\mathbb{F}$ a field of characteristic $\neq 2$, and suppose we have a function $Q : V \to \mathbb{F}$ of the form

$$Q\left(\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}\right) = \frac{1}{2}\sum_i a_{ii}x_i^2 + \sum_{i<j} a_{ij}x_i x_j.$$

Then Q is a quadratic form associated to the symmetric bilinear form q where $[q]_{\mathcal{E}}$ is the matrix $A = (a_{ij})$. Then $[q]_{\mathcal{E}}$ is diagonalizable, and that provides a diagonalization of Q in the obvious sense. In other words, there is a nonsingular change of variable

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \mapsto \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} \quad \text{such that } Q\left(\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}\right) = \sum_i b_{ii}y_i^2$$

for some $b_{11}, b_{22}, \ldots, b_{nn} \in \mathbb{F}$. If $\mathbb{F} = \mathbb{R}$ we may choose each $b_{ii} = \pm 1$.

Most interesting is the following: Let $\mathbb{F} = \mathbb{R}$ and suppose that

$$Q\left(\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}\right) > 0 \quad \text{whenever } \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \neq \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Then q is positive definite, and we call Q positive definite in this case as well. We then see that for an appropriate change of variable

$$Q\left(\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}\right) = \sum_{i=1}^n y_i^2.$$

That is, over $\mathbb{R}$ every positive definite quadratic form can be expressed as a sum of squares. $\diamond$

Let us now classify skew-symmetric bilinear forms.

Theorem 6.2.40. *Let V be a vector space of finite dimension n over an arbitrary field $\mathbb{F}$, and let φ be a nonsingular skew-symmetric bilinear form on V. Then n is even and φ is isometric to $(n/2)\left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$, or, equivalently, to $\left[\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right]$, where I is the $(n/2)$-by-$(n/2)$ identity matrix.*

Proof. We proceed by induction on n. If $n = 1$ and φ is skew-symmetric, then we must have $[\varphi]_{\mathcal{B}} = [0]$, which is singular, so that case cannot occur.

Suppose the theorem is true for all vector spaces of dimension less than n and let V have dimension n.

Choose $v_1 \in V$, $v_1 \neq 0$. Then, since φ is nonsingular, there exists $w \in V$ with $\varphi(w, v_1) = a \neq 0$, and w is not a multiple of v_1 as φ is skew-symmetric. Let $v_2 = (1/a)w$, let $\mathcal{B}_1 = \{v_1, v_2\}$, and let V_1 be the subspace of V spanned by $\mathcal{B}_1$. Then $[\varphi|V_1]_{\mathcal{B}_1} = [\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}]$. V_1 is a nonsingular subspace so, by Lemma 6.2.16, $V = V_1 \perp V_1^{\perp}$. Now $\dim(V_1^{\perp}) = n - 2$ so we may assume by induction that $V_1^{\perp}$ has a basis $\mathcal{B}_2$ with $[\varphi|V_1^{\perp}]_{\mathcal{B}_2} = ((n-2)/2)[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}]$. Let $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$. Then $[\varphi]_{\mathcal{B}} = (n/2)[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}]$.

Finally, if $\mathcal{B} = \{v_1, \ldots, v_n\}$, let $\mathcal{B}' = \{v_1, v_3, \ldots, v_{n-1}, v_2, v_4, \ldots, v_n\}$. Then $[\varphi]_{\mathcal{B}'} = [\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}]$. □

Finally, we consider skew-Hermitian forms. In this case, by convention, the field $\mathbb{F}$ of scalars has $\operatorname{char}(\mathbb{F}) \neq 2$. We begin with a result about $\mathbb{F}$ itself.

Lemma 6.2.41. *Let $\mathbb{F}$ be a field with $\operatorname{char}(\mathbb{F}) \neq 2$ equipped with a nontrivial conjugation $c \mapsto \overline{c}$. Then:*

(1) $\mathbb{F}_0 = \{c \in \mathbb{F} \mid \overline{c} = c\}$ is a subfield of $\mathbb{F}$.

(2) There is a nonzero element $j \in \mathbb{F}$ with $\overline{j} = -j$.

(3) Every element of $\mathbb{F}$ can be written uniquely as $c = c_1 + jc_2$ with $c_1, c_2 \in \mathbb{F}$ (so that $\mathbb{F}$ is a 2-dimensional $\mathbb{F}_0$-vector space with basis $\{1, j\}$). In particular, $\overline{c} = -c$ if and only if $c = c_2 j$ for some $c_2 \in \mathbb{F}_0$.

Proof. (1) is easy to check. (Note that $\overline{1} = \overline{(1 \cdot 1)} = \overline{1} \cdot \overline{1}$ so $\overline{1} = 1$.)

(2) Let c be any element of $\mathbb{F}$ with $\overline{c} \neq c$ and let $j = (c - \overline{c})/2$.

(3) Observe that $c = c_1 + jc_2$ with $c_1 = (c + \overline{c})/2$ and $c_2 = (c - \overline{c})/2j$. It is easy to check that $c_1, c_2 \in \mathbb{F}_0$.

Also, if $c = c_1 + c_2 j$ with $c_1, c_2 \in \mathbb{F}_0$, then $\overline{c} = c_1 - jc_2$ and, solving for c_1 and c_2, we obtain $c_1 = (c + \overline{c})/2$ and $c_2 = (c - \overline{c})/2j$. □

REMARK 6.2.42. If $\mathbb{F} = \mathbb{C}$ and the conjugation is complex conjugation, $\mathbb{F}_0 = \mathbb{R}$ and we may choose $j = i$. ◇

Theorem 6.2.43. *Let V be a finite-dimensional vector space and let φ be a nonsingular skew-Hermitian form on V. Then φ is diagonalizable, i.e., φ is isometric to $[a_1] \perp \ldots \perp [a_n]$ with $a_i \in \mathbb{F}$, $a_i \neq 0$, $\overline{a_i} = -a_i$, or equivalently $a_i = jb_i$ with $b_i \in \mathbb{F}_0$, $b_i \neq 0$, for each i.*

Proof. First we claim there is a vector $v \in V$ with $\varphi(v, v) \neq 0$. Choose $v_1 \in V$, $v_1 \neq 0$, arbitrarily. If $\varphi(v_1, v_1) \neq 0$, choose $v = v_1$. Otherwise, since φ is nonsingular there is a vector $v_2 \in V$ with $\varphi(v_1, v_2) = a \neq 0$.

(Then $\varphi(v_2, v_1) = -\overline{a}$.) If $\varphi(v_2, v_2) \neq 0$, choose $v = v_2$. Otherwise, for any $c \in \mathbb{F}$, let $v_3 = v_1 + \overline{c}v_2$. We easily compute that $\varphi(v_3, v_3) = ac - \overline{a}\,\overline{c} = ac - (\overline{ac})$. Thus if we let $v = v_1 + (j/a)v_2$, $\varphi(v, v) \neq 0$.

Now proceed as in the proof of Theorem 6.2.26. $\square$

Corollary 6.2.44. *Let V be a complex vector space of dimension n and let φ be a nonsingular skew-Hermitian form on V. Then φ is isometric to $r[i] \perp s[-i]$ for well-defined integers r and s with $r + s = n$.*

Proof. By Theorem 6.2.43, V has a basis $\mathcal{B} = \{v_1, \dots, v_n\}$ with $[\varphi]_{\mathcal{B}}$ diagonal with entries $ib_1, \dots, ib_n$ for nonzero real numbers $b_1, \dots, b_n$. Letting $\mathcal{B}' = \{v_1', \dots, v_n'\}$ with $v_i' = (\sqrt{1/|b_i|})v_i$ we see that $[\varphi]_{\mathcal{B}'}$ is diagonal with all diagonal entries $\pm i$. It remains to show that the numbers r of $+i$ and s of $-i$ entries are well-defined.

The proof is almost identical to the proof of Theorem 6.2.29, the only difference being that instead of considering $\varphi(v, v)$ we consider $(1/i)\varphi(v, v)$. $\square$

6.3 THE ADJOINT OF A LINEAR TRANSFORMATION

We now return to the general situation. We assume in this section that (V, φ) and (W, ψ) are nonsingular, where the forms φ and ψ are either both bilinear or both sesquilinear. Given a linear transformation $\mathcal{T} : V \to W$, we define its adjoint $\mathcal{T}^{\text{adj}} : W \to V$. We then investigate properties of the adjoint.

DEFINITION 6.3.1. Let $\mathcal{T} : V \to W$ be a linear transformation. The adjoint of $\mathcal{T}$ is the linear transformation $\mathcal{T}^{\text{adj}} : W \to V$ defined by

$$\psi\big(\mathcal{T}(x), y\big) = \varphi\big(x, \mathcal{T}^{\text{adj}}(y)\big) \quad \text{for all } x \in V,\ y \in W. \qquad \diamond$$

This is a rather complicated definition, and the first thing we need to see is that it in fact makes sense.

Lemma 6.3.2. *$\mathcal{T}^{\text{adj}} : W \to V$, as given in Definition 6.3.1, is a well-defined linear transformation.*

Proof. We give two proofs, the first more concrete and the second more abstract.

The first proof proceeds in two steps. The first step is to observe that the formula $\varphi(x, z) = \psi(\mathcal{T}(x), y)$, where $x \in V$ is arbitrary and $y \in W$ is any fixed element, defines a unique element z of V, since φ is nonsingular. Hence $\mathcal{T}^{\text{adj}}(y) = z$ is well-defined. The second step is to show that $\mathcal{T}^{\text{adj}}$ is a linear transformation. We compute, for $x \in V$ arbitrary,

$$\begin{aligned}\varphi\big(x, \mathcal{T}^{\text{adj}}(y_1 + y_2)\big) &= \psi\big(\mathcal{T}(x), y_1 + y_2\big) = \psi\big(\mathcal{T}(x), y_1\big) + \psi\big(\mathcal{T}(x), y_2\big) \\ &= \varphi\big(x, \mathcal{T}^{\text{adj}}(y_1)\big) + \varphi\big(x, \mathcal{T}^{\text{adj}}(y_2)\big)\end{aligned}$$

and

$$\begin{aligned}\varphi\big(x, \mathcal{T}^{\text{adj}}(cy)\big) &= \psi\big(\mathcal{T}(x), cy\big) = \bar{c}\,\psi\big(\mathcal{T}(x), y\big) \\ &= \bar{c}\,\varphi\big(x, \mathcal{T}^{\text{adj}}(y)\big) = \varphi\big(x, c\mathcal{T}^{\text{adj}}(y)\big).\end{aligned}$$

For the second proof, we first consider the bilinear case. The formula in Definition 6.3.1 is equivalent to

$$\alpha_\varphi\big(\mathcal{T}^{\text{adj}}(y)\big)(x) = \alpha_\psi(y)\big(\mathcal{T}(x)\big) = \mathcal{T}^*\big(\varphi_\psi(y)\big)(x),$$

where $\mathcal{T}^* : W^* \to V^*$ is the dual of $\mathcal{T}$, which gives

$$\mathcal{T}^{\text{adj}} = \alpha_\varphi^{-1} \circ \mathcal{T}^* \circ \alpha_\psi.$$

In the sesquilinear case we have a bit more work to do, since α_φ and α_ψ are conjugate linear rather than linear. The formula in Definition 6.3.1 is equivalent to $\overline{\psi(\mathcal{T}(x), y)} = \overline{\varphi(x, \mathcal{T}^{\text{adj}}(y))}$. Define $\alpha_{\overline{\varphi}}$ by $\alpha_{\overline{\varphi}}(y)(x) = \overline{\varphi(x, y)}$, and define $\alpha_{\overline{\psi}}$ similarly. Then $\alpha_{\overline{\varphi}}$ and $\alpha_{\overline{\psi}}$ are linear transformations and by the same logic we obtain

$$\mathcal{T}^{\text{adj}} = \alpha_{\overline{\varphi}}^{-1} \circ \mathcal{T}^* \circ \alpha_{\overline{\psi}}. \qquad \square$$

REMARK 6.3.3. $\mathcal{T}^{\text{adj}}$ is often denoted by $\mathcal{T}^*$, but we will not use that notation in this section as we are also considering $\mathcal{T}^*$, the dual of $\mathcal{T}$, here. $\diamond$

Suppose V and W are finite dimensional. Then, since $\mathcal{T}^{\text{adj}} : W \to V$ is a linear transformation, once we have chosen bases, we may represent $\mathcal{T}^{\text{adj}}$ by a matrix.

Lemma 6.3.4. *Let $\mathcal{B}$ and $\mathcal{C}$ be bases of V and W respectively and let $P = [\varphi]_{\mathcal{B}}$ and $Q = [\psi]_{\mathcal{C}}$. Then*

$$\big[\mathcal{T}^{\text{adj}}\big]_{\mathcal{B}\leftarrow\mathcal{C}} = P^{-1}\,{}^t[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}\,Q \quad \textit{if } \varphi \textit{ and } \psi \textit{ are bilinear,}$$

and

$$\big[\mathcal{T}^{\text{adj}}\big]_{\mathcal{B}\leftarrow\mathcal{C}} = \overline{P}^{-1}\,\overline{{}^t[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}}\,\overline{Q} \quad \textit{if } \varphi \textit{ and } \psi \textit{ are sesquilinear.}$$

In particular, if $V = W$, $\varphi = \psi$ and $\mathcal{B} = \mathcal{C}$, and $P = [\varphi]_{\mathcal{B}}$, then

$$\left[\mathcal{T}^{\mathrm{adj}}\right]_{\mathcal{B}} = P^{-1}\,{}^t[\mathcal{T}]_{\mathcal{B}}P \quad \textit{if } \varphi \textit{ is bilinear,}$$

and

$$\left[\mathcal{T}^{\mathrm{adj}}\right]_{\mathcal{B}} = \overline{P}^{-1}\,{}^t\overline{[\mathcal{T}]_{\mathcal{B}}}\,\overline{P} \quad \textit{if } \varphi \textit{ is sesquilinear.}$$

Proof. Again we give two proofs, the first more concrete and the second more abstract.

For the first proof, let $[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}} = M$ and $[\mathcal{T}^{\mathrm{adj}}]_{\mathcal{C}\leftarrow\mathcal{B}} = N$. Then

$$\psi\big(\mathcal{T}(x), y\big) = \big\langle\mathcal{T}(x), y\big\rangle = {}^t\big(M[x]_{\mathcal{B}}\big)Q\overline{[y]}_{\mathcal{C}} = {}^t[x]_{\mathcal{B}}\,{}^tMQ\overline{[y]}_{\mathcal{C}}$$

and

$$\varphi\big(x, \mathcal{T}^{\mathrm{adj}}(y)\big) = \big\langle x, \mathcal{T}^{\mathrm{adj}}(y)\big\rangle = {}^t[x]_{\mathcal{B}}P\big(\overline{N[y]_{\mathcal{C}}}\big) = {}^t[x]_{\mathcal{B}}P\overline{N}\,\overline{[y]}_{\mathcal{C}}$$

from which we obtain

$${}^tMQ = P\overline{N} \quad \text{and hence} \quad N = \overline{P}^{-1}\,{}^t\overline{M}\,\overline{Q}.$$

For the second proof, let $\mathcal{B} = \{v_1, v_2, \ldots\}$ and set $\overline{\mathcal{B}} = \{\overline{v}_1, \overline{v}_2, \ldots\}$. Then, keeping track of conjugations, we know from the second proof of Lemma 6.3.2 that

$$[\mathcal{T}^{\mathrm{adj}}]_{\mathcal{B}\leftarrow\mathcal{C}} = \big([\alpha_{\overline{\varphi}}]_{\overline{\mathcal{B}}^*\leftarrow\mathcal{B}}\big)^{-1}[\mathcal{T}^*]_{\overline{\mathcal{B}}^*\leftarrow\overline{\mathcal{C}}^*}[\alpha_{\overline{\psi}}]_{\overline{\mathcal{C}}^*\leftarrow\mathcal{C}}.$$

But $[\alpha_{\overline{\varphi}}]_{\overline{\mathcal{B}}^*\leftarrow\mathcal{B}} = \overline{P}$, $[\alpha_{\overline{\psi}}]_{\overline{\mathcal{C}}^*\leftarrow\mathcal{C}} = \overline{Q}$, and from Definition 2.4.1 and Lemma 2.4.2 we see that $[\mathcal{T}^*]_{\overline{\mathcal{B}}^*\leftarrow\overline{\mathcal{C}}^*} = {}^t[\mathcal{T}]_{\overline{\mathcal{C}}\leftarrow\overline{\mathcal{B}}} = \overline{{}^t[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}}$. □

In one very important case this simplifies.

DEFINITION 6.3.5. Let V be a vector space and let φ be a form on V. A basis $\mathcal{B} = \{v_1, v_2, \ldots\}$ of V is *orthonormal* if $\varphi(v_i, v_j) = \varphi(v_j, v_i) = 1$ if $i = j$ and 0 if $i \neq j$. ◇

REMARK 6.3.6. We see from Corollary 6.2.30 that if $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$ then V has an orthonormal basis if and only if φ is real symmetric or complex Hermitian, and positive definite in either case. ◇

Corollary 6.3.7. *Let V and W be finite-dimensional vector spaces with orthonormal bases $\mathcal{B}$ and $\mathcal{C}$ respectively. Let $\mathcal{T} : V \to W$ be a linear transformation. Then*

$$[\mathcal{T}^{\mathrm{adj}}]_{\mathcal{B}\leftarrow\mathcal{C}} = {}^t[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}} \quad \textit{if } \varphi \textit{ and } \psi \textit{ are bilinear}$$

and

$$[\mathcal{T}^{\mathrm{adj}}]_{\mathcal{B}\leftarrow\mathcal{C}} = \overline{{}^t[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}} \quad \text{if } \varphi \text{ and } \psi \text{ are sesquilinear.}$$

In particular, if $\mathcal{T} : V \to V$ *then*

$$[\mathcal{T}^{\mathrm{adj}}]_{\mathcal{B}} = {}^t[\mathcal{T}]_{\mathcal{B}} \quad \text{if } \varphi \text{ is bilinear}$$

and

$$[\mathcal{T}^{\mathrm{adj}}]_{\mathcal{B}} = \overline{{}^t[\mathcal{T}]_{\mathcal{B}}} \quad \text{if } \varphi \text{ is sesquilinear.}$$

Proof. In this case, both P and Q are identity matrices. □

REMARK 6.3.8. There is an important generalization of the definition of the adjoint. We have seen in the proof of Lemma 6.3.2 that $\mathcal{T}^{\mathrm{adj}}$ is defined by $\alpha_{\overline{\varphi}} \circ \mathcal{T}^{\mathrm{adj}} = \mathcal{T} \circ \alpha_{\overline{\psi}}$. Suppose now that $\alpha_{\overline{\varphi}}$, or equivalently α_{φ}, is injective but not surjective, which may occur when V is infinite dimensional. Then $\mathcal{T}^{\mathrm{adj}}$ may not be defined. But if $\mathcal{T}^{\mathrm{adj}}$ is defined, then it is well-defined, i.e., if there is a linear transformation $\mathcal{S} : W \to V$ satisfying $\varphi(\mathcal{T}(x), y) = \psi(x, \mathcal{S}(y))$ for every $x \in V$, $y \in W$, then there is a unique such linear transformation $\mathcal{S}$, and we set $\mathcal{T}^{\mathrm{adj}} = \mathcal{S}$. ◇

REMARK 6.3.9. (1) It is obvious, but worth noting, that if α_{φ} is injective the identity $\mathcal{I} : V \to V$ has adjoint $\mathcal{I}^* = \mathcal{I}$, as $\varphi(\mathcal{I}(x), y) = \varphi(x, y) = \varphi(x, \mathcal{I}(y))$ for every $x, y \in V$.

(2) On the other hand, if α_{φ} is not injective there is no hope of defining an adjoint. For suppose $V_0 = \mathrm{Ker}(\alpha_{\varphi}) \neq \{0\}$. Let $\mathcal{P}_0 : W \to V$ be any linear transformation with $\mathcal{P}_0(W) \subseteq V_0$. If $\mathcal{S} : W \to V$ is a linear transformation with $\psi(\mathcal{T}(x), y) = \varphi(x, \mathcal{S}(y))$, then $\mathcal{S}' = \mathcal{S} + \mathcal{P}_0$ also satisfies $\psi(\mathcal{T}(x), y) = \varphi(x, \mathcal{S}'(y))$ for $x \in V$, $y \in W$. ◇

We state some basic properties of adjoints.

Lemma 6.3.10. *(1) Suppose* $\mathcal{T}_1 : V \to W$ *and* $\mathcal{T}_2 : V \to W$ *both have adjoints. Then* $\mathcal{T}_1 + \mathcal{T}_2 : V \to W$ *has an adjoint and* $(\mathcal{T}_1 + \mathcal{T}_2)^{\mathrm{adj}} = \mathcal{T}_1^{\mathrm{adj}} + \mathcal{T}_2^{\mathrm{adj}}$.

(2) Suppose $\mathcal{T} : V \to W$ *has an adjoint. Then* $c\mathcal{T} : V \to W$ *has an adjoint and* $(c\mathcal{T})^{\mathrm{adj}} = \overline{c}\,\mathcal{T}^{\mathrm{adj}}$.

(3) Suppose $\mathcal{S} : V \to W$ *and* $\mathcal{T} : W \to X$ *both have adjoints. Then* $\mathcal{T} \circ \mathcal{S} : V \to X$ *has an adjoint and* $(\mathcal{T} \circ \mathcal{S})^{\mathrm{adj}} = \mathcal{S}^{\mathrm{adj}} \circ \mathcal{T}^{\mathrm{adj}}$.

(4) Suppose $\mathcal{T} : V \to V$ *has an adjoint. Then for any polynomial* $p(x) \in \mathbb{F}[x]$, $p(\mathcal{T})$ *has an adjoint and* $(p(\mathcal{T}))^{\mathrm{adj}} = \overline{p}(\mathcal{T}^{\mathrm{adj}})$.

Lemma 6.3.11. *Suppose that φ and ψ are either both symmetric, both Hermitian, both skew-symmetric, or both skew-Hermitian. If $\mathcal{T} : V \to W$ has an adjoint, then $\mathcal{T}^{\mathrm{adj}} : W \to V$ has an adjoint and $(\mathcal{T}^{\mathrm{adj}})^{\mathrm{adj}} = \mathcal{T}$.*

Proof. We prove the Hermitian case, which is typical. Let $\mathcal{S} = \mathcal{T}^{\mathrm{adj}}$. By definition, $\psi(\mathcal{T}(x), y) = \varphi(x, \mathcal{S}(y))$ for $x \in V$, $y \in W$. Now $\mathcal{S}$ has an adjoint $\mathcal{R}$ if and only if $\varphi(\mathcal{S}(y), x) = \psi(y, \mathcal{R}(x))$. But

$$\varphi\big(\mathcal{S}(y), x\big) = \overline{\varphi\big(x, \mathcal{S}(y)\big)} = \overline{\psi\big(\mathcal{T}(x), y\big)} = \psi\big(y, \mathcal{T}(x)\big)$$

so $\mathcal{R} = \mathcal{T}$, i.e., $(\mathcal{T}^{\mathrm{adj}})^{\mathrm{adj}} = \mathcal{T}$. $\square$

We will present a number of interesting examples of and related to adjoints in Section 7.3 and in Section 7.4.

