TEXTBOOKS in MATHEMATICS

ADVANCED LINEAR ALGEBRA

Second Edition

Bruce N. Cooperstein

CRC Press
Taylor & Francis Group
A CHAPMAN & HALL BOOK

ADVANCED LINEAR ALGEBRA

Second Edition

This page intentionally left blank

TEXTBOOKS in MATHEMATICS

ADVANCED LINEAR ALGEBRA

Second Edition

Bruce N. Cooperstein

University of California
Santa Cruz, USA

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group an **informa** business
A CHAPMAN & HALL BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20150316

International Standard Book Number-13: 978-1-4822-4885-2 (eBook - PDF)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

This is dedicated to all the ...steins in my life:
Saul, Ezra, Tessa, Laser, Marci, and Rebecca

This page intentionally left blank

Contents

This page intentionally left blank

Preface to the Second Edition

The main differences between this edition and the first (apart from the correction of numerous typos) is the addition of a substantial amount of material, including four wholly new chapters. As a consequence, through the choice of various subsets of the chapters, this book can be appropriate for a single upper-division or graduate course in linear algebra, or an upper-division or graduate sequence. Furthermore, this book can function as a supplementary text for a graduate course on classical groups. As with the first edition, the approach remains general (nearly everything is done over arbitrary fields) and structural. We have also attempted to continue to build up to significant results from a few simple ideas. Following is a description of how the new edition specifically differs from its predecessor.

The first nine chapters of the edition have been carried over to the new edition with very few substantive changes. The most obvious is renumbering: A chapter has been inserted between Chapters 8 and 9 so that Chapter 9 has now become Chapter 10. Apart from the addition of several new exercises across these chapters, the most significant changes are:

Chapter 5 has been renamed "Normed and Inner Product Spaces" since we have added a section at the end of the chapter on "normed vector spaces". Here we introduce several norms that are not induced by an inner product such as the l_p-norm for $p \geq 1$ and the l_∞-norm. We show that all norms on a finite-dimensional real or complex space are equivalent, which implies that they induce the same topology.

In Chapter 8 we have added a section on orthogonal spaces over perfect fields of characteristic two and we prove Witt's theorem for such spaces.

In Chapter 10 (previously 9), the fourth section on symmetric and exterior algebras has been split into two separate sections. Additionally, we have added a section on Clifford algebras, which is a powerful tool for studying the structure of orthogonal spaces.

The new chapters are as follows:

Chapter 8 is devoted to sesquilinear forms, which generalize the notion of a multilinear form. In the first section we introduce the basic concepts, including the notion of a reflexive sesquilinear form and obtain a characterization: such forms are equivalent to Hermitian or skew-Hermitian forms. In the second section we define what is meant by a *unitary space*, an isometry of a unitary space, and prove Witt's theorem for non-degenerate unitary spaces.

Chapter 11 deals with linear groups and groups of isometries. In the first section we define the special linear group as well as the concept of a transvection. We prove that the special linear group is generated by transvections. We determine the center of the special linear group and prove that, with three small exceptions, the special linear group is perfect. We then show that when the special linear group is perfect, the quotient group by its center is a simple group. The second section is concerned with the symplectic group, the group of isometries of a non-degenerate symplectic space. Section three investigates the group of isometries of a non-degenerate singular orthogonal space over a field of characteristic not two. The final section is devoted to the group of isometries of a non-denerate isotropic unitary space.

Chapter 12 is devoted to some additional topics in linear algebra (more specifically, matrices). In the first section we introduce the notion of a matrix or operator norm and develop many of its properties. Section two is concerned with the Penrose–Moore pseudoinverse, which is a generalization of the notion of an inverse of a square matrix. The subsequent section takes on the subject of non-negative square matrices, real $n \times n$ matrices, all of whose entries are non-negative. Section four is devoted to the location of eigenvalues of a complex matrix. The main result is the Geršgorin disc theorem. The final section deals with functions of square matrices defined by polynomials and power series.

The final chapter deals with three important applications of linear algebra. Section one is devoted to the method of least squares, which can be used to estimate the parameters of a model to a set of observed data points. In the second section we introduce coding theory that is ubiquitous and embedded in all the digital devices we now take for granted. In our final section we discuss how linear algebra is used to define a page rank algorithm that might be applied in a web search engine.

Writing this new edition, while time-consuming, has nonetheless been a pleasure, particularly the opportunity to write about the classical groups (a research interest of mine) as well as important applications of linear algebra. That pleasure will be heightened if the reader gets as much out of reading the text as I have by writing it.