CHAPTER 7

Real and complex inner product spaces

In this chapter we consider real and complex vector spaces equipped with an inner product. An inner product is a special case of a symmetric bilinear form, in the real case, or of a Hermitian form, in the complex case. But it is a very important special case, one in which much more can be said than in general.

7.1 Basic definitions

We begin by defining the objects we will be studying.

Definition 7.1.1. An *inner product* $\varphi(x, y) = \langle x, y \rangle$ on a real vector space V is a symmetric bilinear form with the property that $\langle v, v \rangle > 0$ for every $v \in V$, $v \neq 0$.

An *inner product* $\varphi(x, y) = \langle x, y \rangle$ on a complex vector space V is a Hermitian form with the property that $\langle v, v \rangle > 0$ for every $v \in V$, $v \neq 0$.

A real or complex vector space equipped with an inner product is an *inner product space*. ◇

Example 7.1.2. (1) The cases $\mathbb{F} = \mathbb{R}$ and $\mathbb{C}$ of Example 6.1.5(1) give inner product spaces.

(2) Let $\mathbb{F} = \mathbb{R}$ and let A be a real symmetric matrix (i.e., ${}^tA = A$), or let $\mathbb{F} = \mathbb{C}$ and let A be a complex Hermitian matrix (i.e., ${}^tA = \overline{A}$) in Example 6.1.5(2). Then we obtain inner product spaces if and only if A is positive definite.

(3) Let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$ in Example 6.1.5(3).

(4) Example 6.1.5(4). ◇

In this chapter we let $\mathbb{F}$ be $\mathbb{R}$ or $\mathbb{C}$. We will frequently state and prove results only in the complex case when the real case can be obtained by ignoring the conjugation.

Let us begin by relating inner products to the forms we considered in Chapter 6.

Lemma 7.1.3. *Let φ be an inner product on the finite-dimensional real or complex vector space V. Then φ is nonsingular in the sense of Definition 6.1.8.*

Proof. Since $\varphi(y, y) > 0$ for every $y \in V$, $y \neq 0$, we may apply Lemma 6.1.10, choosing $x = y$. □

REMARK 7.1.4. Inner products are particularly nice symmetric or Hermitian forms. One of the ways they are nice is that if φ is such a form on a vector space V, then not only is φ nonsingular but its restriction to any subspace W of V is nonsingular. Conversely, if φ is a form on a real or complex vector space V such that the restriction of φ to any subspace W of V is nonsingular, then either φ or $-\varphi$ must be an inner product. For if neither φ nor $-\varphi$ is an inner product, there are two possibilities: (1) There is a vector w_0 with $\varphi(w_0, w_0) = 0$, or (2) There are vectors w_1 and w_2 with $\varphi(w_1, w_1) > 0$ and $\varphi(w_2, w_2) < 0$. In this case $f(t) = \varphi(tw_1 + (1-t)w_2, tw_1 + (1-t)w_2)$ is a continuous real-valued function with $f(0) > 0$ and $f(1) < 0$, so there is a value t_0 with $f(t_0) = 0$, i.e., $\varphi(w_0, w_0) = 0$ for $w_0 = t_0 w_1 + (1-t_0)w_2$. Then φ is identically 0 on $\mathrm{Span}(\{w_0\})$. ◇

We now turn our attention to norms of vectors.

DEFINITION 7.1.5. Let V be an inner product space. The *norm* $\|v\|$ of a vector $v \in V$ is

$$\|v\| = \sqrt{\langle v, v\rangle}. \qquad \diamond$$

Lemma 7.1.6. *Let V be an inner product space.*

(1) $\|cv\| = |c|\|v\|$ for any $c \in \mathbb{F}$ and any $v \in V$.

(2) $\|v\| \geq 0$ for all $v \in V$ and $\|v\| = 0$ if and only if $v = 0$.

(3) (Cauchy-Schwartz-Buniakowsky inequality) $|\langle v, w\rangle| \leq \|v\|\|w\|$ for all $v, w \in V$, with equality if and only if $\{v, w\}$ is linearly dependent.

(4) (Triangle inequality) $\|v + w\| \leq \|v\| + \|w\|$ for all $v, w \in V$, with equality if and only if $w = 0$ or $v = pw$ for some nonnegative real number p.

Proof. (1) and (2) are immediate.

For (3), if $\{v, w\}$ is linearly dependent then $w = 0$ or $w \neq 0$ and $v = cw$ for some $c \in \mathbb{F}$, and it is easy to check that in both cases we have equality. Assume that $\{v, w\}$ is linearly independent. Then for any $c \in \mathbb{F}$, $x = v - cw \neq 0$, and then direct computation shows that

$$\begin{aligned}0 < \|x\|^2 &= \langle x, x\rangle = \langle v, v\rangle + \langle -cw, v\rangle + \langle v, -cw\rangle + \langle -cw, -cw\rangle \\ &= \langle v, v\rangle - c\overline{\langle v, w\rangle} - \overline{c}\langle v, w\rangle + |c|^2\langle w, w\rangle.\end{aligned}$$

Setting $c = \langle v, w\rangle/\langle w, w\rangle$ gives

$$0 < \langle v, v\rangle - \left|\langle v, w\rangle\right|^2/\langle w, w\rangle,$$

which gives the inequality.

For (4), we have that

$$\begin{aligned}\left\|v + w\right\|^2 &= \langle v + w, v + w\rangle \\ &= \langle v, v\rangle + \langle v, w\rangle + \langle w, v\rangle + \langle w, w\rangle \\ &= \|v\|^2 + \left(\langle v, w\rangle + \overline{\langle v, w\rangle}\right) + \|w\|^2 \\ &\leq \|v\|^2 + 2\left|\langle v, w\rangle\right| + \|w\|^2 \\ &\leq \|v\|^2 + 2\|v\|\|w\| + \|w\|^2 = \left(\|v\| + \|w\|\right)^2,\end{aligned}$$

which gives the triangle inequality. The second inequality in the proof is the Cauchy-Schwartz-Buniakowsky inequality. The first inequality in the proof holds because for a complex number c, $c + \overline{c} \leq 2|c|$, with equality only if c is a nonnegative real number.

To have $\|v+w\|^2 = (\|v\|+\|w\|)^2$ both inequalities in the proof must be equalities. The second one is an equality if and only if $w = 0$, in which case the first one is, too, or if and only if $w \neq 0$ and $v = pw$ for some complex number p. Then $\langle v, w\rangle + \langle w, v\rangle\langle pw, w\rangle + \langle w, pw\rangle = (p + \overline{p})\|w\|^2$ and then the first inequality is an equality if and only if p is a nonnegative real number. □

If V is an inner product space, we may recover the inner product from the norms of vectors.

Lemma 7.1.7 (Polarization identities)**.** *(1) Let V be a real inner product space. Then for any $v, w \in V$,*

$$\langle v, w\rangle = (1/4)\|v + w\|^2 - (1/4)\|v - w\|^2.$$

(2) Let V be a complex inner product space. Then for any $v, w \in V$,

$$\langle v, w\rangle = (1/4)\|v + w\|^2 + (i/4)\|v + iw\|^2 \\ - (1/4)\|v - w\|^2 - (i/4)\|v - iw\|^2.$$

For convenience, we repeat here some earlier definitions.

DEFINITION 7.1.8. Let V be an inner product space. A vector $v \in V$ is a *unit vector* if $\|v\| = 1$. Two vectors v and w are *orthogonal* if $\langle v, w\rangle = 0$. A set $\mathcal{B}$ of vectors in V, $\mathcal{B} = \{v_1, v_2, \ldots\}$, is *orthogonal* if the vectors in $\mathcal{B}$ are pairwise orthogonal, i.e., if $\langle v_i, v_j\rangle = 0$ whenever $i \neq j$. The set $\mathcal{B}$ is *orthonormal* if $\mathcal{B}$ is an orthogonal set of unit vectors, i.e., if $\langle v_i, v_i\rangle = 1$ for every i and $\langle v_i, v_j\rangle = 0$ for every $i \neq j$. ◇

EXAMPLE 7.1.9. Let $\langle\ ,\ \rangle$ be the standard inner product on $\mathbb{F}^n$, defined by $\langle v, w\rangle = {}^t v\overline{w}$. Then the standard basis $\mathcal{E} = \{e_1, \ldots, e_n\}$ is orthonormal. ◇

Lemma 7.1.10. *Let $\mathcal{B} = \{v_1, v_2, \ldots\}$ be an orthogonal set of nonzero vectors in V. If $v \in V$ is a linear combination of the vectors in $\mathcal{B}$, $v = \sum_i c_i v_i$, then $c_j = \langle v, v_j\rangle/\|v_j\|^2$ for each j. In particular, if $\mathcal{B}$ is orthonormal then $c_j = \langle v, v_j\rangle$ for each j.*

Proof. For any j,

$$\langle v, v_j\rangle = \left\langle \sum_i c_i v_i, v_j \right\rangle = \sum_i c_i\langle v_i, v_j\rangle = c_j\langle v_j, v_j\rangle$$

as $\langle v_i, v_j\rangle = 0$ for $i \neq j$. □

Corollary 7.1.11. *Let $\mathcal{B} = \{v_1, v_2, \ldots\}$ be an orthogonal set of nonzero vectors in V. Then $\mathcal{B}$ is linearly independent.*

Lemma 7.1.12. *Let $\mathcal{B} = \{v_1, v_2, \ldots\}$ be an orthogonal set of nonzero vectors in V. If $v \in V$ is a linear combination of the vectors in $\mathcal{B}$, $v = \sum_i c_i v_i$, then $\|v\|^2 = \sum_i |c_i|^2\|v_i\|^2$. In particular if $\mathcal{B}$ is orthonormal then $\|v\|^2 = \sum_i |c_i|^2$.*

Proof. We compute

$$\|v\|^2 = \langle v, v\rangle = \left\langle \sum_i c_i v_i, \sum_j c_j v_j \right\rangle \\ = \sum_{i,j} c_i\overline{c}_j\langle v_i, v_j\rangle = \sum_i |c_i|^2\langle v_i, v_i\rangle.$$ □

Corollary 7.1.13 (Bessel's inequality). *Let $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ be a finite orthogonal set of nonzero vectors in V. For any vector $v \in V$,*

$$\sum_{i=1}^{n} \left|\langle v, v_i\rangle\right|^2 / \|v_i\|^2 \leq \|v\|^2,$$

with equality if and only if $v = \sum_{i=1}^{n} \langle v, v_i\rangle v_i$.

In particular, if $\mathcal{B}$ is orthonormal then

$$\sum_{i=1}^{n} \left|\langle v, v_i\rangle\right|^2 \leq \|v\|^2$$

with equality if and only if $v = \sum_{i=1}^{n} \langle v, v_i\rangle v_i$.

Proof. Let $w = \sum_{i=1}^{n} (\langle v, v_i\rangle / \|v_i\|^2) v_i$ and let $x = v - w$. Then $\langle v, v_i\rangle = \langle w, v_i\rangle$ for each i, so $\langle x, v_i\rangle = 0$ for each i and hence $\langle x, w\rangle = 0$. Then

$$\begin{aligned}\|v\|^2 = \langle v, v\rangle = \langle w + x, w + x\rangle &= \|w\|^2 + \|x\|^2 \geq \|w\|^2 \\ &= \sum_{i=1}^{n} \left|\langle v, v_i\rangle\right|^2 / \|v_i\|^2,\end{aligned}$$

with equality if and only if $x = 0$. $\square$

We have a more general notion of a norm.

DEFINITION 7.1.14. Let V be a vector space over $\mathbb{F}$. A *norm* on V is a function $\|\cdot\| : V \to \mathbb{R}$ satisfying:

(a) $\|v\| \geq 0$ and $\|v\| = 0$ if and only if $v = 0$,

(b) $\|cv\| = |c|\|v\|$ for $c \in \mathbb{F}$ and $v \in V$,

(c) $\|v + w\| \leq \|v\| + \|w\|$ for $v, w \in V$. $\diamond$

Theorem 7.1.15. *(1) Let V be an inner product space. Then*

$$\|v\| = \sqrt{\langle v, v\rangle}$$

is a norm in the sense of Definition 7.1.14.

(2) Let V be a vector space and let $\|\cdot\|$ be a norm on V. There is an inner product $\langle\ ,\ \rangle$ on V such that $\|v\| = \sqrt{\langle v, v\rangle}$ if and only if $\|\cdot\|$ satisfies the parallelogram law

$$\|v + w\|^2 + \|v - w\|^2 = 2\big(\|v\|^2 + \|w\|^2\big) \quad \textit{for all } v, w \in V.$$

Proof. (1) is immediate. For (2), given any norm we can define $\langle\ ,\ \rangle$ by use of the polarization identities of Lemma 7.1.7, and it is easy to verify that this is an inner product if and only if $\|\cdot\|$ satisfies the parallelogram law. We omit the proof. $\square$

EXAMPLE 7.1.16. If

$$v = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

define $\|\cdot\|$ on $\mathbb{F}^n$ by $\|v\| = |x_1| + \cdots + |x_n|$. Then $\|\cdot\|$ is a norm that does not come from an inner product. $\diamond$

We now investigate some important topological properties.

DEFINITION 7.1.17. Two norms $\|\cdot\|_1$ and $\|\cdot\|_2$ on a vector space V are *equivalent* if there are positive constants a and A such that

$$a\|v\|_1 \leq \|v\|_2 \leq A\|v\|_1 \quad \text{for every } v \in V. \qquad \diamond$$

REMARK 7.1.18. It is easy to check that this gives an equivalence relation on norms. $\diamond$

Lemma 7.1.19. *(1) Let $\|\cdot\|$ be any norm on a vector space V. Then $d(v, w) = \|v - w\|$ is a metric on V.*

(2) If $\|\cdot\|_1$ and $\|\cdot\|_2$ are equivalent norms on V, then the metrics $d_1(v, w) = \|v - w\|_1$ and $d_2(v, w) = \|v - w\|_2$ give the same topology on V.

Proof. (1) A metric on a space V is a function $d : V \times V \to V$ satisfying:

(a) $d(v, w) \geq 0$ and $d(v, w) = 0$ if and only if $w = v$

(b) $d(v, w) = d(w, v)$

(c) $d(v, x) \leq d(v, w) + d(w, x)$.

It is then immediate that $d(v, w) = \|v - w\|$ is a metric.

(2) The metric topology on a space V with metric d is the one with a basis of open sets $B_\varepsilon(v_0) = \{v \mid d(v, v_0) \leq \varepsilon\}$ for every $v_0 \in V$ and every $\varepsilon > 0$. Thus $\|\cdot\|_i$ gives the topology with basis of open sets $B^i_\varepsilon(v_0) = \{v \mid \|v - v_0\|_i < \varepsilon\}$ for $v_0 \in V$ and $\varepsilon > 0$, for $i = 1, 2$. By the definition of equivalence $B^2_{\varepsilon/A}(v_0) \subseteq B^1_\varepsilon(v_0)$ and $B^1_{\varepsilon/a}(v_0) \subseteq B^2_\varepsilon(v_0)$ so these two bases give the same topology. $\square$

Theorem 7.1.20. *Let V be a finite-dimensional $\mathbb{F}$-vector space. Then V has a norm, and any two norms on V are equivalent.*

Proof. First we consider $V = \mathbb{F}^n$. Then V has the standard norm

$$\|v\| = \langle v, v\rangle = {}^t v\overline{v}$$

coming from the standard inner product $\langle \cdot, \cdot \rangle$.

It suffices to show that any other norm $\| \cdot \|_2$ is equivalent to this one.

By property (b) of a norm, it suffices to show that there are positive constants a and A with

$$a \leq \|v\|_2 \leq A \quad \text{for every } v \in V \text{ with } \|v\| = 1.$$

First suppose that $\| \cdot \|_2$ comes from an inner product $\langle \ , \ \rangle_2$. Then $\langle v, v\rangle_2 = {}^t vB\overline{v}$ for some matrix B, and so we see that $f(v) = \langle v, v\rangle_2$ is a quadratic function of the entries of v (in the real case) or the real and complex parts of the entries of v (in the complex case). In particular $f(v)$ is a continuous function of the entries of v. Now $\{v \mid \|v\| = 1\}$ is a compact set, and so $f(v)$ has a minimum a (necessarily positive) and a maximum A there.

In the general case we must work a little harder. Let

$$m = \min\left(\|e_1\|_2, \dots, \|e_n\|_2\right) \quad \text{and} \quad M = \max\left(\|e_1\|_2, \dots, \|e_n\|_2\right)$$

where $\{e_1, \dots, e_n\}$ is the standard basis of $\mathbb{F}^n$.

Let $v = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ with $\|v\| = 1$. Then $|x_i| \leq 1$ for each i, so, by the properties of a norm,

$$\begin{aligned} \|v\|_2 &= \|x_1e_1 + \cdots + x_ne_n\|_2 \\ &\leq \|x_1e_1\|_2 + \cdots + \|x_ne_n\|_2 \\ &= |x_1|\|e_1\|_2 + \cdots + |x_n|\|e_n\|_2 \\ &\leq 1 \cdot M + \cdots + 1 \cdot M = nM. \end{aligned}$$

We prove the other inequality by contradiction. Suppose there is no such positive constant a. Then we may find a sequence of vectors $v_1, v_2, \dots$ with $\|v_i\| = 1$ and $\|v_i\|_2 < 1/i$ for each i.

Since $\{v \mid \|v\| = 1\}$ is compact, this sequence has a convergent subsequence $w_1, w_2, \dots$ with $\|w_i\| = 1$ and $\|w_i\|_2 < 1/i$ for each i. Let $w_\infty = \lim_{i\to\infty} w_i$, and let $d = \|w_\infty\|_2$. (We cannot assert that $d = 0$ since we do not know that $\| \cdot \|_2$ is continuous.)

For any $\delta > 0$, let $w \in V$ be any vector with $\|w - w_\infty\| < \delta$. Then

$$d = \left\|w_\infty\right\|_2 \le \left\|w_\infty - w\right\|_2 + \left\|w\right\|_2 \le \delta n M + \|w\|_2.$$

Choose $\delta = d/(2nM)$. Then $\|w - w_\infty\| < \delta$ implies, by the above inequality, that

$$\|w\|_2 \ge d - \delta n M = d/2.$$

Choosing i large enough we have $\|w_i - w_\infty\| < \delta$ and $\|w_i\|_2 < d/2$, a contradiction.

This completes the proof for $V = \mathbb{F}^n$. For V an arbitrary vector space of dimension n, choose any basis $\mathcal{B}$ of V and define $\|\cdot\|$ on V by

$$\|v\| = \left\|[v]_{\mathcal{B}}\right\|$$

where $\|\cdot\|$ is the standard norm on $\mathbb{F}^n$. □

REMARK 7.1.21. It is possible to put an inner product (and hence a norm) on any vector space V, as follows: Choose a basis $\mathcal{B} = \{v_1, v_2, \ldots\}$ of V and define $\langle\ ,\ \rangle$ by $\langle v_i, v_j\rangle = 1$ if $i = j$ and 0 if $i \ne j$, and extend $\langle\ ,\ \rangle$ to V by (conjugate) linearity. However, unless we can actually write down the basis $\mathcal{B}$, this is not very useful. ◇

EXAMPLE 7.1.22. If V is any infinite-dimensional vector space then V admits norms that are not equivalent. Here is an example. Let $V = {}^r\mathbb{F}^\infty$. Let $v = [x_1, x_2, \ldots]$ and $w = [y_1, y_2, \ldots]$. Define $\langle\ ,\ \rangle$ on V by $\langle v, w\rangle = \sum_{j=1}^{\infty} x_j \overline{y}_j$ and define $\langle\ ,\ \rangle'$ on V by $\langle v, w\rangle = \sum_{j=1}^{\infty} x_j \overline{y}_j/2^j$. Then $\langle\ ,\ \rangle$ and $\langle\ ,\ \rangle'$ give norms $\|\cdot\|$ and $\|\cdot\|'$ that are not equivalent, and moreover the respective metrics d and d' on V define different topologies, as the sequence of points $\{e_1, e_2, \ldots\}$ does not have a limit on the topology on V given by d, but converges to $[0, 0, \ldots]$ in the topology given by d'. ◇

7.2 THE GRAM-SCHMIDT PROCESS

Let V be an inner product space. The Gram-Schmidt process is a method for transforming a basis for a finite-dimensional subspace of V into an orthonormal basis for that subspace. In this section we introduce this process and investigate its consequences.

We fix V, the inner product $\langle\ ,\ \rangle$, and the norm $\|\cdot\|$ coming from this inner product, throughout this section.

Theorem 7.2.1. *Let W be a finite-dimensional subspace of V,* $\dim(W) = k$*, and let $\mathcal{B} = \{v_1, v_2, \ldots, v_k\}$ be a basis of W. Then there is an orthonormal basis $\mathcal{C} = \{w_1, w_2, \ldots, w_k\}$ of W such that* $\mathrm{Span}(\{w_1, \ldots, w_i\}) = \mathrm{Span}(\{v_1, \ldots, v_i\})$ *for each $i = 1, \ldots, k$. In particular, W has an orthonormal basis.*

Proof. By Lemma 7.1.3 and Theorem 6.2.29 we see immediately that W has an orthonormal basis. Here is an independent construction.

Define vectors x_i inductively:

$$\begin{aligned} x_1 &= w_1, \\ x_i &= v_i - \sum_{j<i} \frac{\langle v_i, x_j \rangle}{\langle x_j, x_j \rangle} x_j \quad \text{for } i > 1. \end{aligned}$$

Then set

$$w_i = x_i / \|x_i\| \quad \text{for each } i. \qquad \square$$

DEFINITION 7.2.2. The basis $\mathcal{C}$ of W obtained in the proof of Theorem 7.2.1 is said to be obtained from the basis $\mathcal{B}$ of W by applying the *Gram-Schmidt process* to $\mathcal{B}$. ◇

REMARK 7.2.3. The Gram-Schmidt process generalizes without change to the following situation: Let W be a vector space of countably infinite dimension, and let $\mathcal{B} = \{v_1, v_2, \ldots\}$ be a basis of V whose elements are indexed by the positive (or nonnegative) integers. The proof of Theorem 7.2.1 applies to give an orthonormal basis $\mathcal{C}$ of W. ◇

We recall another two definitions from Chapter 6.

DEFINITION 7.2.4. Let W be a subspace of V. Its *orthogonal complement* $W^\perp$ is the subspace of V defined by

$$W^\perp = \{x \in V \mid \langle x, w \rangle = 0 \text{ for every } w \in W\}. \qquad \diamond$$

DEFINITION 7.2.5. V is the *orthogonal direct sum* $V = W_1 \perp W_2$ of subspaces W_1 and W_2 if (1) $V = W_1 \oplus W_2$ is the direct sum of the subspaces W_1 and W_2 (2) W_1 and W_2 are orthogonal subspaces of V. Equivalently, if $v = w_1 + w_2$ with $w_1 \in W_1$ and $w_2 \in W_2$, then

$$\|v\|^2 = \|w_1\|^2 + \|w_2\|^2. \qquad \diamond$$

Theorem 7.2.6. *Let W be a finite-dimensional subspace of V. Then V is the orthogonal direct sum $V = W \perp W^\perp$.*

Proof. If V finite-dimensional, then, by Lemma 7.1.3, $\varphi|W$ is nonsingular (as is φ itself), so, by Lemma 6.2.16, $V = W \perp W^{\perp}$.

Alternatively, let $\dim(V) = n$ and $\dim(W) = k$. Choose a basis $\mathcal{B}_1 = \{v_1, \dots, v_k\}$ of W and extend it to a basis $\mathcal{B} = \{v_1, \dots, v_n\}$ of V. Apply the Gram-Schmidt process to $\mathcal{B}$ to obtain a basis $\mathcal{C} = \{w_1, \dots, w_n\}$ of V. Then $\mathcal{C}_1 = \{w_1, \dots, w_k\}$ is a basis of W. It is easy to check that $\mathcal{C}_2 = \{w_{k+1}, \dots, w_n\}$ is a basis of $W^{\perp}$, from which it follows that $V = W \perp W^{\perp}$.

In general, choose an orthogonal basis $\mathcal{C} = \{w_1, \dots, w_k\}$ of W. For $v \in V$, let $x = \sum \langle v, w_i \rangle w_i$. Then $x \in W$ and $\langle x, w_i \rangle = \langle v, w_i \rangle$ for $i = 1, \dots, k$, which implies $\langle x, w \rangle = \langle v, w \rangle$ for every $w \in W$. Thus $\langle v - x, w \rangle = 0$ for every $w \in W$, and so $v - x \in W^{\perp}$. Since $v = x + (v - x)$, we see that $V = W + W^{\perp}$. Now $\langle y, z \rangle = 0$ whenever $y \in W$ and $z \in W^{\perp}$. If $w \in W \cap W^{\perp}$, set $y = w$ and $z = w$ to conclude that $\langle w, w \rangle = 0$, which implies that $w = 0$. Thus $V = W \oplus W^{\perp}$. Finally, if $V = W \oplus W^{\perp}$ then $V = W \perp W^{\perp}$ by the definition of $W^{\perp}$. □

Lemma 7.2.7. *Let W be a subspace of V and suppose that $V = W \perp W^{\perp}$. Then $(W^{\perp})^{\perp} = W$.*

Proof. If V is finite-dimensional, this is Corollary 6.2.18. The following argument works in general.

It is easy to check that $(W^{\perp})^{\perp} \supseteq W$. Let $v \in (W^{\perp})^{\perp}$. Since $v \in V$, we may write $v = x + y$ with $x \in W$ and $y \in W^{\perp}$. Then $0 = \langle v, y \rangle = \langle x + y, y \rangle = \langle x, y \rangle + \langle y, y \rangle = \langle y, y \rangle$ so $y = 0$, and hence $v = x$. Thus $(W^{\perp})^{\perp} = W$. □

Corollary 7.2.8. *Let W be a finite-dimensional subspace of V. Then $(W^{\perp})^{\perp} = W$.*

Proof. Immediate from Theorem 7.2.6 and Lemma 7.2.7. □

EXAMPLE 7.2.9. Let $V \subseteq {}^r\mathbb{F}^{\infty\infty}$ be the subspace consisting of all elements $[x_1, x_2, \dots]$ with $\{x_i\}$ bounded (i.e., such that there is a constant M with $|x_i| < M$ for each i). Give V the inner product

$$\langle [x_1, x_2, \dots], [y_1, y_2, \dots] \rangle = \sum_{j=1}^{\infty} x_j \overline{y}_j / 2^j.$$

Let $W = {}^r\mathbb{F}^{\infty}$ and note that W is a subspace of V. If $y = [y_1, y_2, \dots] \in W^{\perp}$ then, since $e_i \in W$ for each i, $0 = \langle e_i, y \rangle = y_i / 2^i$, so $y = [0, 0, \dots]$. Thus $W^{\perp} = \{0\}$, and we see that $V \neq W \perp W^{\perp}$ and that $(W^{\perp})^{\perp} \neq W$. ◇

DEFINITION 7.2.10. Let W be a subspace of V and suppose that $V = W \perp W^{\perp}$. The *orthogonal projection* Π_W is the linear transformation defined by $\Pi_W(v) = x$ where $v = x + y$ with $x \in W$ and $y \in W^{\perp}$. ◇

Lemma 7.2.11. *Let W be a finite-dimensional subspace of V and let $\mathcal{C} = \{w_1, \dots, w_k\}$ be an orthonormal basis of W. Then*

$$\Pi_W(v) = \sum_{i=1}^{k} \langle v, w_i \rangle w_i \quad \textit{for every } v \in V.$$

Proof. Immediate from the proof of Theorem 7.2.6. □

Corollary 7.2.12. *Let W be a finite-dimensional subspace of V and let $\mathcal{C} = \{w_1, \dots, w_k\}$ and $\mathcal{C}' = \{w_1', \dots, w_k'\}$ be two orthonormal bases of W. Then*

$$\sum_{i=1}^{k} \langle v, w_i \rangle w_i = \sum_{i=1}^{k} \langle v, w_i' \rangle w_i' \quad \textit{for every } v \in V.$$

Proof. Both are equal to $\Pi_W(v)$. □

Lemma 7.2.13. *Let W be a subspace of V such that $V = W \perp W^{\perp}$. Then $\Pi_W^2 = \Pi_W$, $\Pi_{W^\perp} = \mathcal{I} - \Pi_W$, and $\Pi_{W^\perp}\Pi_W = \Pi_W \Pi_{W^\perp} = 0$.*

Proof. This follows immediately from Definition 7.2.10. □

REMARK 7.2.14. Suppose that V is finite-dimensional. Let $\mathcal{T} = \Pi_W$. By Lemma 7.2.13, $\mathcal{T}^2 = \mathcal{T}$ so $p(\mathcal{T}) = 0$ where $p(x)$ is the polynomial $p(x) = x^2 - x = x(x-1)$. Then the minimum polynomial $m_{\mathcal{T}}(x)$ divides $p(x)$. Thus $m_{\mathcal{T}}(x) = x$, which occurs if and only if $W = \{0\}$, or $m_{\mathcal{T}}(x) = x - 1$, which occurs if and only if $W = V$, or $m_{\mathcal{T}}(x) = x(x-1)$. In this last case W is the 1-eigenspace of Π_W and $W^{\perp}$ is the 0-eigenspace of Π_W. In any case Π_W is diagonalizable (over $\mathbb{R}$ or over $\mathbb{C}$), as $m_{\mathcal{T}}(x)$ is a product of distinct linear factors. ◇

Let us revisit the Gram-Schmidt process from the point of view of orthogonal projections. First we need another definition.

DEFINITION 7.2.15. The *normalization map* $N : V - \{0\} \to \{v \in V \mid \|v\| = 1\}$ is the function $N(v) = v/\|v\|$. ◇

Corollary 7.2.16. *Let W be a finite-dimensional subspace of V and let $\mathcal{B} = \{v_1, \dots, v_k\}$ be a basis of W. Let*

$$W_0 = \{0\} \quad \textit{and} \quad W_i = \operatorname{Span}(\{v_1, \dots, v_i\})$$

for $1 \le i < k$. Then the basis $\mathcal{C} = \{w_1, \dots, w_k\}$ of W obtained from V by the Gram-Schmidt procedure is given by

$$w_i = N\left(\Pi_{W_{i-1}^{\perp}}(v_i)\right) \quad \textit{for } i = 1, \dots, k.$$

The Gram-Schmidt process has important algebraic and topological consequences.

DEFINITION 7.2.17. Let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$. A *k-frame* in $\mathbb{F}^n$ is a linearly independent k-tuple $\{v_1, \dots, v_k\}$ of vectors in $\mathbb{F}^n$. An *orthonormal k-frame* in $\mathbb{F}^n$ is an orthonormal k-tuple $\{v_1, \dots, v_k\}$ of vectors in $\mathbb{F}^n$. Set

$$\mathcal{G}_{n,k}(\mathbb{F}) = \left\{k\text{-frames in } \mathbb{F}^n\right\}$$

and

$$\mathcal{S}_{n,k}(\mathbb{F}) = \left\{\text{orthonormal } k\text{-frames in } \mathbb{F}^n\right\}.$$

By identifying $\{v_1, \dots, v_n\}$ with the n-by-k matrix $[v_1|\cdots|v_k]$ we identify $\mathcal{G}_{n,k}(\mathbb{F})$ and $\mathcal{S}_{n,k}(\mathbb{F})$ with subsets of $\mathcal{M}_{n,k}(\mathbb{F})$. Let $\mathbb{F}^{nk}$ have its usual topology. The natural identification of $\mathcal{M}_{n,k}(\mathbb{F})$ with $\mathbb{F}^{nk}$ gives a topology on $\mathcal{M}_{n,k}(\mathbb{F})$ and hence on $\mathcal{G}_{n,k}(\mathbb{F})$ and $\mathcal{S}_{n,k}(\mathbb{F})$ as well. $\diamond$

In order to formulate our result we need a preliminary definition.

DEFINITION 7.2.18. Let $\mathcal{A}_k^+ =$\{k-by-k diagonal matrices with positive real number entries\}. For $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$, let $\mathcal{N}_k(\mathbb{F}) =$\{$k$-by-$k$ upper triangular matrices with entries in $\mathbb{F}$ and with all diagonal entries equal to 1\}. Topologize $\mathcal{A}_k^+$ and $\mathcal{N}_k(\mathbb{F})$ as subsets of $\mathbb{F}^{k^2}$. $\diamond$

Lemma 7.2.19. *With these identifications, any matrix $P \in \mathcal{G}_{n,k}(\mathbb{R})$ can be written uniquely as $P = QAN$ where $Q \in \mathcal{S}_{n,k}(\mathbb{R})$, $A \in \mathcal{A}_k^+$, and $N \in \mathcal{N}_k(\mathbb{R})$, and any matrix $P \in \mathcal{G}_{n,k}(\mathbb{C})$ can be written uniquely as $P = QAN$ where $Q \in \mathcal{S}_{n,k}(\mathbb{C})$, $A \in \mathcal{A}_k^+$, and $N \in \mathcal{N}_k(\mathbb{C})$.*

Proof. The proof is identical in both cases, so we let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$.

Let $P = [v_1|\cdots|v_n]$. In the notation of the proof of Theorem 7.2.1, we see that for each $i = 1, \dots, k$, x_i is a linear combination of v_i and $x_1, \dots, x_{i-1}$, which implies that v_i is a linear combination of $x_1, \dots, x_i$. Also we see that in any such linear combination the x_i-coefficient of v_i is 1. Thus $P = Q'N$ where $Q' = [x_1|\cdots|x_k]$ and $N \in \mathcal{N}_k(\mathbb{F})$. But $x_i = \|x_i\|_{w_i}$ so $Q' = QA$ where $Q = [w_1|\cdots|w_k]$ and $A \in \mathcal{A}_k^+$ is the diagonal matrix with entries $\|x_1\|, \ldots, \|x_k\|$. Hence P can be written as $P = QAN$.

To show uniqueness, suppose $P = Q_1A_1N_1 = Q_2A_2N_2$. Let $M_1 = A_1N_1$ and $M_2 = A_2N_2$. Then $Q_1M_1 = Q_2M_2$ so $Q_1 = Q_2M_2M_1^{-1}$, where $M_2M_1^{-1}$ is upper triangular with positive real entries on the diagonal. Let $Q_1 = [w_1|w_2|\cdots|w_k]$ and $Q_2 = [w_1'|w_2'|\cdots|w_k']$. If $M_2M_1^{-1}$ had a nonzero entry in the (i, j) position with $i < j$, then, choosing the smallest such j, $\langle w_i, w_j \rangle \neq 0$, which is impossible. Thus $M_2M_1^{-1}$ is a diagonal matrix. Since $\langle w_i, w_i \rangle = 1$ for each i, the diagonal entries of $M_2M_1^{-1}$ all have absolute value 1, and since they are positive real numbers, they are all 1. Thus $M_2M_1^{-1} = I$. Then $M_2 = M_1$ and hence $Q_2 = Q_1$. Hence $M = M_1$ and $Q = Q_1$ are uniquely determined. For any matrices $A \in \mathcal{A}_k^+$ and $N \in \mathcal{N}_k(\mathbb{F})$, the diagonal entries of AN are equal to the diagonal entries of A, so the diagonal entries of A are equal to the diagonal entries of M. Thus A, being a diagonal matrix, is also uniquely determined. Then $N = A^{-1}M$ is uniquely determined as well. □

Theorem 7.2.20. *With the above identifications, the multiplication maps*

$$m : \mathcal{S}_{n,k}(\mathbb{R}) \times \mathcal{A}_k^+ \times \mathcal{N}_k(\mathbb{R}) \longrightarrow \mathcal{G}_{n,k}(\mathbb{R})$$

and

$$m : \mathcal{S}_{n,k}(\mathbb{C}) \times \mathcal{A}_k^+ \times \mathcal{N}_k(\mathbb{C}) \longrightarrow \mathcal{G}_{n,k}(\mathbb{C})$$

given by $P = m(Q, A, N) = QAN$ are homeomorphisms.

Proof. In either case, the map m is obviously continuous, and Lemma 7.2.19 shows that it is 1-to-1 and onto. The proof of Theorem 7.2.1 shows that $m^{-1} : P \to (Q, A, N)$ is also continuous, so m is a homeomorphism. □

Corollary 7.2.21. *With the above identifications, $\mathcal{S}_{n,k}(\mathbb{R})$ is a strong deformation retract of $\mathcal{G}_{n,k}(\mathbb{R})$ and $\mathcal{S}_{n,k}(\mathbb{C})$ is a strong deformation retract of $\mathcal{G}_{n,k}(\mathbb{C})$.*

Proof. Let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$. $\mathcal{S}_{n,k}(\mathbb{F})$ is a subspace of $\mathcal{G}_{n,k}(\mathbb{F})$ and, in the notation of Lemma 7.2.19, we have $Q = QII$ where the first I is in $\mathcal{A}_k^+$ and the second is in $\mathcal{N}_k(\mathbb{F})$.

A subspace X of a space Y is a strong deformation retract of Y if there is a continuous function $R : Y \times [0, 1] \to Y$ with

(a) $R(y, 0) = y$ for every $y \in Y$,

(b) $R(x, t) = x$ for every $x \in X$, $t \in [0, 1]$,

(c) $R(y, 1) \in X$ for every $y \in Y$.

(We think of t as "time" and set $\overline{R}_t(y) = R(y,t)$. Then $\overline{R}_0$ is the identity on Y, $\overline{R}_1 : Y \to X$, and $\overline{R}_t(x) = x$ for every x and t, so points in X "never move".)

In our case, the map R is defined as follows. If $P = QAN$ then

$$R(P,t) = QA^{(1-t)}\big(tI + (1-t)N\big). \qquad \square$$

7.3 Adjoints, normal linear transformations, and the spectral theorem

In this section we derive additional properties of adjoints in the case of inner product spaces. Then we introduce the notion of a normal linear transformation $\mathcal{T} : V \to V$ and study its properties, culminating in the spectral theorem.

We fix V, the inner product $\varphi(x,y) = \langle x, y\rangle$, and the norm $\|x\| = \langle x, x\rangle$, throughout.

Let $\mathcal{T} : V \to W$ be a linear transformation between inner product spaces. In Definition 6.3.1 we defined its adjoint $\mathcal{T}^{\mathrm{adj}}$. We here follow common mathematical practice and denote $\mathcal{T}^{\mathrm{adj}}$ by $\mathcal{T}^*$. (This notation is ambiguous because $\mathcal{T}^*$ also denotes the dual of $\mathcal{T}$, $\mathcal{T}^* : W^* \to V^*$, but in this section we will always be considering the adjoint and never the dual.) Lemma 6.3.2 guaranteed the existence of $\mathcal{T}^*$ only in case V is finite-dimensional, but we observed in Remark 6.3.8 that if $\mathcal{T}^*$ is defined, it is well-defined.

We first derive some relationships between $\mathcal{T}$ and $\mathcal{T}^*$.

Lemma 7.3.1. *Let V and W be finite-dimensional inner product spaces and let $\mathcal{T} : V \to W$ be a linear transformation. Then*

(1) $\mathrm{Im}(\mathcal{T}^*) = \mathrm{Ker}(\mathcal{T})^{\perp}$ *and* $\mathrm{Ker}(\mathcal{T}^*) = \mathrm{Im}(\mathcal{T})^{\perp}$

(2) $\dim(\mathrm{Ker}(\mathcal{T}^*)) = \dim(\mathrm{Ker}(\mathcal{T}))$

(3) If $\dim(W) = \dim(V)$ *then* $\dim(\mathrm{Im}(\mathcal{T}^*)) = \dim(\mathrm{Im}(\mathcal{T}))$.

Proof. Let $U = \mathrm{Ker}(\mathcal{T})$. Let $\dim(V) = n$ and $\dim(U) = k$, so $\dim(U^{\perp}) = n - k$. Then, for any $u \in U$ and any $v \in V$,

$$\big\langle u, \mathcal{T}^*(v)\big\rangle = \big\langle \mathcal{T}(u), v\big\rangle = \langle 0, v\rangle = 0,$$

so $\mathrm{Im}(\mathcal{T}^*) \subseteq U^{\perp}$. Hence $\dim(\mathrm{Ker}(\mathcal{T}^*)) \geq k = \dim(\mathrm{Ker}(\mathcal{T}))$. Replacing $\mathcal{T}$ by $\mathcal{T}^*$ we obtain $\dim(\mathrm{Ker}(\mathcal{T}^{**})) \geq \dim(\mathrm{Ker}(\mathcal{T}^*))$. But $\mathcal{T}^{**} = \mathcal{T}$, so $\dim(\mathrm{Ker}(\mathcal{T}^*)) = \dim(\mathrm{Ker}(\mathcal{T}))$ and $\mathrm{Im}(\mathcal{T}^*) = \mathrm{Ker}(\mathcal{T})^{\perp}$. The proof that $\mathrm{Ker}(\mathcal{T}^*) = \mathrm{Im}(\mathcal{T})^{\perp}$ is similar. Then (3) follows from Theorem 1.3.1. □

Corollary 7.3.2. *Let V be a finite-dimensional inner product space and let $\mathcal{T} : V \to V$ be a linear transformation. Suppose that $\mathcal{T}$ has a Jordan Canonical Form over $\mathbb{F}$ (which is always the case if $\mathbb{F} = \mathbb{C}$). Then $\mathcal{T}^*$ has a Jordan Canonical Form over $\mathbb{F}$. The Jordan Canonical Form of $\mathcal{T}^*$ is obtained from the Jordan Canonical Form of $\mathcal{T}$ by taking the conjugate of each diagonal entry if $\mathbb{F} = \mathbb{C}$ and is the same as the Jordan Canonical Form of $\mathcal{T}$ if $\mathbb{F} = \mathbb{R}$.*

Proof. By Lemma 6.3.10, $(\mathcal{T} - \lambda\mathcal{I})^* = \mathcal{T}^* - \overline{\lambda}\mathcal{I}$. Apply Lemma 7.3.1 with $\mathcal{T}$ replaced by $(\mathcal{T} - \lambda\mathcal{I})^k$ to obtain that the spaces E_{λ}^{k} of $\mathcal{T}$ and $E_{\overline{\lambda}}^{k}$ of $\mathcal{T}^*$ have the same dimension for every eigenvalue λ of $\mathcal{T}$ and every positive integer k. These dimensions determine the Jordan Canonical Forms. □

Corollary 7.3.3. *Let V be a finite-dimensional inner product space and let $\mathcal{T} : V \to V$ be a linear transformation. Then*

(1) $m_{\mathcal{T}^*}(x) = \overline{m_{\mathcal{T}}(x)}$

(2) $c_{\mathcal{T}^*}(x) = \overline{c_{\mathcal{T}}(x)}$.

Proof. (1) Follows immediately from Lemma 6.3.10 and Lemma 7.3.1.

(2) Follows immediately from Corollary 7.3.2 in case $\mathbb{F} = \mathbb{C}$. In case $\mathbb{F} = \mathbb{R}$, choose a basis of V, represent T in that basis by a matrix, and then regard that matrix as a matrix over $\mathbb{C}$. □

Now we come to the focus of our attention, normal linear transformations.

DEFINITION 7.3.4. A linear transformation $\mathcal{T} : V \to V$ is *normal* if

(1) $\mathcal{T}$ has an adjoint $\mathcal{T}^*$

(2) $\mathcal{T}$ commutes with $\mathcal{T}^*$, i.e., $\mathcal{T} \circ \mathcal{T}^* = \mathcal{T}^* \circ \mathcal{T}$. ◇

Let us look at a couple of special cases.

DEFINITION 7.3.5. A linear transformation $\mathcal{T} : V \to V$ is *self-adjoint* if $\mathcal{T}$ has an adjoint $\mathcal{T}^*$ and $\mathcal{T}^* = \mathcal{T}$. ◇

We also recall the definition of an isometry, which we restate for convenience in the special case we are considering here, and establish some properties of isometries.

DEFINITION 7.3.6. Let V be an inner product space. An *isometry* $\mathcal{T} : V \to V$ is an invertible linear transformation such that $\langle \mathcal{T}(v), \mathcal{T}(w)\rangle = \langle v, w\rangle$ for all $v, w \in V$. $\diamond$

We observe that sometimes invertibility is automatic.

Lemma 7.3.7. *Let $\mathcal{T} : V \to V$ be a linear transformation. Then*

$$\langle \mathcal{T}(v), \mathcal{T}(w)\rangle = \langle v, w\rangle$$

for all $v, w \in V$ if and only if $\|\mathcal{T}(v)\| = \|(v)\|$ for all $v \in V$. If these equivalent conditions are satisfied, then $\mathcal{T}$ is an injection. If furthermore V is finite dimensional, then $\mathcal{T}$ is an isomorphism.

Proof. Since $\|\mathcal{T}(v)\|^2 = \langle \mathcal{T}(v), \mathcal{T}(v)\rangle$, the first condition implies the second, and the second implies the first by the polarization identities.

Suppose these conditions are satisfied. Let $v \in V$, $v \neq 0$. Then $0 \neq \|v\| = \|\mathcal{T}(v)\|$ so $\mathcal{T}(v) \neq 0$ and $\mathcal{T}$ is an injection. Any injection from a finite-dimensional vector space to itself is an isomorphism. $\square$

EXAMPLE 7.3.8. Let $V = {}^r\mathbb{F}^\infty$ with the standard inner product

$$\langle [x_1, x_2, \ldots], [y_1, y_2, \ldots]\rangle = \sum x_i \overline{y}_i .$$

Then right-shift $\mathbf{R} : V \to V$ satisfies $\langle \mathbf{R}(v), \mathbf{R}(w)\rangle = \langle v, w\rangle$ for every $v, w \in V$ and $\mathbf{R}$ is an injection but not an isomorphism. $\diamond$

Lemma 7.3.9. *Let $\mathcal{T} : V \to V$ be an isometry. Then $\mathcal{T}$ has an adjoint $\mathcal{T}^*$ and $\mathcal{T}^* = \mathcal{T}^{-1}$.*

Proof. If there is a linear transformation $\mathcal{S} : V \to V$ such that

$$\big\langle \mathcal{T}(v), w\big\rangle = \big\langle v, \mathcal{S}(w)\big\rangle \quad \text{for every } v, w \in V,$$

then $\mathcal{S}$ is well-defined and $\mathcal{S} = \mathcal{T}^*$. Since $\mathcal{T}$ is an isometry, we see that

$$\big\langle v, \mathcal{T}^{-1}(w)\big\rangle = \big\langle \mathcal{T}(v), \mathcal{T}\big(\mathcal{T}^{-1}(w)\big)\big\rangle = \big\langle \mathcal{T}(v), w\big\rangle. \qquad \square$$

Corollary 7.3.10. *(1) If $\mathcal{T}$ is self-adjoint then $\mathcal{T}$ is normal.*

(2) If $\mathcal{T}$ is an isometry then $\mathcal{T}$ is normal.