Bruce Cooperstein
September 2014
Santa Cruz, California

Preface to the First Edition

My own initial exposure to linear algebra was as a first-year student at Queens College of the City University of New York more than four decades ago, and I have been in love with the subject ever since. I still recall the excitement I felt when I could prove on the final exam that if A is an $n \times n$ matrix then there exists a polynomial $f(x)$ such that $f(A) = \mathbf{0}_{nn}$. It is only fitting that this result plays a major role in the first half of this book.

This book started out as notes for a one quarter second course in linear algebra at the University of California, Santa Cruz. Taken primarily by our most sophisticated and successful juniors and seniors, the purpose of this course was viewed as preparing these students for the continued study of mathematics. This dictated the pedagogical approach of the book as well as the choice of material.

The pedagogical approach is both structural and general: Linear algebra is about vector spaces and the maps between them that preserve their structure (linear transformations). Whenever a result is independent of the choice of an underlying field, it is proved in full generality rather than specifically for the real or complex field.

Though the approach is structural and general, which will be new to many students at this level, it is undertaken gradually, starting with familiar concepts and building slowly from simpler to deeper results. For example, the whole structure theory of a linear operator on a finite dimensional vector space is developed from a collection of some very simple results: mainly properties of the division of polynomials familiar to a sophisticated high school student as well as the fact that in a vector space of dimension n any sequence of more than n vectors is linearly dependent (the Exchange Theorem).

The material you will find here is at the core of linear algebra and what a beginning graduate student would be expected to know when taking her first course in group or field theory or functional analysis:

In Chapter 1, we introduce the main object of the course: vector spaces over fields as well as the fundamental concepts of linear combination, span of vectors, linear independence, basis, and dimension. We also introduce the concept of a coordinate vector with respect to a basis, which allows us to relate an abstract n dimensional vector space to the concrete space $\mathbb{F}^n$, where $\mathbb{F}$ is a field.

In almost every mathematical field, after introducing the basic object of study, one quickly moves on to the maps between these objects that preserve their structure. In linear algebra, the appropriate functions are linear transformations, and Chapter 2 is devoted to their introduction.

Over the field of rational, real, or complex numbers most of the material of Chapters 1 and 2 will be familiar but we begin to add sophistication and gravitate more towards the structural approach at the end of Chapter 2 by developing the *algebra* of the space $\mathcal{L}(V, W)$ of linear transformations, where V and W are finite-dimensional vector spaces. In particular, we introduce the notion of an algebra over a field and demonstrate that the space $\mathcal{L}(V, V)$ of linear operators on a finite-dimensional vector space V is an algebra with identity.

Chapter 3 is devoted to the algebra of polynomials with coefficients in a field, especially concentrating on those results that are consequences of the division algorithm, which should be familiar to students as "division of polynomials with remainder."

In Chapter 4, we comprehensively uncover the structure of a single linear operator on a finite-dimensional vector space. Students who have had a first course in abstract algebra may find some similarity in both the content and methods that they encountered in the study of cyclic and finite Abelian groups. As an outgrowth of our structure theory for operators, we obtain the various canonical forms for matrices.

Chapter 5 introduces inner product spaces, and in Chapter 6, we study operators on inner product spaces. Thus, in Chapter 5, after defining the notion of an inner product space, we prove that every such space has an orthonormal basis and give the standard algorithm for obtaining one starting from a given basis (the Gram-Schmidt process). Making use of the notion of the dual of a vector space, we define the adjoint of a linear transformation from one inner product space to another. In Chapter 6, we introduce the concepts of normal and self-adjoint operators on an inner product space and obtain characterizations. By exploiting the relationship between operators and matrices, we obtain the important result that any symmetric matrix can be diagonalized via an orthogonal matrix.

This is followed by a chapter devoted to the trace and determinant of linear operators and square matrices. More specifically, we independently define these concepts for operators and matrices with the ultimate goal to prove that if T is an operator, and A any matrix which represents T (with respect to some basis) then $Tr(T) = Trace(A)$ and $det(T) = det(A)$. We go on to prove the co-factor formula for the determinant of a matrix, a result missing from most treatments (and often taken as the ***definition*** of the determinant of a matrix). The chapter concludes with a section in which we show how we can interpret the determinant as an alternating n-multilinear form on an n dimensional vector space and we prove that it is unique.