We introduce some traditional language.

DEFINITION 7.3.11. If V is a real inner product space an isometry of V is *orthogonal*. If V is a complex inner product space an isometry of V is *unitary*. $\diamond$

DEFINITION 7.3.12. A matrix P is *orthogonal* if ${}^tP = P^{-1}$. A matrix P is *unitary* if $\overline{{}^tP} = P^{-1}$. $\diamond$

Corollary 7.3.13. *Let V be a finite-dimensional inner product space and let $\mathcal{T} : V \to V$ be a linear transformation. Let $\mathcal{C}$ be an orthonormal basis of V and set $M = [\mathcal{T}]_{\mathcal{C}}$.*

(1) If V is a real vector space, then

(a) If $\mathcal{T}$ is self-adjoint, M is symmetric.

(b) If $\mathcal{T}$ is orthogonal, M is orthogonal.

(2) If V is a complex vector space, then

(a) If $\mathcal{T}$ is self-adjoint, M is Hermitian.

(b) If $\mathcal{T}$ is unitary, M is unitary.

Proof. Immediate from Corollary 6.3.7. $\square$

Let us now look at some interesting examples on infinite dimensional vector spaces.

EXAMPLE 7.3.14. (1) Let $V = {}^r\mathbb{F}^\infty$. Let $\mathbf{R} : V \to V$ be right shift, and $\mathbf{L} : V \to V$ be left shift. Let $v = [x_1, x_2, \ldots]$ and $w = [y_1, y_2, \ldots]$. Then

$$\langle \mathbf{R}(v), w \rangle = x_1\overline{y}_2 + x_2\overline{y}_3 + \cdots = \langle v, \mathbf{L}(w) \rangle$$

so $\mathbf{L} = \mathbf{R}^*$. Similarly,

$$\langle \mathbf{L}(v), w \rangle = x_2\overline{y}_1 + x_3\overline{y}_2 + \cdots = \langle v, \mathbf{R}(w) \rangle$$

so $\mathbf{R} = \mathbf{L}^*$ (as we expect from Lemma 6.3.11). Note that $\mathbf{LR} = \mathcal{I}$ but $\mathbf{RL} \neq \mathcal{I}$ so $\mathbf{L}$ and $\mathbf{R}$ are not normal. Also note that $1 = \dim(\mathrm{Ker}(\mathbf{L})) \neq 0 = \dim(\mathrm{Ker}(\mathbf{R}))$, giving a counterexample to the conclusion of Lemma 7.3.1 in the infinite-dimensional case.

(2) Let V be the vector space of doubly infinite sequences of elements of $\mathbb{F}$ only finitely many of which are nonzero

$$V = \{[\ldots, x_{-2}, x_{-1}, x_0, x_1, x_2, \ldots] \mid x_i = 0 \text{ for all but finitely many } i\}.$$

V has the inner product $\langle v, w\rangle = \sum x_i \overline{y}_i$ (in the obvious notation) and linear transformations $\mathbf{R}$ (right shift) and $\mathbf{L}$ (left shift) defined in the obvious way. Then $\mathbf{L}$ and $\mathbf{R}$ are both isometries, and are inverses of each other. Direct computation as in (1) shows that $\mathbf{L} = \mathbf{R}^*$ and $\mathbf{R} = \mathbf{L}^*$, as we expect from Lemma 7.3.9.

(3) Let $V = {}^r\mathbb{F}^\infty$ and let $\mathcal{T} : V \to V$ be defined as follows:

$$\mathcal{T}\big([x_1, x_2, x_3, \dots]\big) = \left[\sum_{i\geq 1} x_i, 0, 0, \dots\right].$$

We claim that $\mathcal{T}$ does not have an adjoint. We prove this by contradiction. Suppose $\mathcal{T}^*$ existed. Let $\mathcal{T}^*(e_1) = [a_1, a_2, a_3, \dots]$. Then for each $k = 1, 2, 3, \dots,$

$$1 = \big\langle (e_k), e_1\big\rangle = \big\langle e_k, \mathcal{T}^*\big(e_1\big)\big\rangle = a_k,$$

which is impossible as $\mathcal{T}^*(e_1) \in V$ has only finitely many nonzero entries. ◇

We may construct normal linear transformations as follows.

EXAMPLE 7.3.15. Let $\lambda_1, \dots, \lambda_k$ be distinct scalars and let $W_1, \dots, W_k$ be nonzero subspaces of V with $V = W_1 \perp \cdots \perp W_k$. Define $\mathcal{T} : V \to V$ as follows: Let $v \in V$ and write v uniquely as $v = v_1 + \cdots + v_k$ with $v_i \in W_i$. Then

$$\mathcal{T}(v) = \lambda_1 v_1 + \cdots + \lambda_k v_k.$$

(Thus $\lambda_1, \dots, \lambda_k$ are the distinct eigenvalues of $\mathcal{T}$ and $W_1, \dots, W_k$ are the associated eigenspaces.) It is easy to check that

$$\mathcal{T}^*(v) = \overline{\lambda}_1 v_1 + \cdots + \overline{\lambda}_k v_k$$

(so $\overline{\lambda}_1, \dots, \overline{\lambda}_k$ are the distinct eigenvalues of $\mathcal{T}^*$ and $W_1, \dots, W_k$ are the associated eigenspaces). Then

$$\mathcal{T}^*\mathcal{T}(v) = |\lambda_1|^2 v_1 + \cdots + |\lambda_k|^2 v_k = \mathcal{T}\mathcal{T}^*(v),$$

so $\mathcal{T}$ is normal. Clearly $\mathcal{T}$ is self-adjoint if and only if $\overline{\lambda_i} = \lambda_i$ for each i, i.e., if and only if each λ_i is real. ◇

Our next goal is the spectral theorem, which shows that on a finite-dimensional complex vector space V, *every* normal linear transformation is of this form, and on a finite-dimensional real vector space *every* self-adjoint linear transformation is of this form.

We first derive a number of properties of normal linear transformations (on an arbitrary vector space V).

Lemma 7.3.16. *Let $\mathcal{T} : V \to V$ be a normal linear transformation. Then $\mathcal{T}^*$ is normal. Furthermore,*

(1) $p(\mathcal{T})$ *is normal for any polynomial* $p(x) \in \mathbb{C}[x]$. *If* $\mathcal{T}$ *is self-adjoint,* $p(\mathcal{T})$ *is self-adjoint for any polynomial* $p(x) \in \mathbb{R}[x]$.

(2) $\|\mathcal{T}(v)\| = \|\mathcal{T}^*(v)\|$ *for every* $v \in V$. *Consequently* $\operatorname{Ker}(\mathcal{T}) = \operatorname{Ker}(\mathcal{T}^*)$.

(3) $\operatorname{Ker}(\mathcal{T}) = \operatorname{Im}(\mathcal{T})^\perp$ *and* $\operatorname{Ker}(\mathcal{T}^*) = \operatorname{Im}(\mathcal{T}^*)^\perp$.

(4) If $\mathcal{T}^2(v) = 0$ *then* $\mathcal{T}(v) = 0$.

(5) The vector $v \in V$ *is an eigenvector of* $\mathcal{T}$ *with eigenvalue* λ *if and only* v *is an eigenvector of* $\mathcal{T}^*$ *with eigenvalue* $\overline{\lambda}$.

(6) Eigenspaces of distinct eigenvalues of $\mathcal{T}$ *are orthogonal.*

Proof. By Lemma 6.3.11, $\mathcal{T}^*$ has adjoint $\mathcal{T}^{**} = \mathcal{T}$, and then $\mathcal{T}^*\mathcal{T}^{**} = \mathcal{T}^*\mathcal{T} = \mathcal{T}\mathcal{T}^* = \mathcal{T}^{**}\mathcal{T}^*$.

(1) follows from Lemma 6.3.10.

For (2), we compute

$$\begin{aligned}\left\|\mathcal{T}(v)\right\|^2 &= \langle \mathcal{T}(v), \mathcal{T}(v)\rangle = \langle v, \mathcal{T}^*\mathcal{T}(v)\rangle = \langle v, \mathcal{T}\mathcal{T}^*(v)\rangle \\ &= \langle v, \mathcal{T}^{**}\mathcal{T}^*(v)\rangle = \langle \mathcal{T}^*(v), \mathcal{T}^*(v)\rangle = \left\|\mathcal{T}^*(v)\right\|^2.\end{aligned}$$

Also, we observe that $v \in \operatorname{Ker}(\mathcal{T}) \Leftrightarrow \mathcal{T}(v) = 0 \Leftrightarrow \|\mathcal{T}(v)\| = 0$.

For (3), $u \in \operatorname{Ker}(\mathcal{T}) \Leftrightarrow u \in \operatorname{Ker}(\mathcal{T}^*)$, by (2), $\Leftrightarrow \langle \mathcal{T}^*(u), v\rangle = 0$ for all $v \Leftrightarrow \langle u, \mathcal{T}(v)\rangle = 0$ for all $v \Leftrightarrow u \in \operatorname{Im}(\mathcal{T})^\perp$, yielding the first half of (3), and replacing $\mathcal{T}$ by $\mathcal{T}^*$, which is also normal, we obtain the second half of (3).

For (4), let $w = \mathcal{T}(v)$. Then $w \in \operatorname{Im}(\mathcal{T})$. But $\mathcal{T}(w) = \mathcal{T}^2(v) = 0$, so $w \in \operatorname{Ker}(\mathcal{T})$. Thus $w \in \operatorname{Ker}(\mathcal{T}) \cap \operatorname{Im}(\mathcal{T}) = \{0\}$ by (3).

For (5), v is an eigenvector of $\mathcal{T}$ with eigenvalue $\lambda \Leftrightarrow v \in \operatorname{Ker}(\mathcal{T} - \lambda\mathcal{I}) \Leftrightarrow v \in \operatorname{Ker}((\mathcal{T} - \lambda\mathcal{I})^*)$ by (2) $= \operatorname{Ker}(\mathcal{T}^* - \overline{\lambda}\mathcal{I})$ by Lemma 6.3.10(4).

For (6), let v_1 be an eigenvector of $\mathcal{T}$ with eigenvalue λ_1 and let v_2 be an eigenvector of $\mathcal{T}$ with eigenvalue λ_2, with $\lambda_2 \neq \lambda_1$. Set $\mathcal{S} = \mathcal{T} - \lambda_1\mathcal{I}$. Then $\mathcal{S}(v_1) = 0$ so

$$\begin{aligned}0 = \langle \mathcal{S}(v_1), v_2\rangle = \langle v_1, \mathcal{S}^*(v_2)\rangle &= \langle v_1, (\mathcal{T}^* - \overline{\lambda}_1\mathcal{I})(v_2)\rangle \\ &= \langle v_1, (\overline{\lambda}_2 - \overline{\lambda}_1)v_2\rangle \text{ (by (5))} \\ &= (\lambda_2 - \lambda_1)\langle v_1, v_2\rangle\end{aligned}$$

so $\langle v_1, v_2\rangle = 0$. $\square$

Corollary 7.3.17. *Let V be finite-dimensional and let $\mathcal{T} : V \to V$ be a normal linear transformation. Then* $\mathrm{Im}(\mathcal{T}) = \mathrm{Im}(\mathcal{T}^*)$.

Proof. By Corollary 7.2.8 and Lemma 7.3.16(2) and (3),

$$\mathrm{Im}(\mathcal{T}) = \mathrm{Ker}(\mathcal{T})^{\perp} = \mathrm{Ker}\left(\mathcal{T}^*\right)^{\perp} = \mathrm{Im}\left(\mathcal{T}^*\right). \qquad \square$$

While Lemma 7.3.16 gives information about the eigenvectors of a normal linear transformation $\mathcal{T} : V \to V$, when V is infinite dimensional $\mathcal{T}$ may have no eigenvalues or eigenvectors.

EXAMPLE 7.3.18. Let $\mathbf{R}$ be right shift, or $\mathbf{L}$ left shift, on the vector space V of Example 7.3.14(2). It is easy to check that, since every element of V can have only finitely many nonzero entries, neither $\mathbf{R}$ nor $\mathbf{L}$ has any eigenvalues or eigenvectors. $\diamond$

By contrast, in the finite-dimensional case we may obtain strong information about the structure of $\mathcal{T}$.

Lemma 7.3.19. *Let V be a finite-dimensional inner product space and let $\mathcal{T} : V \to V$ be a normal linear transformation. Then the minimum polynomial $m_{\mathcal{T}}(x)$ is a product of distinct irreducible factors. If V is a complex vector space, or if V is a real vector space and $\mathcal{T}$ is self-adjoint, every irreducible factor of $m_{\mathcal{T}}(x)$ is linear.*

Proof. Let $p(x)$ be an irreducible factor of $m_{\mathcal{T}}(x)$. We prove that $p^2(x)$ does not divide $m_{\mathcal{T}}(x)$ by contradiction. Suppose $p^2(x)$ divides $m_{\mathcal{T}}(x)$. Then there is a vector $v \in V$ with $p^2(\mathcal{T})(v) = 0$ but $p(\mathcal{T})(v) \neq 0$. Let $\mathcal{S} = p(\mathcal{T})$. Then $\mathcal{S}$ is normal and $\mathcal{S}^2(v) = 0$ but $\mathcal{S}(v) \neq 0$, contradicting Lemma 7.3.16(4).

If V is a complex vector space there is nothing further to do, as every complex polynomial is a product of linear factors.

Suppose that V is a real vector space. Then every real polynomial is a product of linear and irreducible quadratic factors, and we must show none of the latter occur. Again we argue by contradiction. Suppose $p(x) = x^2 + bx + c$ is an irreducible factor of $m_{\mathcal{T}}(x)$, and let $v \in V$ be a nonzero vector with $p(\mathcal{T})(v) = 0$. We can write $p(x) = (x + b/2)^2 + d^2$ where d is the real number $d = \sqrt{c^2 - b^2/4}$. Set $\mathcal{S} = \mathcal{T} + (b/2)\mathcal{I}$, so $(\mathcal{S}^2 + d^2\mathcal{I})(v) = 0$, i.e., $\mathcal{S}^2(v) = -d^2 v$. Then, as $\mathcal{S}$ is self-adjoint,

$$0 < \langle \mathcal{S}(v), \mathcal{S}(v) \rangle = \langle v, \mathcal{S}^*\mathcal{S}(v) \rangle = \langle v, \mathcal{S}^2(v) \rangle = -d^2 \langle v, v \rangle,$$

which is impossible. $\square$

Corollary 7.3.20 (Spectral theorem)**.** *(1) Let V be a finite-dimensional complex inner product space and let $\mathcal{T} : V \to V$ be a normal linear transformation. Then V has an orthonormal basis of eigenvectors of $\mathcal{T}$.*

(2) Let V be a finite-dimensional real inner product space and let $\mathcal{T} : V \to V$ be a self-adjoint linear transformation. Then V has an orthogonal basis of eigenvectors of $\mathcal{T}$.

Proof. The proof in both cases is identical. By Lemma 7.3.19, $m_{\mathcal{T}}(x)$ is a product of distinct linear factors. Let $\lambda_1, \dots, \lambda_k$ be the roots of $m_{\mathcal{T}}(x)$, i.e., by Lemma 4.2.6, the eigenvalues of $\mathcal{T}$. Let E_{λ_i} be the associated eigenspace of $\mathcal{T}$, for each i. By Theorem 4.3.4, $V = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_k}$, and then by Lemma 7.3.16(6), $V = E_{\lambda_1} \perp \cdots \perp E_{\lambda_k}$. By Theorem 7.2.1, each E_{λ_i} has an orthonormal basis $\mathcal{C}_i$. Then $\mathcal{C} = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_k$ is an orthonormal basis of eigenvectors of $\mathcal{T}$. □

We restate this result in matrix terms.

Corollary 7.3.21. *(1) Let A be a Hermitian matrix. Then there is a unitary matrix P and a diagonal matrix D with*

$$A = PDP^{-1} = PD\,{}^t\overline{P}.$$

(2) Let A be a real symmetric matrix. Then there is a real orthogonal matrix P and a diagonal matrix D with real entries with

$$A = PDP^{-1} = PD\,{}^tP.$$

We have a third formulation of the spectral theorem, in terms of orthogonal projections.

Corollary 7.3.22. *Under the hypotheses of the spectral theorem, there are distinct complex numbers $\lambda_1, \dots, \lambda_k$, which are real in case $\mathcal{T}$ is self-adjoint, and subspaces $W_1, \dots, W_k$, such that*

(1) $V = W_1 \perp \cdots \perp W_k$

(2) If $\mathcal{T}_i = \Pi_{W_i}$ is the orthogonal projection of V onto the subspace W_i, then $\mathcal{T}_i^2 = \mathcal{T}_i$, $\mathcal{T}_i\mathcal{T}_j = \mathcal{T}_j\mathcal{T}_i = 0$ for $i \neq j$, and $\mathcal{I} = \mathcal{T}_1 + \cdots + \mathcal{T}_k$. Furthermore,

$$\mathcal{T} = \lambda_1\mathcal{T}_1 + \cdots + \lambda_k\mathcal{T}_k.$$

Proof. Here $\lambda_1, \dots, \lambda_k$ are the eigenvalues of $\mathcal{T}$ and the subspaces $W_1, \dots, W_k$ are the eigenspaces $E_{\lambda_1}, \dots, E_{\lambda_k}$. □

Corollary 7.3.23. *In the situation of, and in the notation of, Corollary 7.3.22,*

$$\mathcal{T}^* = \overline{\lambda}_1\mathcal{T}_1 + \cdots + \overline{\lambda}_k\mathcal{T}_k.$$

Corollary 7.3.24. *Let V be a finite-dimensional inner product space and let $\mathcal{T} : V \to V$ be a linear transformation. Suppose that $m_{\mathcal{T}}(x)$ is a product of linear factors over $\mathbb{F}$ (which is always the case if $\mathbb{F} = \mathbb{C}$). Then $\mathcal{T}$ is an isometry if and only if $|\lambda| = 1$ for every eigenvalue $\lambda \in \mathbb{F}$ of $\mathcal{I}$.*

Let us compare arbitrary and normal linear transformations.

Theorem 7.3.25 (Schur's theorem)**.** *Let V be a finite-dimensional inner product space and let $\mathcal{T} : V \to V$ be an arbitrary linear transformation. Then V has an orthonormal basis $\mathcal{C}$ in which $[\mathcal{T}]_{\mathcal{C}}$ is upper triangular if and only if the minimum polynomial $m_{\mathcal{T}}(x)$ is a product of linear factors (this being automatic if $\mathbb{F} = \mathbb{C}$).*

Proof. The "only if" direction is clear. We prove the "if" direction.

For any linear transformation $\mathcal{T}$, if W is a $\mathcal{T}$-invariant subspace of V then $W^{\perp}$ is a $\mathcal{T}^*$-invariant subspace of V, because for any $x \in W$ and $y \in W^{\perp}$

$$0 = \langle \mathcal{T}(x), y \rangle = \langle x, \mathcal{T}^*(y) \rangle.$$

We prove the theorem by induction on $n = \dim(V)$. If $n = 1$ there is nothing to prove. Suppose the theorem is true for all inner product spaces of dimension $n - 1$ and let V have dimension n.

Since $m_{\mathcal{T}}(x)$ is a product of linear factors, so is $m_{\mathcal{T}^*}(x)$, by Corollary 7.3.3. In particular $\mathcal{T}^* : V \to V$ has an eigenvector v_n, and we may assume $\|v_n\| = 1$. Let W be the subspace of V spanned by $\{v_n\}$. Then $W^{\perp}$ is a subspace of V of dimension $n - 1$ that is invariant under $\mathcal{T}^{**} = \mathcal{T}$. If $\mathcal{S}$ is the restriction of $\mathcal{T}$ to $W^{\perp}$, then $m_{\mathcal{S}}(x)$ divides $m_{\mathcal{T}}(x)$, so $m_{\mathcal{S}}(x)$ is a product of linear factors. Applying the inductive hypothesis, we conclude that $W^{\perp}$ has an orthonormal basis $\mathcal{C}_1 = \{v_1, \ldots, v_{n-1}\}$ with $[\mathcal{S}]_{\mathcal{C}_1}$ upper triangular. Set $\mathcal{C} = \{v_1, \ldots, v_n\}$. Then $[\mathcal{T}]_{\mathcal{C}}$ is upper triangular. □

Theorem 7.3.26. *Let V be a finite-dimensional inner product space and let $\mathcal{T} : V \to V$ be a linear transformation. Let $\mathcal{C}$ be any orthonormal basis of V with $[\mathcal{T}]_{\mathcal{C}}$ upper triangular. Then $\mathcal{T}$ is normal if and only if $[\mathcal{T}]_{\mathcal{C}}$ is diagonal.*

Proof. The "if" direction is clear. We prove the "only if" direction. Let $E = [\mathcal{T}]_{\mathcal{C}}$. By the spectral theorem, Corollary 7.3.21, V has a basis $\mathcal{C}_1$ with $D = [\mathcal{T}]_{\mathcal{C}_1}$ diagonal. Then $E = PDP^{-1}$ where $P = P_{\mathcal{C} \leftarrow \mathcal{C}_1}$ is the change of basis matrix. We know $P = Q^{-1}R$ where $Q = P_{\mathcal{E}\leftarrow\mathcal{C}}$ and $R = P_{\mathcal{E}\leftarrow\mathcal{C}_1}$. Since $\mathcal{C}$ and $\mathcal{C}_1$ are both orthonormal, Q and R are both isometries, and hence P is an isometry, ${}^tP = P^{-1}$ in the real case and ${}^tP = \overline{P}^{-1}$ in the complex case. Thus ${}^tE = {}^t(PDP^{-1}) = {}^t(PD\,{}^tP) = P\,{}^tD\,{}^tP = PDP^{-1} = E$ in the real case, and similarly $\overline{{}^tE} = \overline{E}$ in the complex case. Since E is upper triangular, this forces E to be diagonal. □

7.4 EXAMPLES

In this section we present some interesting and important examples of inner product spaces and related phenomena. We look at orthogonal or orthonormal sets, linear transformations that do or do not have adjoints, and linear transformations that are or are not normal.

Our examples share a common set-up. We begin with an interval $I \subseteq \mathbb{R}$ and a "weight" function $w(x)$ on I. We further suppose that we have a vector space V of functions on I with the properties that

(a) $\int_I f(x)\overline{g(x)}w(x)\,dx$ is defined for all $f(x), g(x) \in V$

(b) $\int_I f(x)\overline{f}(x)w(x)\,dx$ is a nonnegative real number for every $f(x) \in V$, and is zero only if $f(x) = 0$.

Then V together with

$$\langle f(x), g(x)\rangle = \int_I f(x)\overline{g}(x)w(x)dx$$

is an inner product space.

Except in Examples 7.4.3 and 7.4.4, we restrict our attention to the real case. This is purely for convenience, and the results generalize to the complex case without change.

EXAMPLE 7.4.1. (1) Let $V = P_\infty(\mathbb{R})$, the space of all real polynomials. Then

$$\varphi\big(f(x), g(x)\big) = \langle f(x), g(x)\rangle = \int_0^1 f(x)g(x)dx$$

gives V the structure of an inner product space.

We claim that the map $\alpha_\varphi : V \to V^*$ is not surjective, where

$$\alpha_\varphi(g(x)f(x)) = \varphi(f(x), g(x)).$$

For any $a \in [0, 1]$, we have the element $\mathbf{E}_a$ of V^* given by $\mathbf{E}_a(f(x)) = f(a)$. We claim that for any finite set of points $\{a_1, \ldots, a_k\}$ in $[0, 1]$ and any constants $\{c_1, \ldots, c_k\}$, not all zero, $\sum c_i\mathbf{E}_{a_i}$ is not in $\alpha_\varphi(V)$. We prove this by contradiction. Suppose $\sum c_i \mathbf{E}_{a_i} = \alpha_\varphi(g(x))$ for some $g(x) \in V$. Then for any polynomial $f(x) \in V$,

$$\int_0^1 f(x)g(x) = \sum_{i=1}^{k} c_i f\big(a_i\big).$$

Clearly $g(x) \neq 0$.

Choose

$$f(x) = \left(\prod_{i=1}^{k} \big(x - a_i\big)^2\right) g(x).$$

The left-hand side of this equation is positive while the right-hand side is zero, which is impossible.

(2) For any n, let $V = P_{n-1}(\mathbb{R})$, the space of all real polynomials of degree at most n. Again

$$\varphi\big(f(x), g(x)\big) = \big\langle f(x), g(x)\big\rangle = \int_0^1 f(x)g(x)dx$$

gives V the structure of an inner product space. Here $\dim(V) = n$ so $\dim(V^*) = n$ as well.

(a) Any n linearly independent elements of V^* form a basis of V^*. In particular $\{\mathbf{E}_{a_1}, \ldots, \mathbf{E}_{a_n}\}$ is a basis of V^* for any distinct set of points $\{a_1, \ldots, a_n\}$ in $[0, 1]$. Then for any fixed $g(x) \in V$, $\alpha_\varphi(g(x)) \in V^*$, so $\alpha_\varphi(g(x))$ is a linear combination of $\{\mathbf{E}_{a_1}, \ldots, \mathbf{E}_{a_n}\}$. In other words, there are constants $c_1, \ldots, c_n$ such that

$$\int_0^1 f(x)g(x)dx = \sum_{i=1}^{n} c_i f\big(a_i\big).$$

In particular, we may choose $g(x) = 1$, so there are constants $c_1, \ldots, c_n$ with

$$\int_0^1 f(x)dx = \sum_{i=1}^{n} c_i f_i\big(a_i\big) \quad \text{for every } f(x) \in P_{n-1}(x).$$

(b) Since α_φ is an injection and V is finite-dimensional, it is a surjection. Thus any element of V^* is $\alpha_\varphi(g(x))$ for a unique polynomial $g(x) \in P_{n-1}$. In particular, this is true for $\mathbf{E}_a$, for any $a \in [0, 1]$. Thus there is a polynomial $g(x) \in P_{n-1}(x)$ such that

$$f(a) = \int_0^1 f(x)g(x)dx \quad \text{for every } f(x) \in P_{n-1}(x).$$

Concrete instances of both parts (a) and (b) of this example were given in Example 1.6.9(3) and (4). ◇

EXAMPLE 7.4.2. We let $V = P_\infty(\mathbb{R})$ and we choose the standard basis

$$\mathcal{E} = \{p_0(x), p_1(x), p_2(x), \ldots\} = \{1, x, x^2, \ldots\}$$

of V. We may apply the Gram-Schmidt process to obtain an orthonormal basis $\mathcal{C} = \{q_0(x), q_1(x), q_2(x), \ldots\}$ of V. Actually, we will obtain an orthogonal basis $\mathcal{C}$ of V, but we will normalize the basis elements by $\|q_i(x)\|^2 = h_i$ where $\{h_0, h_1, h_2, \ldots\}$ is not necessarily $\{1, 1, 1, \ldots\}$. This is partly for historical reasons, but mostly because the purposes for which these functions were originally derived made the given normalizations more useful.

(1) Let $I = [-1, 1]$ and $w(x) = 1$. Let $h_n = 2/(2n + 1)$. The sequence of polynomials we obtain in this way are the *Legendre polynomials* $P_0(x), P_1(x), P_2(x), \ldots$. The first few of these are

$$\begin{aligned}
P_0(x) &= 1\\
P_1(x) &= x\\
P_2(x) &= \frac{1}{2}\big(-1 + 3x^2\big)\\
P_3(x) &= \frac{1}{2}\big(-3x + 5x^3\big)\\
P_4(x) &= \frac{1}{8}\big(3 - 30x^2 + 35x^4\big),
\end{aligned}$$

and, expressing the elements of $\mathcal{E}$ in terms of them,

$$\begin{aligned}
1 &= P_0(x)\\
x &= P_1(x)\\
x^2 &= \frac{1}{3}\big(P_0(x) + P_2(x)\big)\\
x^3 &= \frac{1}{5}\big(3P_1(x) + 2P_3(x)\big)\\
x^4 &= \frac{1}{35}\big(7P_0(x) + 20P_2(x) + 8P_4(x)\big).
\end{aligned}$$

(2) Let $I = [-1, 1]$ and $w(x) = 1/\sqrt{1 - x^2}$. Let $h_0 = \pi$ and $h_n = \pi/2$ for $n \geq 1$. The sequence of polynomials we obtain in this way are the *Chebyshev polynomials of the first kind* $T_0(x), T_1(x), T_2(x), \ldots$. The first

few of these are given by

$$\begin{aligned}
T_0(x) &= 1\\
T_1(x) &= x\\
T_2(x) &= -1 + 2x^2\\
T_3(x) &= -3x + 4x^3\\
T_4(x) &= 1 - 8x^2 + 8x^4,
\end{aligned}$$

and, expressing the elements of $\mathcal{E}$ in terms of them,

$$\begin{aligned}
1 &= T_0(x)\\
x &= T_1(x)\\
x^2 &= \frac{1}{2}\big(T_0(x) + T_2(x)\big)\\
x^3 &= \frac{1}{4}\big(3T_1(x) + T_3(x)\big)\\
x^4 &= \frac{1}{8}\big(3T_0(x) + 4T_2(x) + T_4(x)\big).
\end{aligned}$$

(3) Let $I = [-1, 1]$ and $w(x) = \sqrt{1 - x^2}$. Let $h_n = \pi/2$ for all n. The sequence of polynomials we obtain in this way are the *Chebyshev polynomials of the second kind* $U_0(x), U_1(x), U_2(x), \ldots$. The first few of these are

$$\begin{aligned}
U_0(x) &= 1\\
U_1(x) &= 2x\\
U_2(x) &= -1 + 4x^2\\
U_3(x) &= -4x + 8x^3\\
U_4(x) &= 1 - 12x^2 + 16x^4,
\end{aligned}$$

and, expressing the elements of $\mathcal{E}$ in terms of them,

$$\begin{aligned}
1 &= U_0(x)\\
x &= \frac{1}{2}U_1(x)\\
x^2 &= \frac{1}{4}\big(U_0(x) + U_2(x)\big)\\
x^3 &= \frac{1}{8}\big(2U_1(x) + U_3(x)\big)\\
x^4 &= \frac{1}{16}\big(2U_0(x) + 3U_2(x) + U_4(x)\big).
\end{aligned}$$

(4) Let $I = R$ and $w(x) = e^{-x^2}$. Let $h_n = \sqrt{\pi}2^n n!$. The sequence of polynomials we obtain in this way are the *Hermite polynomials* $H_0(x)$, $H_1(x)$, $H_2(x)$, ... The first few of these are

$$\begin{aligned} H_0(x) &= 1 \\ H_1(x) &= 2x \\ H_2(x) &= -2 + 4x^2 \\ H_3(x) &= -12x + 8x^3 \\ H_4(x) &= 12 - 48x^2 + 8x^4 \end{aligned}$$

and, expressing the elements of $\mathcal{E}$ in terms of them,

$$\begin{aligned} 1 &= H_0(x) \\ x &= \frac{1}{2}H_1(x) \\ x^2 &= \frac{1}{4}\big(2H_0(x) + H_2(x)\big) \\ x^3 &= \frac{1}{8}\big(6H_1(x) + H_3(x)\big) \\ x^4 &= \frac{1}{16}\big(12H_0(x) + 12H_2(x) + H_4(x)\big). \end{aligned} \qquad \diamond$$

EXAMPLE 7.4.3. We consider an orthogonal (and hence linearly independent) set $\mathcal{C} = \{q_0(x), q_1(x), q_2(x), \ldots\}$ of nonzero functions in V. Let $h_n = \|q_n\|$ for each n.

Let $f(x) \in V$ be arbitrary. For each $n = 0, 1, 2, \ldots$ let

$$c_n = \big(1/h_n\big)\big\langle f(x), q_n(x)\big\rangle,$$

the *Fourier coefficients* of $f(x)$ in terms of $\mathcal{C}$, and form the sequence of functions $\{g_0(x), g_1(x), g_2(x), \ldots\}$ defined by

$$g_m(x) = \sum_{k=1}^{m} c_k q_k(x).$$

Then for any m,

$$\big\langle g_m(x), q_n(x)\big\rangle = \big\langle f(x), q_n(x)\big\rangle \quad \text{for all } n \leq m$$

and of course

$$\big\langle g_m(x), q_n(x)\big\rangle = 0 \quad \text{for all } n > m.$$

We think of $\{g_0(x), g_1(x), g_2(x), \ldots\}$ as a sequence of approximations to $f(x)$, and we hope that it converges in some sense to $f(x)$. Of course, the question of convergence is one of analysis and not linear algebra. $\diamond$

We do, however, present the following extremely important special case.

EXAMPLE 7.4.4. Let $V = L^2([-\pi, \pi])$. By definition, this is the space of complex-valued measurable function $f(x)$ on $[-\pi, \pi]$ such that the Lebesgue integral

$$\int_{-\pi}^{\pi} \left|f(x)\right|^2 dx$$

is finite.

Then, by the Cauchy-Schwartz-Buniakowsky inequality, V is an inner product space with inner product

$$\langle f(x), g(x)\rangle = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)\overline{g}(x)dx.$$

For each integer n, let $p_n(x) = e^{inx}$. Then $\{p_n(x)\}$ is an orthonormal set, as we see from the equalities

$$\left\|p_n(x)\right\|^2 = \frac{1}{2\pi}\int_{-\pi}^{\pi} e^{inx}e^{-inx}dx = \frac{1}{2\pi}\int_{-\pi}^{\pi} 1\,dx = 1$$

and, for $m \neq n$,

$$\begin{aligned}\langle p_m(x), p_n(x)\rangle &= \frac{1}{2\pi}\int_{-\pi}^{\pi} e^{imx}e^{-inx}dx = \frac{1}{2\pi}\int_{-\pi}^{\pi} e^{i(m-n)x} \\ &= \frac{1}{2\pi i(m-n)}e^{i(m-n)x}\Big|_{-\pi}^{\pi} = 0.\end{aligned}$$

For any function $f(x) \in L^2([-\pi, \pi])$ we have its *classical Fourier coefficients*

$$\widehat{f}(n) = \langle f(x), p_n(x)\rangle = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)\overline{p_n}(x)dx = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)e^{-inx}dx$$

for any integer n, and the Fourier expansion

$$g(x) = \sum_{n=-\infty}^{\infty} \widehat{f}(n)p_n(x).$$

It is a theorem from analysis that the right-hand side is well-defined, i.e., that if for a nonnegative integer m we define

$$g_m(x) = \sum_{n=-m}^{m} \widehat{f}(n) p_n(x),$$

then $g(x) = \lim_{m\to\infty} g_m(x)$ exists, and furthermore it is another theorem from analysis that, as functions in $L^2([-\pi, \pi])$,

$$f(x) = g(x).$$

This is equivalent to $\lim_{m\to\infty} \|f(x) - g_m(x)\| = 0$, and so we may regard $g_0(x)$, $g_1(x)$, $g_2(x), \ldots$ as a series of approximations that converges to $f(x)$ (in norm). $\diamond$

Now we turn from orthogonal sets to adjoints and normality.

EXAMPLE 7.4.5. (1) Let $V = C_0^\infty(\mathbb{R})$ be the space of real valued infinitely differentiable functions on $\mathbb{R}$ with compact support (i.e., for every $f(x) \in C_0^\infty(\mathbb{R})$ there is a compact interval $I \subseteq \mathbb{R}$ with $f(x) = 0$ for $x \notin I$). Then V is an inner product space with inner product given by

$$\langle f(x), g(x)\rangle = \int_{-\infty}^{\infty} f(x)g(x)dx.$$

Let $\mathbf{D} : V \to V$ be defined by $\mathbf{D}(f(x)) = f'(x)$. Then $\mathbf{D}$ has an adjoint $\mathbf{D}^* : V \to V$ given by $\mathbf{D}^*(f(x)) = E(x) = -f'(x)$, i.e., $\mathbf{D}^* = -\mathbf{D}$. To see this, we compute

$$\begin{aligned}
&\langle \mathbf{D}(f(x)), g(x)\rangle - \langle f(x), E(g(x))\rangle \\
&\quad = \int_{-\infty}^{\infty} f'(x)g(x)dx - \int_{-\infty}^{\infty} f(x)\big(-g'(x)\big)dx \\
&\quad = \int_{-\infty}^{\infty} \big(f'(x)g(x) + f(x)g'(x)\big)dx \\
&\quad = \int_{-\infty}^{\infty} \big(f(x)g(x)\big)' dx = f(x)g(x)|_a^b = 0,
\end{aligned}$$

where the support of $f(x)g(x)$ is contained in the interval $[a, b]$.

Since $\mathbf{D}^* = -\mathbf{D}$, $\mathbf{D}^*$ commutes with $\mathbf{D}$, so $\mathbf{D}$ is normal.

(2) Let $V = C^\infty(\mathbb{R})$ or $V = P_\infty(\mathbb{R})$, with inner product given by

$$\langle f(x), g(x)\rangle = \int_0^1 f(x)g(x)dx.$$

We claim that $\mathbf{D} : V \to V$ defined by $\mathbf{D}(f(x)) = f'(x)$ does not have an adjoint. We prove this by contradiction. Suppose $\mathbf{D}$ has an adjoint $\mathbf{D}^* = E$. Guided by (1) we write $E(f(x)) = -f'(x) + F(f(x))$. Then we compute

$$\begin{aligned}
&\big\langle \mathbf{D}\big(f(x)\big), g(x)\big\rangle - \big\langle f(x), E\big(g(x)\big)\big\rangle \\
&\qquad = \int_0^1 \big(f(x)g(x)\big)'\,dx - \int_0^1 f(x)F\big(g(x)\big)\,dx \\
&\qquad = f(1)g(1) - f(0)g(0) - \int_0^1 f(x)F\big(g(x)\big)\,dx,
\end{aligned}$$

true for every pair of functions $f(x), g(x) \in V$. Suppose there is some function $g_0(x)$ with $F(g_0(x)) \neq 0$. Setting $f(x) = x^2(x-1)^2F(g_0(x))$ we find a nonzero right-hand side, so E is not an adjoint of $\mathbf{D}$. Thus the only possibility is that $F(f(x)) = 0$ for every $f(x) \in V$, and hence that $E(f(x)) = -f'(x)$. Then $f(1)g(1) - f(0)g(0) = 0$ for every pair of functions $f(x), g(x) \in V$, which is false (e.g., for $f(x) = 1$ and $g(x) = x$).

(3) For any fixed n let $V = P_{n-1}(\mathbb{R})$ with the same inner product. Then V is finite-dimensional. Thus $\mathbf{D} : V \to V$ has an adjoint $\mathbf{D}^* : V \to V$. In case $n = 1$, $\mathbf{D} = 0$ so $\mathbf{D}^* = 0$, and $\mathbf{D}$ is trivially normal. For $n \geq 1$, $\mathbf{D}$ is not normal: Let $f(x) = x$. Then $\mathbf{D}^2(f(x)) = 0$ but $\mathbf{D}(f(x)) \neq 0$, so $\mathbf{D}$ cannot be normal, by Lemma 7.3.16(4).

Let us compute $\mathbf{D}^*$ for some small values of n. If we set $\mathbf{D}^*(g(x)) = h(x)$, we are looking for functions satisfying

$$\int_0^1 f'(x)g(x)dx = \int_0^1 f(x)h(x)dx \quad \text{for every } f(x) \in V.$$

Since $\mathbf{D}^*$ is a linear transformation, it suffices to give the values of $\mathbf{D}^*$ on the elements of a basis of V. We choose the standard basis $\mathcal{E}$.

On $P_0(\mathbb{R})$:

$$\mathbf{D}^*(1) = 0.$$

On $P_1(\mathbb{R})$:

$$\begin{aligned}
\mathbf{D}^*(1) &= -6 + 12x \\
\mathbf{D}^*(x) &= -3 + 6x.
\end{aligned}$$

On $P_2(\mathbb{R})$:

$$\mathbf{D}^*(1) = -6 + 12x$$
$$\mathbf{D}^*(x) = 2 - 24x + 30x^2$$
$$\mathbf{D}^*\left(x^2\right) = 3 - 26x + 30x^2. \qquad \diamond$$

7.5 THE SINGULAR VALUE DECOMPOSITION

In this section we augment our results on normal linear transformations to obtain geometric information on an arbitrary linear transformation $\mathcal{T} : V \to W$ between finite dimensional inner product spaces. We assume we are in this situation throughout.

Lemma 7.5.1. *(1) $\mathcal{T}^*\mathcal{T}$ is self-adjoint.*
(2) $\operatorname{Ker}(\mathcal{T}^*\mathcal{T}) = \operatorname{Ker}(\mathcal{T})$.

Proof. For (1), $(\mathcal{T}^*\mathcal{T})^* = \mathcal{T}^*\mathcal{T}^{**} = \mathcal{T}^*\mathcal{T}$.

For (2), we have $\operatorname{Ker}(\mathcal{T}^*\mathcal{T}) \supseteq \operatorname{Ker}(\mathcal{T})$. On the other hand, let $v \in \operatorname{Ker}(\mathcal{T}^*\mathcal{T})$. Then

$$0 = \langle v, 0\rangle = \left\langle v, \mathcal{T}^*\mathcal{T}(v)\right\rangle = \left\langle \mathcal{T}(v), \mathcal{T}(v)\right\rangle$$

so $\mathcal{T}(v) = 0$ and hence $\operatorname{Ker}(\mathcal{T}^*\mathcal{T}) \subseteq \operatorname{Ker}(\mathcal{T})$. $\square$

DEFINITION 7.5.2. A linear transformation $\mathcal{S} : V \to V$ is *nonnegative* (respectively *positive*) if $\mathcal{S}$ is self-adjoint and $\langle \mathcal{S}(v), v\rangle \geq 0$ (respectively $\langle \mathcal{S}(v), v\rangle > 0$) for every $v \in V$, $v \neq 0$. $\diamond$

Lemma 7.5.3. *The following are equivalent:*

(1) $\mathcal{S} : V \to V$ is nonnegative (respectively positive).

(2) $\mathcal{S} : V \to V$ is self-adjoint and all the eigenvalues of $\mathcal{S}$ are nonnegative (respectively positive).

(3) $\mathcal{S} = \mathcal{T}^*\mathcal{T}$ for some (respectively some invertible) linear transformation $\mathcal{T} : V \to V$.

Proof. (1) and (2) are equivalent by the spectral theorem, Corollary 7.3.20.

If $\mathcal{S}$ is self-adjoint with distinct eigenvalues $\lambda_1, \ldots, \lambda_k$, all ≥ 0, then in the notation of Corollary 7.3.22 we have $\mathcal{S} = \lambda_1\mathcal{T}_1 + \cdots + \lambda_k\mathcal{T}_k$. Choosing $\mathcal{T} = \mathcal{R} = \sqrt{\lambda_1}\mathcal{T}_1 + \cdots + \sqrt{\lambda_k}\mathcal{T}_k$, we have $\mathcal{T}^* = \mathcal{R}$ as well, and then $\mathcal{T}^*\mathcal{T} = \mathcal{R}^2 = \mathcal{S}$, so (2) implies (3).

Suppose (3) is true. We already know by Lemma 7.5.1(1) that $\mathcal{T}^*\mathcal{T}$ is self-adjoint. Let λ be an eigenvalue of $\mathcal{T}^*\mathcal{T}$, and let v be an associated eigenvector. Then

$$\lambda\langle v, v\rangle = \langle v, \lambda v\rangle = \big\langle v, \mathcal{T}^*\mathcal{T}(v)\big\rangle = \big\langle \mathcal{T}(v), \mathcal{T}(v)\big\rangle,$$

so $\lambda \geq 0$. By Lemma 7.5.1(2), $\mathcal{T}^*\mathcal{T}$ is invertible if and only if $\mathcal{T}$ is invertible, and we know that $\mathcal{T}$ is invertible if and only if all its eigenvalues are nonzero. Thus (3) implies (2). ☐

Corollary 7.5.4. *For any nonnegative linear transformation $\mathcal{S} : V \to V$ there is a unique nonnegative linear transformation $\mathcal{R} : V \to V$ with $\mathcal{R}^2 = \mathcal{S}$.*

Proof. $\mathcal{R}$ is constructed in the proof of Lemma 7.5.3. Uniqueness follows easily by considering eigenvalues and eigenspaces. ☐

DEFINITION 7.5.5. Let $\mathcal{T} : V \to W$ have rank r. Let $\lambda_1, \ldots, \lambda_r$ be the (not necessarily distinct) nonzero eigenvalues of $\mathcal{T}^*\mathcal{T}$ (all of which are necessarily positive) ordered so that $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_r$. Then $\sigma_1 = \sqrt{\lambda_1}, \ldots, \sigma_r = \sqrt{\lambda_r}$ are the *singular values* of $\mathcal{T}$. ◇

Theorem 7.5.6 (Singular value decomposition)**.** *Let $\mathcal{T} : V \to W$ have rank r, and let $\sigma_1, \ldots, \sigma_r$ be the singular values of $\mathcal{T}$. Then there are orthonormal bases $\mathcal{C} = \{v_1, \ldots, v_n\}$ of V and $\mathcal{D} = \{w_1, \ldots, w_m\}$ of W such that*

$$\mathcal{T}\big(v_i\big) = \sigma_i w_i \quad \textit{for } i = 1, \ldots, r \quad \textit{and } \mathcal{T}\big(v_i\big) = 0 \quad \textit{for } i > r.$$

Proof. Since $\mathcal{T}^*\mathcal{T}$ is self-adjoint, we know that there is an orthonormal basis $\mathcal{C} = \{v_1, \ldots, v_n\}$ of V of eigenvectors of $\mathcal{T}^*\mathcal{T}$ and we order the basis so that the associated eigenvalues are $\lambda_1, \ldots, \lambda_r, 0, \ldots, 0$. For $i = 1, \ldots, r$, let

$$w_i = \big(1/\sigma_i\big)\mathcal{T}\big(v_i\big).$$

We claim $\mathcal{C}_1 = \{w_1, \ldots, w_r\}$ is an orthonormal set. We compute

$$\big\langle w_i, w_i\big\rangle = \big(1/\sigma_i\big)^2\big\langle\mathcal{T}\big(v_i\big), \mathcal{T}\big(v_i\big)\big\rangle = \big(1/\sigma_i\big)^2\lambda_i = 1$$

and for $i \neq j$

$$\begin{aligned}\big\langle w_i, w_j\big\rangle &= \big(1/\sigma_i\sigma_j\big)\big\langle\mathcal{T}\big(v_i\big), \mathcal{T}\big(v_j\big)\big\rangle = \big(1/\sigma_i\sigma_j\big)\big\langle v_i, \mathcal{T}^*\mathcal{T}\big(v_j\big)\big\rangle \\ &= \big(1/\sigma_i\sigma_j\big)\big\langle v_i, \lambda_j v_j\big\rangle = \big(\lambda_j/\sigma_i\sigma_j\big)\big\langle v_i, v_j\big\rangle = 0.\end{aligned}$$

Then extend $\mathcal{C}$ to an orthonormal basis $\mathcal{C}$ of W. ☐

REMARK 7.5.7. This theorem has a geometric interpretation: We choose new letters to have an unbiased description. Let X be an inner product space and consider an orthonormal set $\mathcal{B} = \{x_1, \ldots, x_n\}$ of vectors in X. Then for any positive real numbers $a_1, \ldots, a_k$,

$$\left\{ x = c_1x_1 + \cdots + c_kx_k \,\middle|\, \sum_{i=1}^{k} \left|c_i\right|^2/a_i^2 = 1 \right\}$$

defines an ellipsoid in X. If $k = \dim(X)$ and $a_i = 1$ for each i this ellipsoid is the unit sphere in X.

The singular value decomposition says that if $\mathcal{T} : V \to W$ is a linear transformation, then the image of the unit sphere of V under $\mathcal{T}$ is an ellipsoid in W, and furthermore it completely identifies that ellipsoid. $\diamond$

We also observe the following.

Corollary 7.5.8. *$\mathcal{T}$ and $\mathcal{T}^*$ have the same singular values.*

Proof. This is a special case of Theorem 5.9.2. $\square$

Proceeding along these lines we now derive the polar decomposition of a linear transformation.

Theorem 7.5.9 (Polar decomposition)**.** *Let $\mathcal{T} : V \to V$ be a linear transformation. Then there is a unique positive semidefinite linear transformation $\mathcal{R} : V \to V$ and an isometry $\mathcal{Q} : V \to V$ with $\mathcal{T} = \mathcal{Q}\mathcal{R}$. If $\mathcal{T}$ is invertible, $\mathcal{Q}$ is also unique.*

Proof. Suppose $\mathcal{T} = \mathcal{Q}\mathcal{R}$. By definition, $\mathcal{Q}^* = \mathcal{Q}^{-1}$ and $\mathcal{R}^* = \mathcal{R}$. Then

$$\mathcal{T}^*\mathcal{T} = (\mathcal{Q}\mathcal{R})^*\mathcal{Q}\mathcal{R} = \mathcal{R}^*(\mathcal{Q}^*\mathcal{Q})\mathcal{R} = \mathcal{R}\mathcal{I}\mathcal{R} = \mathcal{R}^2.$$

Then, by Corollary 7.5.4, $\mathcal{R}$ is unique.

Suppose that $\mathcal{T}$ is invertible, and define $\mathcal{R}$ as in Corollary 7.5.4. Then $\mathcal{R}$ is invertible, and then $\mathcal{T} = \mathcal{Q}\mathcal{R}$ for the unique linear transformation $\mathcal{Q} = \mathcal{T}\mathcal{R}^{-1}$. It remains to show that $\mathcal{Q}$ is an isometry. We compute, for any $v \in V$,

$$\begin{aligned}\left\langle \mathcal{Q}(v), \mathcal{Q}(v) \right\rangle &= \left\langle \mathcal{T}\mathcal{R}^{-1}(v), \mathcal{T}\mathcal{R}^{-1}(v) \right\rangle = \left\langle v, \left(\mathcal{T}\mathcal{R}^{-1}\right)^*\mathcal{T}\mathcal{R}^{-1}(v) \right\rangle \\ &= \left\langle v, \left(\mathcal{R}^{-1}\right)^*\mathcal{T}^*\mathcal{T}\mathcal{R}^{-1}(v) \right\rangle = \left\langle v, \mathcal{R}^{-1}\left(\mathcal{T}^*\mathcal{T}\right)\mathcal{R}^{-1}(v) \right\rangle \\ &= \left\langle v, \mathcal{R}^{-1}\mathcal{R}^2\mathcal{R}^{-1}(v) \right\rangle = \langle v, v \rangle.\end{aligned}$$

Suppose that $\mathcal{T}$ is not (necessarily) invertible. Choose a linear transformation $\mathcal{S} : \mathrm{Im}(\mathcal{R}) \to V$ with $\mathcal{R}\mathcal{S} = \mathcal{I} : \mathrm{Im}(\mathcal{R}) \to \mathrm{Im}(\mathcal{R})$.

By Lemma 7.5.1 we know that $\mathrm{Ker}(\mathcal{T}^*\mathcal{T}) = \mathrm{Ker}(\mathcal{T})$ and also that

$$\mathrm{Ker}(\mathcal{R}) = \mathrm{Ker}(\mathcal{R}^*\mathcal{R}) = \mathrm{Ker}(\mathcal{R}^2) = \mathrm{Ker}(\mathcal{T}^*\mathcal{T}).$$

Hence $Y = \mathrm{Im}(\mathcal{R})^\perp$ and $Z = \mathrm{Im}(\mathcal{T})^\perp$ are inner product spaces of the same dimension $(\dim(\mathrm{Ker}(\mathcal{T})))$ and hence are isometric. Choose an isometry $\mathcal{Q}_0 : Y \to Z$. Define $\mathcal{Q}$ as follows: Let $X = \mathrm{Im}(\mathcal{R})$, so $V = X \perp Y$. Then

$$\mathcal{Q}(v) = \mathcal{T}\big(\mathcal{S}(x)\big) + \mathcal{Q}_0(y) \quad \text{where } v = x + y,\ x \in X,\ y \in Y.$$

(In the invertible case, $\mathcal{S} = \mathcal{R}^{-1}$ and $\mathcal{Q}_0 : \{0\} \to \{0\}$, so $\mathcal{Q}$ is unique, $\mathcal{Q} = \mathcal{T}\mathcal{R}^{-1}$. In general, it can be checked that $\mathcal{Q}$ is independent of the choice of $\mathcal{S}$, but it depends on the choice of $\mathcal{Q}_0$, and is not unique.)

We claim that $\mathcal{Q}\mathcal{R} = \mathcal{T}$ and that $\mathcal{Q}$ is an isometry.

To prove the first claim, we make a preliminary observation. For any $v \in V$, let $x = \mathcal{R}(v)$. Then $\mathcal{R}(\mathcal{S}(x) - v) = \mathcal{R}\mathcal{S}(x) - \mathcal{R}(v) = x - x = 0$, i.e., $\mathcal{S}(x) - v \in \mathrm{Ker}(\mathcal{R})$. But $\mathrm{Ker}(\mathcal{R}) = \mathrm{Ker}(\mathcal{T})$, so $\mathcal{S}(x) - v \in \mathrm{Ker}(\mathcal{T})$, i.e., $\mathcal{T}(\mathcal{S}(x) - v) = 0$, so $\mathcal{T}(\mathcal{S}(x)) = \mathcal{T}(v)$. Using this observation we compute that for any $v \in V$,

$$\mathcal{Q}\mathcal{R}(v) = \mathcal{Q}(x + 0) = \mathcal{T}\mathcal{S}(x) + \mathcal{Q}_0(0) = \mathcal{T}(v) + 0 = \mathcal{T}(v).$$

To prove the second claim, we observe that for any $v \in V$,

$$\big\langle \mathcal{R}(v), \mathcal{R}(v) \big\rangle = \big\langle v, \mathcal{R}^*\mathcal{R}(v) \big\rangle = \big\langle v, \mathcal{R}^2(v) \big\rangle = \big\langle v, \mathcal{T}^*\mathcal{T}(v) \big\rangle = \big\langle \mathcal{T}(v), \mathcal{T}(v) \big\rangle.$$

Then, using the fact that $\mathrm{Im}(\mathcal{Q}_0) \subseteq Z = \mathrm{Im}(\mathcal{T})^\perp$, and writing $v = x + y$ as above,

$$\begin{aligned}
\big\langle \mathcal{Q}(v), \mathcal{Q}(v) \big\rangle &= \big\langle \mathcal{T}\mathcal{S}(x) + \mathcal{Q}_0(y), \mathcal{T}\mathcal{S}(x) + \mathcal{Q}_0(y) \big\rangle \\
&= \big\langle \mathcal{T}\mathcal{S}(x), \mathcal{T}\mathcal{S}(x) \big\rangle + \big\langle \mathcal{Q}_0(y), \mathcal{Q}_0(y) \big\rangle \\
&= \big\langle \mathcal{T}(v), \mathcal{T}(v) \big\rangle + \langle y, y \rangle = \big\langle \mathcal{R}(v), \mathcal{R}(v) \big\rangle + \langle y, y \rangle \\
&= \langle x, x \rangle + \langle y, y \rangle = \langle x + y, x + y \rangle = \langle v, v \rangle. \qquad \square
\end{aligned}$$

CHAPTER 8

Matrix groups as Lie groups

Lie groups are central objects in mathematics. They lie at the intersection of algebra, analysis, and topology. In this chapter, we will show that many of the groups we have already encountered are in fact Lie groups.

This chapter presupposes a certain knowledge of differential topology, and so we will use definitions and theorems from differential topology without further comment. We will also be a bit sketchy in our arguments in places. Throughout this chapter, "smooth" means C^∞. We use c_{ij} to denote a matrix entry that may be real or complex, x_{ij} to denote a real matrix entry and z_{ij} to denote a complex matrix entry, and we write $z_{ij} = x_{ij} + iy_{ij}$ where x_{ij} and y_{ij} are real numbers. We let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$ and $d_{\mathbb{F}} = \dim_{\mathbb{R}} \mathbb{F}$, so that $d_{\mathbb{R}} = 1$ and $d_{\mathbb{C}} = 2$.

8.1 Definition and first examples

DEFINITION 8.1.1. G is a Lie group if

(1) G is a group.

(2) G is a smooth manifold.

(3) The multiplication map $m : G \times G \to G$ by $m(g_1, g_2) = g_1 g_2$ and the inversion map $i : G \to G$ by $i(g) = g^{-1}$ are both smooth maps. $\diamond$

EXAMPLE 8.1.2. (1) The *general linear group*

$$\mathrm{GL}_n(\mathbb{F}) = \{\text{invertible } n\text{-by-}n \text{ matrices with entries in } \mathbb{F}\}.$$

$\mathrm{GL}_n(\mathbb{F})$ is a Lie group: It is an open subset of $\mathbb{F}^{n^2}$ as

$$\mathrm{GL}_n(\mathbb{F}) = \det{}^{-1}(\mathbb{F} - \{0\}),$$

so it is a smooth manifold of dimension $d_{\mathbb{F}}n^2$. It is noncompact for every $n \geq 1$ as $\mathrm{GL}_1(\mathbb{F})$ contains matrices $[c]$ with $|c|$ arbitrarily large. $\mathrm{GL}_n(\mathbb{R})$ has two components and $\mathrm{GL}_n(\mathbb{C})$ is connected, as we showed in Theorem 3.5.1 and Theorem 3.5.7. The multiplication map is a smooth map as it is a polynomial in the entries of the matrices, and the inversion map is a smooth map as it is a rational function of the entries of the matrix with nonvanishing denominator, as we see from Corollary 3.3.9.

(2) The *special linear group*

$$\mathrm{SL}_n(\mathbb{F}) = \{n\text{-by-}n \text{ matrices of determinant 1 with entries in } \mathbb{F}\}.$$

$\mathrm{SL}_n(\mathbb{F})$ is a Lie group: $\mathrm{SL}_n(\mathbb{F}) = \det^{-1}(\{1\})$. To show $\mathrm{SL}_n(\mathbb{F})$ is a smooth manifold we must show that 1 is a regular value of det. Let $M = (c_{ij})$, $M \in \mathrm{SL}_n(\mathbb{F})$. Expanding by minors of row i, we see that

$$1 = \det(M) = (-1)^{i+1}\det(M_{i1}) + (-1)^{i+2}\det(M_{i2}) + \cdots,$$

where M_{ij} is the submatrix obtained by deleting row i and column j of M, so at least one of the terms in the sum is nonzero, say $c_{ij}(-1)^{i+j}\det(M_{ij})$. But then the derivative matrix $\det'$ of det with respect to the matrix entries, when evaluated at M, has the entry $(-1)^{i+j}\det(M_{ij}) \neq 0$, so this matrix has rank $d_{\mathbb{F}}$ everywhere. Hence, by the inverse function theorem, $\mathrm{SL}_n(\mathbb{F})$ is a smooth submanifold of $\mathbb{F}^{n^2}$. Since $\{1\} \subseteq \mathbb{F}$ has codimension $d_{\mathbb{F}}$, $\mathrm{SL}_n(\mathbb{F})$ has codimension $d_{\mathbb{F}}$ in $\mathbb{F}^{n^2}$, so it is a smooth manifold of dimension $d_{\mathbb{F}}(n^2 - 1)$.

$\mathrm{SL}_1(\mathbb{F}) = \{[1]\}$ is a single point and hence is compact, but $\mathrm{SL}_n(\mathbb{F})$ is noncompact for $n > 1$, as we see from the fact that $\mathrm{SL}_2(\mathbb{F})$ contains matrices of the form $\begin{bmatrix} c & 0 \\ 0 & 1/c \end{bmatrix}$ with $|c|$ arbitrarily large. An easy modification of the proofs of Theorem 3.5.1 and Theorem 3.5.7 shows that $\mathrm{SL}_n(\mathbb{F})$ is always connected. Locally, $\mathrm{SL}_n(\mathbb{F})$ is parameterized by all but one matrix entry, and, by the implicit function theorem, that entry is locally a function of the other $n^2 - 1$ entries. We have observed that multiplication and inversion are smooth functions in the entries of a matrix, and hence multiplication and inversion are smooth functions of the parameters in a coordinate patch around each element of $\mathrm{SL}_n(\mathbb{F})$, i.e., $m = \mathrm{SL}_n(\mathbb{F}) \times \mathrm{SL}_n(\mathbb{F}) \to \mathrm{SL}_n(\mathbb{F})$ and $i : \mathrm{SL}_n(\mathbb{F}) \to \mathrm{SL}_n(\mathbb{F})$ are smooth functions. ◇

8.2 ISOMETRY GROUPS OF FORMS

Our next family of examples arises as isometry groups of nonsingular bilinear or sesquilinear forms. Before discussing these, we establish some notation:

I_n is the n-by-n identity matrix.

For $p+q=n$, $I_{p,q}$ is the n-by-n matrix $\begin{bmatrix} I_p & 0 \\ 0 & -I_q \end{bmatrix}$.

For n even, $n=2m$, J_n is the n-by-n matrix $\begin{bmatrix} 0 & I_m \\ -I_m & 0 \end{bmatrix}$.

For a matrix $M=(c_{ij})$, we write $M=[m_1 \mid \cdots \mid m_n]$, so that m_i is the ith column of M, $m_i = \begin{bmatrix} c_{1i} \\ c_{2i} \\ \vdots \\ c_{ni} \end{bmatrix}$.

EXAMPLE 8.2.1. Let φ be a nonsingular symmetric bilinear form on a vector space V of dimension n over $\mathbb{F}$. We have two cases:

(1) $\mathbb{F}=\mathbb{R}$. Here, by Theorem 6.2.29, φ is isometric to $p[1] \perp q[-1]$ for uniquely determined integers p and q with $p+q=n$. The *orthogonal group*

$$\mathrm{O}_{p,q}(\mathbb{R}) = \left\{M \in \mathrm{GL}_n(\mathbb{R}) \mid {}^tMI_{p,q}M = I_{p,q}\right\}.$$

In particular if $p=n$ and $q=0$ we have

$$\mathrm{O}_n(\mathbb{R}) = \mathrm{O}_{n,0}(\mathbb{R}) = \left\{M \in \mathrm{GL}_n(\mathbb{R}) \mid {}^tM = M^{-1}\right\}.$$

(2) $\mathbb{F}=\mathbb{C}$. In this case, by Corollary 6.2.27, φ is isometric to $n[1]$. The *orthogonal group*

$$\mathrm{O}_n(\mathbb{C}) = \left\{M \in \mathrm{GL}_n(\mathbb{C}) \mid {}^tM = M^{-1}\right\}.$$

(The term "the orthogonal group" is often used to mean $\mathrm{O}_n(\mathbb{R})$. Compare Definition 7.3.12.)

Let $G=\mathrm{O}_{p,q}(\mathbb{R})$, $\mathrm{O}_n(\mathbb{R})$, or $\mathrm{O}_n(\mathbb{C})$. G is a Lie group of dimension $d_{\mathbb{F}}n(n-1)/2$. G has two components. Letting $SG = G \cap \mathrm{SL}_n(\mathbb{F})$, we obtain the *special orthogonal groups*. For $G=\mathrm{O}_n(\mathbb{R})$ or $\mathrm{O}_n(\mathbb{C})$, SG is the identity component of G, i.e., the component of G containing the identity matrix. If $G=\mathrm{O}_n(\mathbb{R})$ then G is compact. $\mathrm{O}_1(\mathbb{C}) = \mathrm{O}_1(\mathbb{R}) = \{\pm[1]\}$. If $G=\mathrm{O}_n(\mathbb{C})$ for $n>1$, or $G=\mathrm{O}_{p,q}(\mathbb{R})$ with $p \geq 1$ and $q \geq 1$, then G is not compact.

We first consider the case $G=\mathrm{O}_{p,q}(\mathbb{R})$, including $G=\mathrm{O}_{n,0}(\mathbb{R}) = \mathrm{O}_n(\mathbb{R})$. For vectors $v = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$ and $w = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$, let

$$\langle v, w \rangle = \sum_{i=1}^{p} a_i b_i - \sum_{i=p+1}^{n} a_i b_i.$$

Let $M = [m_1 \mid \cdots \mid m_n]$. Then $M \in G$ if and only if

$$\begin{aligned} f_{ii}(M) &= \langle m_i, m_i \rangle = 1 && \text{for } i = 1, \ldots, p \\ f_{ii}(M) &= \langle m_i, m_i \rangle = -1 && \text{for } i = p+1, \ldots, n \\ f_{ij}(M) &= \langle m_i, m_j \rangle = 0 && \text{for } 1 \leq i < j < n. \end{aligned}$$

Thus if we let $F : \mathrm{M}_n(\mathbb{R}) \to \mathbb{R}^N$, $N = n(n+1)/2$, by

$$F(M) = \big(f_{11}(M), f_{22}(M), \ldots, f_{nn}(M), f_{12}(M), \\ f_{13}(M), \ldots, f_{1n}(M), \ldots, f_{n-1,n}(M)\big)$$

then

$$G = F^{-1}(t_0) \quad \text{where } t_0 = (1, \ldots, -1, 0, \ldots, 0).$$

We claim that $M = I$ is a regular point of F. List the entries of M in the order $x_{11}, x_{22}, \ldots, x_{nn}, x_{12}, \ldots, x_{1n}, \ldots, x_{n-1,n}, x_{21}, \ldots, x_{n1}, \ldots, x_{n,n-1}$. Computation shows that $F'(I)$, the matrix of the derivative of F evaluated at $M = I$, which is an N-by-n^2 matrix, has its leftmost N-by-N submatrix a diagonal matrix with diagonal entries ± 2 or ± 1. Thus $F'(I)$ has rank N, and I is a regular point of F. Hence, by the inverse function theorem, there is an open neighborhood $B(I)$ of I in $\mathrm{M}_n(\mathbb{R})$ such that $F^{-1}(t_0) \cap B(I)$ is a smooth submanifold of $B(I)$ of codimension N, i.e., of dimension $N^2 - n = n(n-1)/2$. But for any fixed $M_0 \in \mathrm{GL}_n(\mathbb{R})$, multiplication by M_0 is an invertible linear map, and hence a diffeomorphism, from $M_n(\mathbb{R})$ to itself. Thus we know that $M_0(F^{-1}(t_0) \cap B(I))$ is a smooth submanifold of $M_0 B(I)$, which is an open neighborhood of M_0 in $\mathrm{M}_n(\mathbb{R})$. But, since G is a group, $M_0 F^{-1}(t_0) = M_0 G = G = F^{-1}(t_0)$. Hence we see that G is a smooth manifold. Again we apply the implicit function theorem to see that the group operations on G are smooth maps.

Finally, we observe that any $M = (c_{ij})$ in $\mathrm{O}_n(\mathbb{R})$ has $|c_{ij}| \leq 1$ for every i, j, so $\mathrm{O}_n(\mathbb{R})$ is a closed and bounded, and hence compact, subspace of $\mathbb{R}^{n^2}$. On the other hand, the group $\mathrm{O}_{1,1}(\mathbb{R})$ contains the matrices $\begin{bmatrix} \sqrt{x^2+1} & x \\ x & \sqrt{x^2+1} \end{bmatrix}$ for any $x \in \mathbb{R}$, so it is an unbounded subset of $\mathbb{R}^{n^2}$ and hence it is not compact, and similarly for $\mathrm{O}_{p,q}(\mathbb{R})$ with $p \geq 1$ and $q \geq 1$.

A very similar argument applies in case $G = \mathrm{O}_n(\mathbb{C})$. We let

$$f_{ij}(M) = \mathrm{Re}\left(\langle m_i, m_j \rangle\right) \quad \text{and} \quad g_{ij}(M) = \mathrm{Im}\left(\langle m_i, m_j \rangle\right)$$

where $\mathrm{Re}(\cdot)$ and $\mathrm{Im}(\cdot)$ denote real and imaginary parts respectively. We then let $F : \mathrm{M}_n(\mathbb{C}) \to \mathbb{R}^{2N}$ by

$$F(M) = \big(f_{11}(M), g_{11}(M), f_{22}(M), g_{22}(M), \ldots\big),$$

and we identify $\mathrm{M}_n(\mathbb{C})$ with $\mathbb{R}^{2n^2}$ by identifying the entry $z_{ij} = x_{ij} + iy_{ij}$ of M with the pair (x_{ij}, y_{ij}) of real numbers. Then

$$G = F^{-1}(t_0) \quad \text{where } t_0 = (1, 0, 1, 0, \dots, 1, 0, 0, \dots, 0).$$

Again we show that $M = I$ is a regular point of F, and the rest of the argument is the same, showing that G is a smooth manifold of dimension $2N - 2n^2 = n(n-1)$, and that the group operations are smooth. Also, $\mathrm{O}_2(\mathbb{C})$ contains the matrices $\begin{bmatrix} i\sqrt{x^2-1} & -x \\ x & i\sqrt{x^2-1} \end{bmatrix}$ for any $x \in \mathbb{R}$, so it is not compact, and similarly for $\mathrm{O}_n(\mathbb{C})$ for $n \geq 2$. $\Diamond$

Example 8.2.2. Let φ be a nonsingular Hermitian form on a vector space V of dimension n over $\mathbb{C}$. Then, by Theorem 6.2.29, φ is isometric to $p[1] \perp q[-1]$ for uniquely determined integers p and q with $p + q = n$. The *unitary group*

$$\mathrm{U}_{p,q}(\mathbb{C}) = \left\{ M \in \mathrm{GL}_n(\mathbb{C}) \mid {}^t M I_{p,q} \overline{M} = I_{p,q} \right\}.$$

In particular if $p = n$ and $q = 0$ we have

$$\mathrm{U}_n(\mathbb{C}) = \left\{ M \in \mathrm{GL}_n(\mathbb{C}) \mid {}^t\overline{M} = M^{-1} \right\}.$$

(The term "the unitary group" is often used to mean $\mathrm{U}_n(\mathbb{C})$. Compare Definition 7.3.12.)

Let $G = \mathrm{U}_n(\mathbb{C})$ or $\mathrm{U}_{p,q}(\mathbb{C})$. G is a Lie group of dimension n^2. G is connected. If $G = \mathrm{U}_n(\mathbb{C})$ then G is compact. If $G = \mathrm{U}_{p,q}(\mathbb{C})$ with $p \geq 1$ and $q \geq 1$, then G is not compact. Letting $SG = G \cap \mathrm{SL}_n(\mathbb{R})$, we obtain the *special unitary groups*, which are closed connected subgroups of G of codimension 1.

The argument here is very similar to the argument in the last example. For vectors $v = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$ and $w = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$ we let

$$\langle v, w \rangle = \sum_{i=1}^{p} a_i \overline{b}_i - \sum_{i=p+1}^{n} a_i \overline{b}_i.$$

Let $M = [m_1 \mid \cdots \mid m_n]$. Then $M \in G$ if and only if

$$\begin{aligned} \langle m_i, m_i \rangle &= 1 && \text{for } i = 1, \dots, p \\ \langle m_i, m_i \rangle &= -1 && \text{for } i = p+1, \dots, n \\ \langle m_i, m_j \rangle &= 0 && \text{for } 1 \leq i < j < n. \end{aligned}$$

Let $f_{ii}(M) = \langle m_i, m_i\rangle$, which is always real valued. For $i \neq j$, let $f_{ij}(M) = \mathrm{Re}(\langle m_i, m_j\rangle)$ and $g_{ij} = \mathrm{Im}(\langle m_i, m_j\rangle)$.

Set $N = n + 2(n(n-1)/2) = n^2$. Let $F = \mathrm{M}_n(\mathbb{C}) \to \mathbb{R}^N$ by

$$F(M) = \big(f_{11}(M), \ldots, f_{nn}(M), f_{12}(M), g_{12}(M), \ldots\big).$$

Then

$$G = F^{-1}\big(t_0\big) \quad \text{where } t_0 = (1, \ldots, -1, 0, \ldots, 0).$$

Identify $\mathrm{M}_n(\mathbb{C})$ with $\mathbb{R}^{2n^2}$ as before. We again argue as before, showing that I is a regular point of F and then further that G is a smooth manifold of dimension $2n^2 - n^2 = n^2$, and in fact a Lie group. Also, a similar argument shows that $\mathrm{U}_n(\mathbb{C})$ is compact but that $\mathrm{U}_{p,q}(\mathbb{C})$ is not compact for $p \geq 1$ and $q \geq 1$. $\diamond$

EXAMPLE 8.2.3. Let φ be a nonsingular skew-symmetric form on a vector space V of dimension n over $\mathbb{F}$. Then, by Theorem 6.2.40, φ is isometric to $\left[\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right]$. The *symplectic group*

$$\mathrm{Sp}(n, \mathbb{F}) = \big\{M \in \mathrm{GL}_n(\mathbb{F}) \mid {}^t M J_n M = J_n\big\}.$$

Let $G = \mathrm{Sp}(n, \mathbb{R})$ or $\mathrm{Sp}(n, \mathbb{C})$. G is connected and noncompact. G is a Lie group of dimension $d_{\mathbb{F}}(n(n+1)/2)$. We also have the *symplectic group*

$$\mathrm{Sp}(n) = \mathrm{Sp}(n, \mathbb{C}) \cap \mathrm{U}(n, \mathbb{C}).$$

$G = \mathrm{Sp}(n)$ is a closed subgroup of both $\mathrm{Sp}(n, \mathbb{C})$ and $\mathrm{U}(n, \mathbb{C})$, and is a connected compact Lie group of dimension $n(n+1)/2$. (The term "the symplectic group" is often used to mean $\mathrm{Sp}(n)$.)

We consider $G = \mathrm{Sp}_n(\mathbb{F})$ for $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$.

The argument is very similar. For $V = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$ and $w = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$, let

$$\langle v, w\rangle = \sum_{i=1}^{n/2} (a_i b_{i+n/2} - a_{i+n/2} b_i).$$

If $M = [m_1 \mid \cdots \mid m_n]$ then $M \in G$ if and only if

$$\begin{aligned} \big\langle m_i, m_{i+n/2}\big\rangle &= 1 \quad \text{for } i = 1, \ldots, n/2 \\ \big\langle m_i, m_j\big\rangle &= 0 \quad \text{for } 1 \leq i < j \leq n, \quad j \neq i + n/2. \end{aligned}$$

Let $f_{ij}(M) = \langle m_i, m_j \rangle$ for $i < j$. Set $N = n(n-1)/2$. Let $F : \mathrm{M}_n(\mathbb{F}) \to \mathbb{F}^N$ by

$$F(M) = \big(f_{12}(M), \ldots, f_{n-1,n}(M)\big).$$

Then

$$G = F^{-1}(t_0) \quad \text{where } t_0 = (0, \ldots, 1, \ldots).$$

Again we show that I is a regular point for F, and continue similarly, to obtain that G is a Lie group of dimension $d_{\mathbb{F}} n^2 - d_{\mathbb{F}} N = d_{\mathbb{F}}(n(n+1)/2)$. $\mathrm{Sp}_2(\mathbb{F})$ contains the matrices $\left[\begin{smallmatrix} x & 0 \\ 0 & 1/x \end{smallmatrix}\right]$ for any $x \neq 0 \in \mathbb{R}$, showing that $\mathrm{Sp}_n(\mathbb{F})$ is not compact for any n.

Finally, $\mathrm{Sp}_{(n)} = \mathrm{Sp}_n(\mathbb{C}) \cap \mathrm{U}(n, \mathbb{C})$ is a closed subspace of the compact space $\mathrm{U}(n, \mathbb{C})$, so is itself compact. We shall not prove that it is a Lie group nor compute its dimension, which is $(n^2 + n)/2$, here. $\diamond$

REMARK 8.2.4. A warning to the reader: Notation is not universally consistent and some authors index the symplectic groups by $n/2$ instead of n. $\diamond$

Finally, we have a structure theorem for $\mathrm{GL}_n(\mathbb{R})$ and $\mathrm{GL}_n(\mathbb{C})$. We defined $\mathcal{A}_N^+$, $\mathcal{N}_n(\mathbb{R})$ and $\mathcal{N}_n(\mathbb{C})$ in Definition 7.2.18, and these are obviously Lie groups.

Theorem 8.2.5. *The multiplication maps*

$$m : \mathrm{O}(n, \mathbb{R}) \times \mathcal{A}_n^+ \times \mathcal{N}_n(\mathbb{R}) \to \mathrm{GL}_n(\mathbb{R})$$

and

$$m : \mathrm{U}(n, \mathbb{C}) \times \mathcal{A}_n^+ \times \mathcal{N}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$$

given by $m(P, A, N) = PAN$ are diffeomorphisms.

Proof. The special case of Theorem 7.2.20 with $k = n$ gives that m is a homeomorphism, and it is routine to check that m and m^{-1} are both differentiable. $\square$

REMARK 8.2.6. We have adopted our approach here on two grounds: first, to use elementary arguments to the extent possible, and second, to illustrate and indeed emphasize the linear algebra aspects of Lie groups. But it is possible to derive the results of this chapter by using more theory and less computation. It was straightforward to prove that $\mathrm{GL}_n(\mathbb{R})$ and $\mathrm{GL}_n(\mathbb{C})$ are Lie groups. The fact that the other groups we considered are also Lie groups is a consequence of the theorem that any closed subgroup of a Lie group is a Lie group. But this theorem is a theorem of analysis and topology, not of linear algebra. $\diamond$

CHAPTER A

POLYNOMIALS

In this appendix we gather and prove some important facts about polynomials. We fix a field $\mathbb{F}$ and we let $R = \mathbb{F}[x]$ be the ring of polynomials in the variable x with coefficients in $\mathbb{F}$,

$$R = \{a_n x^n + \cdots + a_1 x + a_0 \mid a_i \in \mathbb{F},\ n \geq 0\}.$$

A.1 BASIC PROPERTIES

We define the degree of a nonzero polynomial to be the highest power of x that appears in the polynomial. More precisely:

DEFINITION A.1.1. Let $p(x) = a_n x^n + \cdots + a_0$ with $a_n \neq 0$. Then the *degree* $\deg p(x) = n$. $\diamond$

REMARK A.1.2. The degree of the 0 polynomial is not defined. A polynomial of degree 0 is a nonzero constant polynomial. $\diamond$

The basic tool in dealing with polynomials is the division algorithm.

Theorem A.1.3. *Let $f(x), g(x) \in R$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ (the quotient) and $r(x)$ (the remainder) such that $f(x) = g(x)q(x) + r(x)$, where $r(x) = 0$ or* $\deg r(x) < \deg g(x)$.

Proof. We first prove existence.

If $f(x) = 0$ we are done: choose $q(x) = 0$ and $r(x) = 0$. Otherwise, let $f(x)$ have degree m and $q(x)$ have degree n. We fix n and proceed by complete induction on m. If $m < n$ we are again done: choose $q(x) = 0$ and $r(x) = f(x)$.

Otherwise, let $g(x) = a_n x^n + \cdots + a_0$ and $f(x) = b_m x^m + \cdots + b_0$. If $q_0(x) = (b_m/a_n)x^{m-n}$, then $f(x) - g(x)q_0(x)$ has the coefficient of

x^m equal to zero. If $f(x) = g(x)q_0(x)$ then we are again done: choose $q(x) = q_0(x)$ and $r(x) = 0$. Otherwise, $f_1(x) = f(x) - g(x)q_0(x)$ is a nonzero polynomial of degree less than m. Thus by the inductive hypothesis there are polynomials $q_1(x)$ and $r_1(x)$ with $f_1(x) = g(x)q_1(x) + r_1(x)$ where $r_1(x) = 0$ or $\deg r_1(x) < \deg g(x)$. Then $f(x) = g(x)q_0(x) + f_1(x) = g(x)q_0(x)+g(x)q_1(x)+r_1(x) = g(x)q(x)+r(x)$ where $q(x) = q_0(x)+q_1(x)$ and $r(x) = r_1(x)$ is as required, so by induction we are done.

To prove uniqueness, suppose $f(x) = g(x)q_1(x) + r_1(x)$ and $f(x) = g(x)q_2(x) + r_2(x)$ with $r_1(x)$ and $r_2(x)$ satisfying the conditions of the theorem. Then $g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x)$. Comparing degrees shows $r_2(x) = r_1(x)$ and $q_2(x) = q_1(x)$. □

REMARK A.1.4. The algebraically well-informed reader will recognize the rest of this appendix as a special case of the theory of ideals in a Euclidean ring, but we will develop this theory from scratch for polynomial rings. ◇

DEFINITION A.1.5. A nonempty subset $\mathcal{J}$ of R is an ideal of R if it has the properties

(1) If $p_1(x) \in \mathcal{J}$ and $p_2(x) \in \mathcal{J}$, then $p_1(x) + p_2(x) \in \mathcal{J}$.

(2) If $p_1(x) \in \mathcal{J}$ and $q(x) \in R$, then $p_1(x)q(x) \in \mathcal{J}$. ◇

REMARK A.1.6. Note that $\mathcal{J} = \{0\}$ is an ideal, the *zero ideal*. Any other ideal (i.e., any ideal containing a nonzero element) is a *nonzero ideal*. ◇

EXAMPLE A.1.7. (1) Fix a polynomial $p_0(x)$ and let $\mathcal{J}$ be the subset of R consisting of all multiples of $p_0(x)$, $\mathcal{J} = \{p_0(x)q(x) \mid q(x) \in R\}$. It is easy to check that $\mathcal{J}$ is an ideal. An ideal of this form is called a *principal ideal* and $p_0(x)$ is called a *generator* of $\mathcal{J}$, or is said to *generate* $\mathcal{J}$.

(2) Let $\{p_1(x), p_2(x), \ldots\}$ be a (possibly infinite) set of polynomials in R and let $\mathcal{J} = \{\sum p_i(x)q_i(x) \mid \text{only finitely many } q_i(x) \neq 0\}$. It is easy to check that $\mathcal{J}$ is an ideal, and $\{p_1(x), p_2(x), \ldots\}$ is called a *generating set* for $\mathcal{J}$ (or is said to *generate* $\mathcal{J}$). ◇

A nonzero polynomial $p(x) = a_n x^n + \cdots + a_0$ is called *monic* if the coefficient of the highest power of x appearing in $p(x)$ is 1, i.e., if $a_n = 1$.

Lemma A.1.8. *Let $\mathcal{J}$ be a nonzero ideal of R. Then $\mathcal{J}$ contains a unique monic polynomial of lowest degree.*

Proof. The set $\{\deg p(x) \mid p(x) \in \mathcal{J},\ p(x) \neq 0\}$ is a nonempty set of nonnegative integers, so, by the well-ordering principle, it has a smallest element d. Let $\widetilde{p}_0(x)$ be a polynomial in $\mathcal{J}$ with $\deg \widetilde{p}_0(x) = d$. Thus

$\widetilde{p}_0(x)$ is a polynomial in $\mathcal{J}$ of lowest degree, which may or may not be monic. Write $\widetilde{p}_0(x) = \widetilde{a}_d x^d + \cdots + \widetilde{a}_0$. By the properties of an ideal, $p_0(x) = (1/\widetilde{a}_d)\widetilde{p}_0(x) = x^d + \cdots + (\widetilde{a}_0/\widetilde{a}_d) = x^d + \cdots + a_0$ is in $\mathcal{J}$. This gives existence. To show uniqueness, suppose we have a different monic polynomial $p_1(x)$ of degree d in $\mathcal{J}$, $p_1(x) = x^d + \cdots + b_0$. Then by the properties of an ideal $\widetilde{q}(x) = p_0(x) - p_1(x)$ is a nonzero polynomial of degree $e < d$ in $\mathcal{J}$, $\widetilde{q}(x) = \widetilde{c}_e x^e + \cdots + \widetilde{c}_0$. But then $q(x) = (1/\widetilde{c}_e)\widetilde{q}(x) = x^e + \cdots + (\widetilde{c}_0/\widetilde{c}_e)$ is a monic polynomial in $\mathcal{J}$ of degree $e < d$, contradicting the minimality of d. □

Theorem A.1.9. *Let $\mathcal{J}$ be any nonzero ideal of R. Then $\mathcal{J}$ is a principal ideal. More precisely, $\mathcal{J}$ is the principal ideal generated by $p_0(x)$, where $p_0(x)$ is the unique monic polynomial of lowest degree in $\mathcal{J}$.*

Proof. By Lemma A.1.8, there is such a polynomial $p_0(x)$. Let $\mathcal{J}_0$ be the principal ideal generated by $p_0(x)$. We show that $\mathcal{J}_0 = \mathcal{J}$.

First we claim that $\mathcal{J}_0 \subseteq \mathcal{J}$. This is immediate. For, by definition, $\mathcal{J}_0$ consists of polynomials of the form $p_0(x)q(x)$, and, by the properties of an ideal, every such polynomial is in $\mathcal{J}$.

Next we claim that $\mathcal{J} \subseteq \mathcal{J}_0$. Choose any polynomial $g(x) \in \mathcal{J}$. By Theorem A.1.3, we can write $g(x) = p_0(x)q(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg p_0(x)$. If $r(x) = 0$ we are done, as then $g(x) = p_0(x)q(x) \in \mathcal{J}_0$. Assume $r(x) \neq 0$. Then, by the properties of an ideal, $r(x) = g(x) - p_0(x)q(x) \in \mathcal{J}$. ($p_0(x) \in \mathcal{J}$ so $p_0(x)(-q(x)) \in \mathcal{J}$; then also $g(x) \in \mathcal{J}$ so $g(x) + p_0(x)(-q_0(x)) = r(x) \in \mathcal{J}$). Now $r(x)$ is a polynomial of some degree $e < d$, $r(x) = a_e x^e + \cdots + a_0$, so $(1/a_e)r(x) = x^e + \cdots + (a_0/a_e) \in \mathcal{J}$. But this is a monic polynomial of degree e, contradicting the minimality of d. □

We now have an important application of this theorem.

Definition A.1.10. Let $\{p_1(x), p_2(x), \ldots\}$ be a (possibly infinite) set of nonzero polynomials in R. Then a monic polynomial $d(x) \in R$ is a *greatest common divisor (*gcd*)* of $\{p_1(x), p_2(x), \ldots\}$ if it has the following properties

(1) $d(x)$ divides every $p_i(x)$.

(2) If $e(x)$ is any polynomial that divides every $p_i(x)$, then $e(x)$ divides $d(x)$. ◇

Theorem A.1.11. *Let $\{p_1(x), p_2(x), \ldots\}$ be a (possibly infinite) set of nonzero polynomials in R. Then $\{p_1(x), p_2(x), \ldots\}$ has a unique* gcd $d(x)$. *More precisely, $d(x)$ is the generator of the principal ideal*

$$\mathcal{J} = \{\sum p_i(x)q_i(x) \mid q_i(x) \in R \textit{ only finitely many nonzero}\}.$$

Proof. By Theorem A.1.9, there is unique generator $d(x)$ of this ideal. We must show it has the properties of a gcd.

Let $\mathcal{J}_0$ be the principal ideal generated by $d(x)$, so that $\mathcal{J}_0 = \mathcal{J}$.

(1) Consider any polynomial $p_i(x)$. Then $p_i(x) \in \mathcal{J}$, so $p_i(x) \in \mathcal{J}_0$. That means that $p_i(x) = d(x)q(x)$ for some $q(x)$, so $d(x)$ divides $p_i(x)$.

(2) Since $d(x) \in \mathcal{J}$, it can be written as $d(x) = \sum p_i(x)q_i(x)$ for some polynomials $\{q_i(x)\}$. Let $e(x)$ be any polynomial that divides every $p_i(x)$. Then it divides every product $p_i(x)q_i(x)$, and hence their sum $d(x)$.

Thus we have shown that $d(x)$ satisfies both properties of a gcd. It remains to show that it is unique. Suppose $d_1(x)$ is also a gcd. Since $d(x)$ is a gcd of $\{p_1(x), p_2(x), \ldots\}$, and $d_1(x)$ divides each of these polynomials, then $d_1(x)$ divides $d(x)$. Similarly, $d(x)$ divides $d_1(x)$. Thus $d(x)$ and $d_1(x)$ are a pair of monic polynomials each of which divides the other, so they are equal. □

We recall an important definition.

DEFINITION A.1.12. A field $\mathbb{F}$ is *algebraically closed* if every nonconstant polynomial $f(x)$ in $\mathbb{F}[x]$ has a root in $\mathbb{F}$, i.e., if for every nonconstant polynomial $f(x)$ in $\mathbb{F}[x]$ there is an element r of $\mathbb{F}$ with $f(r) = 0$. ◇

We have the following famous and important theorem, which we shall not prove.

Theorem A.1.13 (Fundamental Theorem of Algebra)**.** *The field $\mathbb{C}$ of complex numbers is algebraically closed.*

EXAMPLE A.1.14. Let $\mathbb{F}$ be an algebraically closed field and let $a \in \mathbb{F}$. Then $\mathcal{J} = \{p(x) \in R \mid p(a) = 0\}$ is an ideal. It is generated by the polynomial $x - a$. ◇

Here is one of the most important applications of the gcd.

Corollary A.1.15. *Let $\mathbb{F}$ be an algebraically closed field and let $\{p_1(x), \ldots, p_n(x)\}$ be a set of polynomials not having a common zero. Then there is a set of polynomials $\{q_1(x), \ldots, q_n(x)\}$ such that*

$$p_1(x)q_1(x) + \cdots + p_n(x)q_n(x) = 1.$$

Proof. Since $\{p_1(x), \ldots, p_n(x)\}$ have no common zero, they have no nonconstant polynomial as a common divisor. Hence their gcd is 1. The corollary then follows from Theorem A.1.11. □

DEFINITION A.1.16. A set of polynomials $\{p_1(x), p_2(x), \ldots\}$ is *relatively prime* if it has gcd 1. ◇

We often phrase this by saying the polynomials $p_1(x), p_2(x), \ldots$ are relatively prime.

REMARK A.1.17. Observe that $\{p_1(x), p_2(x), \ldots\}$ is relatively prime if and only if the polynomials $p_i(x)$ have no nonconstant common factor. ◇

Closely related to the greatest common divisor (gcd) is the least common multiple (lcm).

DEFINITION A.1.18. Let $\{p_1(x), p_2(x), \ldots\}$ be a set of polynomials. A monic polynomial $m(x)$ is a *least common multiple (*lcm*)* of $\{p_1(x), p_2(x), \ldots\}$ if it has the properties

(1) Every $p_i(x)$ divides $m(x)$.

(2) If $n(x)$ is any polynomial that is divisible by every $p_i(x)$, then $m(x)$ divides $n(x)$. ◇

Theorem A.1.19. *Let $\{p_1(x), \ldots, p_k(x)\}$ be any finite set of nonzero polynomials. Then $\{p_1(x), \ldots, p_k(x)\}$ has a unique lcm $m(x)$.*

Proof. Let $\mathcal{J} = \{\text{polynomials } n(x) \mid n(x) \text{ is divisible by every } p_i(x)\}$. It is easy to check that $\mathcal{J}$ is an ideal (verify the two properties of an ideal in Definition A.1.5). Also, $\mathcal{J}$ is nonzero, as it contains the product $p_1(x) \cdots p_k(x)$.

By Theorem A.1.9, $\mathcal{J}$ is generated by a monic polynomial $m(x)$. We claim $m(x)$ is the lcm of $\{p_1(x), \ldots, p_k(x)\}$. Certainly $m(x)$ is divisible by every $p_i(x)$, as $m(x)$ is in $\mathcal{J}$. Also, $m(x)$ divides every $n(x)$ in $\mathcal{J}$ because $\mathcal{J}$, as the principal ideal generated by $m(x)$, consists precisely of the multiples of $m(x)$. □

REMARK A.1.20. By the proof of Theorem A.1.19, $m(x)$ is the unique monic polynomial of smallest degree in $\mathcal{J}$. Thus the lcm of $\{p_1(x), \ldots, p_k(x)\}$ may alternately be described as the unique monic polynomial of lowest degree divisible by every $p_i(x)$. ◇

Lemma A.1.21. *Suppose $p(x)$ divides the product $q(x)r(x)$ and that $p(x)$ and $q(x)$ are relatively prime. Then $p(x)$ divides $r(x)$.*

Proof. Since $p(x)$ and $q(x)$ are relatively prime there are polynomials $f(x)$ and $g(x)$ with $p(x)f(x) + q(x)g(x) = 1$. Then

$$p(x)f(x)r(x) + q(x)g(x)r(x) = r(x).$$

Now $p(x)$ obviously divides the first term $p(x)f(x)r(x)$, and $p(x)$ also divides the second term as, by hypothesis $p(x)$ divides $q(x)r(x)$, so $p(x)$ divides their sum $r(x)$. □

Corollary A.1.22. *Suppose $p(x)$ and $q(x)$ are relatively prime. If $p(x)$ divides $r(x)$ and $q(x)$ divides $r(x)$, then $p(x)q(x)$ divides $r(x)$.*

Proof. Since $q(x)$ divides $r(x)$, we may write $r(x) = q(x)s(x)$ for some polynomial $s(x)$. Now $p(x)$ divides $r(x) = q(x)s(x)$ and $p(x)$ and $q(x)$ are relatively prime, so by Lemma A.1.21 we have that $p(x)$ divides $s(x)$, and hence we may write $s(x) = p(x)t(x)$ for some polynomial $t(x)$. Then $r(x) = q(x)s(x) = q(x)p(x)t(x)$ is obviously divisible by $p(x)q(x)$. □

Corollary A.1.23. *If $p(x)$ and $q(x)$ are relatively prime monic polynomials, then their* lcm *is the product $p(x)q(x)$.*

Proof. If their lcm is $m(x)$, then on the one hand $m(x)$ divides $p(x)q(x)$, by the definition of the lcm. On the other hand, since both $p(x)$ and $q(x)$ divide $m(x)$, then $p(x)q(x)$ divides $m(x)$, by Corollary A.1.22. Thus $p(x)q(x)$ and $m(x)$ are monic polynomials that divide each other, so they are equal. □

A.2 UNIQUE FACTORIZATION

The most important property that $R = \mathbb{F}[x]$ has is that it is a unique factorization domain.

In order to prove this we need to do some preliminary work.

DEFINITION A.2.1. (1) The *units* in $\mathbb{F}[x]$ are the nonzero constant polynomials.

(2) A nonzero nonunit polynomial $f(x)$ is *irreducible* if

$$f(x) = g(x)h(x) \quad \text{with} \quad g(x)h(x) \in \mathbb{F}(x)$$

implies that one of $g(x)$ and $h(x)$ is a unit.

(3) A nonzero nonunit polynomial $f(x)$ in $\mathbb{F}[x]$ is *prime* if whenever $f(x)$ divides a product $g(x)h(x)$ of two polynomials in $\mathbb{F}[x]$, it divides (at least) one of the factors $g(x)$ or $h(x)$.

(4) Two nonzero polynomials $f(x)$ and $g(x)$ in $\mathbb{F}[x]$ are *associates* if $f(x) = ug(x)$ for some unit u. $\Diamond$

Lemma A.2.2. *A polynomial $f(x)$ in $\mathbb{F}[x]$ is prime if and only if it is irreducible.*

Proof. First suppose $f(x)$ is prime, and let $f(x) = g(x)h(x)$. Certainly both $g(x)$ and $h(x)$ divide $f(x)$. By the definition of prime, $f(x)$ divides $g(x)$ or $h(x)$. If $f(x)$ divides $g(x)$, then $f(x)$ and $g(x)$ divide each other, and so have the same degree. Thus $h(x)$ is constant, and so is a unit. By the same argument, if $f(x)$ divides $h(x)$, then $g(x)$ is constant, and so a unit.

Suppose $f(x)$ is irreducible, and let $f(x)$ divide $g(x)h(x)$. To show that $f(x)$ is prime, we need to show that $f(x)$ divides one of the factors.

By Theorem A.1.11, $f(x)$ and $g(x)$ have a gcd $d(x)$. By definition, $d(x)$ divides both $f(x)$ and $g(x)$, so in particular $d(x)$ divides $f(x)$, $f(x) = d(x)e(x)$. But $f(x)$ is irreducible, so $d(x)$ or $e(x)$ is a unit. If $e(x) = u$ is a unit, then $f(x) = d(x)u$ so $d(x) = f(x)v$ where $uv = 1$. Then, since $d(x)$ divides $g(x)$, $f(x)$ also divides $g(x)$. On the other hand, if $d(x) = u$ is a unit, then $d(x) = 1$ as by definition, a gcd is always a monic polynomial. In other words, by Definition A.1.16, $f(x)$ and $g(x)$ are relatively prime. Then, by Lemma A.1.21, $f(x)$ divides $h(x)$. $\square$

Theorem A.2.3 (Unique factorization)**.** *Let $f(x) \in \mathbb{F}[x]$ be a nonzero polynomial. Then*

$$f(x) = ug_1(x) \cdots g_k(x)$$

for some unit u and some set $\{g_1(x), \ldots, g_k(x)\}$ of irreducible polynomials. Furthermore, if also

$$f(x) = vh_1(x) \cdots h_l(x)$$

for some unit v and some set $\{h_1(x), \ldots, h_l(x)\}$ of irreducible polynomials, then $l = k$ and, after possible reordering, $h_i(x)$ and $g_i(x)$ are associates for each $i = 1, \ldots, k$.

Proof. We prove this by complete induction on $n = \deg f(x)$. First we prove the existence of a factorization and then we prove its uniqueness.

For the proof of existence, we proceed by induction. If $n = 0$ then $f(x) = u$ is a unit and there is nothing further to prove. Suppose that we have existence for all polynomials of degree at most n and let $f(x)$ have degree $n + 1$. If $f(x)$ is irreducible, then $f(x) = f(x)$ is a factorization and there is nothing further to prove. Otherwise $f(x) = f_1(x)f_2(x)$ with $\deg f_1(x) \le n$ and $\deg f_2(x) \le n$. By the inductive hypothesis $f_1(x) = u_1 g_{1,1}(x)\cdots g_{1,s}(x)$ and $f_2(x) = u_2 g_{2,1}(x)\cdots g_{2,t}(x)$ so we have the factorization

$$f(x) = \big(u_1u_2\big)g_{1,1}(x)\cdots g_{1,s}(x)g_{2,1}(x)\cdots g_{2,t}(x),$$

and by induction we are done.

For the proof of uniqueness, we again proceed by induction. If $n = 0$ then $f(x) = u$ is a unit and again there is nothing to prove. ($f(x)$ cannot be divisible by any polynomial of positive degree.) Suppose that we have uniqueness for all polynomials of degree at most n and let $f(x)$ have degree $n+1$. Let $f(x) = ug_1(x)\cdots g_k(x) = vh_1(x)\cdots h_l(x)$. If $f(x)$ is irreducible, then by the definition of irreducibility these factorizations must be $f(x) = ug_1(x) = vh_1(x)$ and then $g_1(x)$ and $h_1(x)$ are associates of each other. If $f(x)$ is not irreducible, consider the factor $g_k(x)$. Now $g_k(x)$ divides $f(x)$, so it divides the product $vh_1(x)\cdots h_l(x) = (vh_1(x)\cdots h_{l-1}(x))h_l(x)$. Since $g_k(x)$ is irreducible, by Lemma A.2.2 it is prime, so $g_k(x)$ must divide one of these two factors. If $g_k(x)$ divides $h_l(x)$, then, since $h_l(x)$ is irreducible, we have $h_l(x) = g_k(x)w$ for some unit w, in which case $g_k(x)$ and $h_l(x)$ are associates. If not, then $g_k(x)$ divides the other factor $vh_1(x)\cdots h_{l-1} = (vh_1(x)\cdots h_{l-2}(x))h_{l-1}(x)$ and we may repeat the argument. Eventually we may find that $g_k(x)$ divides some $h_i(x)$, in which case $g_k(x)$ and $h_i(x)$ are associates. By reordering the factors, we may simply assume that $g_k(x)$ and $h_l(x)$ are associates, $h_l(x) = g_k(x)w$ for some unit w. Then $f(x) = ug_1(x)\cdots g_k(x) = vh_1(x)\cdots h_l(x) = (vw)h_1(x)\cdots h_{l-1}(x)g(x)$. Let $f_1(x) = f(x)/g(x)$. We see that

$$f_1(x) = ug_1(x)\cdots g_{k-1}(x) = (vw)h_1(x)\cdots h_{l-1}(x).$$

Now $\deg f_1(x) \le n$, so by the inductive hypothesis $k-1 = l-1$, i.e., $k = l$, and after reordering $g_i(x)$ and $h_i(x)$ are associates for $i = 1,\ldots,k-1$. We have already shown this is true for $i = k$ as well, so by induction we are done. □

There is an important special case of this theorem that is worth observing separately.

Corollary A.2.4. *Let $\mathbb{F}$ be algebraically closed and let $f(x)$ be a nonzero polynomial in $\mathbb{F}[x]$. Then $f(x)$ can be written uniquely as*

$$f(x) = u\big(x - r_1\big)\cdots\big(x - r_n\big)$$

with $u \neq 0$ and $r_1, \ldots, r_n$ elements of $\mathbb{F}$.

Proof. If $\mathbb{F}$ is algebraically closed, every irreducible polynomial is linear, of the form $g(x) = v(x-r)$, and then this result follows immediately from Theorem A.2.3. (This special case is easy to prove directly, by induction on the degree of $f(x)$. We leave the details to the reader.) □

REMARK A.2.5. By Theorem A.1.13, Corollary A.2.4 applies in particular when $\mathbb{F} = \mathbb{C}$. ◇

A.3 POLYNOMIALS AS EXPRESSIONS AND POLYNOMIALS AS FUNCTIONS

Let $p(x) \in \mathbb{F}[x]$ be a polynomial. There are two ways to regard $p(x)$: as an expression $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, and as a function $p(x) : \mathbb{F} \to \mathbb{F}$ by $c \mapsto p(c)$. We have at times, when dealing with the case $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$, conflated these two approaches. In this section we show there is no harm in doing so. We show that if $\mathbb{F}$ is an infinite field, then two polynomials are equal as expressions if and only if they are equal as functions.

Lemma A.3.1. *Let $p(x) \in \mathbb{F}[x]$ be a polynomial and let $c \in \mathbb{F}$. Then $p(x) = (x-c)q(x) + p(c)$ for some polynomial $q(x)$.*

Proof. By Theorem A.1.3, $p(x) = (x-c)q(x) + a$ for some $a \in \mathbb{F}$. Now substitute $x = c$ to obtain $a = p(c)$. □

Lemma A.3.2. *Let $p(x)$ be a nonzero polynomial of degree n. Then $p(x)$ has at most n roots, counting multiplicities, in $\mathbb{F}$. In particular, $p(x)$ has at most n distinct roots in $\mathbb{F}$.*

Proof. We proceed by induction on n. The lemma is clearly true for $n = 0$. Suppose it is true for all polynomials of degree n. Let $p(x)$ be a nonzero polynomial of degree $n+1$. If $p(x)$ does not have a root in $\mathbb{F}$, we are done. Otherwise let r be a root of $p(x)$. By Lemma A.3.1, $p(x) = (x-r)q(x)$, where $q(x)$ has degree n. By the inductive hypothesis, $q(x)$ has at most n roots in $\mathbb{F}$, so $p(x)$ has at most $n+1$ roots in $\mathbb{F}$, and by induction we are done. □

Corollary A.3.3. *Let $p(x)$ be a polynomial of degree at most n. If $p(x)$ has more than n roots, then $p(x) = 0$ (the 0 polynomial).*

Corollary A.3.4. *(1) Let $f(x)$ and $g(x)$ be polynomials of degree at most n. If $f(c) = g(c)$ for more than n values of c, then $f(x) = g(x)$.*

(2) Let $\mathbb{F}$ be an infinite field. If $f(x) = g(x)$ for every $x \in \mathbb{F}$, then $f(x) = g(x)$.

Proof. Apply Corollary A.3.3 to the polynomial $p(x) = f(x) - g(x)$. $\square$

REMARK A.3.5. Corollary A.3.4(2) is false if $\mathbb{F}$ is a finite field. For example, suppose that $\mathbb{F}$ has n elements $c_1, \ldots, c_n$. Then $f(x) = (x - c_1)(x - c_2) \cdots (x - c_n)$ has $f(c) = 0$ for every $c \in \mathbb{F}$, but $f(x) \neq 0$. $\diamond$

CHAPTER B

Modules over principal ideal domains

In this appendix, for the benefit of the more algebraically knowledgable reader, we show how to derive canonical forms for linear transformations quickly and easily from the basic structure theorems for modules over a principal ideal domain (PID).

B.1 Definitions and structure theorems

We begin by recalling the definition of a module.

DEFINITION B.1.1. Let R be a commutative ring. An R-*module* is a set M with a pair of operations satisfying the conditions of Definition 1.1.1 except that the scalars are assumed to be elements of the ring R. $\diamond$

One of the most basic differences between vector spaces (where the scalars are elements of a field) and modules (where they are elements of a ring) is the possibility that modules may have torsion.

DEFINITION B.1.2. Let M be an R-module. An element $m \neq 0$ of M is a *torsion* element if $rm = 0$ for some $r \in R$, $r \neq 0$. If m is any element of M its *annihilator ideal* $\mathrm{Ann}(m)$ is the ideal of R given by

$$\mathrm{Ann}(m) = \{r \in R \mid rm = 0\}.$$

(Thus $\mathrm{Ann}(0) = R$ and $m \neq 0$ is a torsion element of M if and only if $\mathrm{Ann}(m) \neq \{0\}$.)

If every nonzero element of M is a torsion element then M is a *torsion* R-module. $\diamond$

REMARK B.1.3. Here is a very special case: Let $M = R$ and regard M as an R-module. Then we have the dual module M^* defined analogously to Definition 1.6.1, and we can identify M^* with R as follows: Let $f \in M^*$, so $f : M \to R$. Then we let $f \mapsto f(1)$. (Otherwise said, any $f \in M^*$ is given by multiplication by some fixed element of R, $f(r) = r_0 r$, and then $f \mapsto r_0$.) For $s_0 \in R$ consider the principal ideal $J = s_0 R = \{s_0 r \mid r \in R\}$. Let $N = J$ and regard N as a submodule of M. Then

$$\operatorname{Ann}\left(s_0\right) = \operatorname{Ann}^*(N)$$

where $\operatorname{Ann}^*(N)$ is the annihilator as defined in Definition 1.6.10. $\diamond$

Here is the basic structure theorem. It appears in two forms.

Theorem B.1.4. *Let R be a principal ideal domain (PID). Let M be a finitely generated torsion R-module. Then there is an isomorphism*

$$M \cong M_1 \oplus \cdots \oplus M_k$$

where each M_i is a nonzero R-module generated by a single element w_i, and $\operatorname{Ann}(w_1) \subseteq \cdots \subseteq \operatorname{Ann}(w_k)$. *The integer k and the set of ideals* $\{\operatorname{Ann}(w_1), \ldots, \operatorname{Ann}(w_k)\}$ *are well-defined.*

Theorem B.1.5. *Let R be a principal ideal domain (PID). Let M be a finitely generated torsion R-module. Then there is an isomorphism*

$$M \cong N_1 \oplus \cdots \oplus N_l$$

where each N_i is a nonzero R-module generated by a single element x_i, and $\operatorname{Ann}(x_i) = p_i^{e_i} R$ *is the principal ideal of R generated by the element $p_i^{e_i}$, where $p_i \in R$ is a prime and e_i is a positive integer. The integer l and the set of ideals $\{p_1^{e_1} R, \ldots, p_l^{e_l} R\}$ are well-defined.*

REMARK B.1.6. In the notation of Theorem B.1.4, if $\operatorname{Ann}(w_i)$ is the principal ideal generated by the element r_i of R, the condition $\operatorname{Ann}(w_1) \subseteq \cdots \subseteq \operatorname{Ann}(w_k)$ is that r_i is divisible by r_{i+1} for each $i = 1, \ldots, k-1$. $\diamond$

B.2 DERIVATION OF CANONICAL FORMS

We now use Theorem B.1.4 to derive rational canonical form, and Theorem B.1.5 to derive Jordan canonical form.

We assume throughout that V is a finite-dimensional $\mathbb{F}$-vector space and that $\mathcal{T} : V \to V$ is a linear transformation.

We let R be the polynomial ring $R = \mathbb{F}[x]$ and recall that R is a *PID*. We regard V as an R-module by defining

$$p(x)(v) = p(T)(v) \quad \text{for any } p(x) \in R \text{ and any } v \in V.$$

Lemma B.2.1. *V is a finitely generated torsion R-module.*

Proof. V is a finite-dimensional $\mathbb{F}$-vector space, so it has a finite basis $\mathcal{B} = \{v_1, \ldots, v_n\}$. Then the finite set $\mathcal{B}$ generates V as an $\mathbb{F}$-vector space, so certainly generates V as an R-module.

To prove that $v \neq 0$ is a torsion element, we need to show that $p(T)(v) = 0$ for some nonzero polynomial $p(x) \in R$. We proved this, for every $v \in V$, in the course of proving Theorem 5.1.1 (or, in matrix terms, Lemma 4.1.18). $\square$

To continue, observe that $\mathrm{Ann}(v)$, as defined in Definition B.1.2, is the principal ideal of R generated by the monic polynomial $m_{\mathcal{T},v}(x)$ of Theorem 5.1.1, and we called this polynomial the $\mathcal{T}$-annihilator of v in Definition 5.1.2.

We also observe that a subspace W of V is an R-submodule of V if and only if it is $\mathcal{T}$-invariant.

Theorem B.2.2 (Rational canonical form)**.** *Let V be a finite-dimensional vector space and let $\mathcal{T} : V \to V$ be a linear transformation. Then V has a basis $\mathcal{B}$ such that $[\mathcal{T}]_{\mathcal{B}} = M$ is in rational canonical form. Furthermore, M is unique.*

Proof. We have simply restated (verbatim) Theorem 5.5.4(1). This is the matrix translation of Theorem 5.5.2 about the existence of rational canonical $\mathcal{T}$-generating sets. Examining the definition of a rational canonical $\mathcal{T}$-generating set in Definition 5.5.1, we see that the elements $\{w_i\}$ of that definition are exactly the elements $\{w_i\}$ of Theorem B.1.4, and the ideals $\mathrm{Ann}(w_i)$ are the principal ideals of R generated by the polynomials $m_{\mathcal{T},w_i}(x)$. $\square$

Corollary B.2.3. *In the notation of Theorem B.1.4, let $f_i(x) = m_{\mathcal{T},w_i}(x)$. Then*

(1) The minimum polynomial $m_{\mathcal{T}}(x) = f_1(x)$.

(2) The characteristic polynomial $c_{\mathcal{T}}(x) = f_1(x) \cdots f_k(x)$.

(3) $m_{\mathcal{T}}(x)$ divides $c_{\mathcal{T}}(x)$.

(4) $m_{\mathcal{T}}(x)$ and $c_{\mathcal{T}}(x)$ have the same irreducible factors.

(5) (Cayley-Hamilton Theorem) $c_{\mathcal{T}}(\mathcal{T}) = 0$.

Proof. For parts (1) and (2), see Corollary 5.5.6. Parts (3) and (4) are then immediate. For (5), $m_{\mathcal{T}}(\mathcal{T}) = 0$ and $m_{\mathcal{T}}(x)$ divides $c_{\mathcal{T}}(x)$, so $c_{\mathcal{T}}(\mathcal{T}) = 0$. □

REMARK B.2.4. We have restated this result here for convenience, but the full strength of Theorem B.2.2 is not necessary to obtain parts (2), (4), and (5) of Corollary B.2.3—see Theorem 5.3.1 and Corollary 5.3.4. ◇

Theorem B.2.5 (Jordan canonical form)**.** *Let $\mathbb{F}$ be an algebraically closed field and let V be a finite-dimensional $\mathbb{F}$-vector space. Let $\mathcal{T} : V \to V$ be a linear transformation. Then V has a basis $\mathcal{B}$ with $[\mathcal{T}]_{\mathcal{B}} = J$ a matrix in Jordan canonical form. J is unique up to the order of the blocks.*

Proof. We have simply restated (verbatim) Theorem 5.6.5(1). To prove this, apply Theorem B.1.5 to V to obtain a decomposition $V = N_1 \oplus \cdots \oplus N_l$ as R-modules, or, equivalently, a $\mathcal{T}$-invariant direct sum decomposition of V. Since $\mathbb{F}$ is algebraically closed, each prime in R is a linear polynomial. Now apply Lemma 5.6.1 and Corollary 5.6.2 to each submodule N_i. □

REMARK B.2.6. This proof goes through verbatim to establish Theorem 5.6.6, the existence and essential uniqueness of Jordan canonical form, under the weaker hypothesis that the characteristic polynomial $c_{\mathcal{T}}(x)$ factors into a product of linear factors. Also, replacing Lemma 5.6.1 by Lemma 5.6.8 and Corollary 5.6.2 by Corollary 5.6.10 gives Theorem 5.6.13, the existence and essential uniqueness of generalized Jordan canonical form. ◇

Bibliography

There are dozens, if not hundreds, of elementary linear algebra texts, and we leave it to the reader to choose her or his favorite. Other than that, we have:

[1] Kenneth M. Hoffman and Ray A. Kunze, *Linear Algebra*, second edition, Prentice Hall, 1971.

[2] Paul R. Halmos, *Finite Dimensional Vector Spaces*, second edition, Springer-Verlag, 1987.

[3] William A. Adkins and Steven H. Weintraub, *Algebra: An Approach via Module Theory*, Springer-Verlag, 1999.

[4] Steven H. Weintraub, *Jordan Canonical Form: Theory and Practice*, Morgan and Claypool, 2009.

[1] is an introductory text that is on a distinctly higher level than most, and is highly recommended.

[2] is a text by a recognized master of mathematical exposition, and has become a classic.

[3] is a book on a higher level than this one, that proves the structure theorems for modules over a PID and uses them to obtain canonical forms for linear transformations (compare the approach in Appendix B).

[4] is a short book devoted entirely to Jordan canonical form. The proof there is a bit more elementary, avoiding use of properties of polynomials. While the algorithm for finding a Jordan basis and the Jordan canonical form of a linear transformation is more or less canonical, our exposition of it here follows the exposition in [4]. In particular, the eigenstructure picture (ESP) of a linear transformation was first introduced there.

Index

About the Author

Steven H. Weintraub is Professor of Mathematics at Lehigh University. He was born in New York, received his undergraduate and graduate degrees from Princeton University, and was on the permanent faculty at Louisiana State University for many years before moving to Lehigh in 2001. He has had visiting appointments at UCLA, Rutgers, Yale, Oxford, Göttingen, Bayreuth, and Hannover, and has lectured at universities and conferences around the world. He is the author of over 50 research papers, and this is his ninth book.

Prof. Weintraub has served on the Executive Committee of the Eastern Pennsylvania-Delaware section of the MAA, and has extensive service with the AMS, including currently serving as the Associate Secretary for the AMS Eastern Section.