The final two chapters consist of elective material at the undergraduate level, but it is hoped that the inclusion of these subjects makes this book an ideal choice for a one-term graduate course dedicated to linear algebra over fields (and taught independent of the theory of modules over principal ideal domains). The first of these two chapters is on bilinear forms, and the latter on tensor products and related material. More specifically, in Chapter 8, we classify nondegenerate reflexive forms and show that they are either alternating or symmetric. Subsequently, in separate sections, we study symplectic space (a vector space equipped with a non-degenerate alternating form) and orthogonal space (a vector space equipped with a nonsingular quadratic form). The final section of the chapter classifies quadratic forms defined on a real finite-dimensional vector space.

The ultimate chapter introduces the notion of universal mapping problems, defines the tensor product of spaces as the solution to such a problem and explicitly gives a construction. The second section explores the functorial properties of the tensor product. There is then a section devoted to the construction of the tensor algebra. In the final section we construct the symmetric and exterior algebras.

Hopefully the reader will find the material accessible, engaging, and useful. Much of my own mathematical research has involved objects built out of subspaces of vector spaces (Grassmannians, for example) so I have a very high regard and appreciation for both the beauty and utility of linear algebra. If I have succeeded with this book, then its student readers will be on a path to the same recognition.

Bruce Cooperstein
University of California, Santa Cruz
December 2009

This page intentionally left blank

Acknowledgments

My first thanks goes to all the students in my advanced linear algebra and graduate linear algebra classes over the past five years. They have patiently used this text and worked to get the most out of it despite the presence of errors. Lecturing on this material is a joy and my students have been the inspiration for this text. I am also indebted to my wife, Rebecca, and my nine-year-old daughter, Tessa, for their patience and encouragement while I spent the last six months focused on my writing and was often physically present but mentally unavailable. I must thank my institution, the University of California, Santa Cruz, and its mathematics department, which facilitated this project by granting me a sabbatical leave for Spring 2014, during which much of this text was written. Finally, my eternal gratitude to my friend and colleague, Professor Emeritus Arthur Wayman, from California State University, Long Beach, who volunteered to put a fresh pair of eyes to the manuscript and aid me in the hunt for typos as well as any problems with the exposition. Art found many embarrassing errors which have since been corrected and offered numerous worthwhile editorial suggestions. To the extent that the text is free of errors and the pedagogy clear, much credit is due Art. On the other hand, if there are any continuing deficiencies, the fault is all mine.

This page intentionally left blank

List of Figures

This page intentionally left blank

Symbol Description

$\mathbb{N}$	The set of natural numbers
$\mathbb{Q}$	The field of rational numbers
$\mathbb{R}$	The field of real numbers
$\mathbb{C}$	The field of complex numbers
$\mathbb{F}[x]$	The algebra of polynomials in a variable x with coefficients in the field $\mathbb{F}$
$\mathbb{F}_{(n)}[x]$	The space of all polynomials of degree at most n with entries in the field $\mathbb{F}$
$D(f)$	The derived polynomial of the polynomial f
$\mathbb{F}_{p^n}$	The finite field of cardinality p^n for a prime p and a natural number n
$\overline{c}$	The conjugate of a complex number c
$\mathbb{F}^n$	The vector space of n-tuples with entries in the field $\mathbb{F}$
$spt(f)$	The set of x such that $f(x) \neq 0$
$A\sharp B$	The concatenation of two finite sequences A and B
$U + W$	The sum of two subspaces U and W of a vector space
$U \oplus W$	The direct sum of two vector spaces U and W
$M_{mn}(\mathbb{F})$	The space of all $m \times n$ matrices with entries in the field $\mathbb{F}$
$D_n(\mathbb{F})$	The space of all diagonal $n \times n$ matrices with entries in the field $\mathbb{F}$
$U_n(\mathbb{F})$	The space of all lower triangular $n \times n$ matrices with entries in the field $\mathbb{F}$
$V = U_1 \oplus \cdots \oplus U_k$	The vector space V is the internal direct sum of subspaces $U_1, \ldots, U_k$
$\oplus_{i \in I} U_i$	The external direct sum of the collection of vector spaces $\{U_i \mid i \in I\}$
$\boldsymbol{u} \equiv \boldsymbol{v} \pmod{W}$	The vector $\boldsymbol{u}$ is congruent to the vector $\boldsymbol{w}$ modulo the subgroup W
V/W	The quotient space of the space V by the subspace W
$Span(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$	The span of a sequence $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$

	of vectors from a vector space
E_{ij}^{mn}	The $m \times n$ matrix, which has a single non-zero entry occurring in the (i, j)-position
$\mathcal{M}(X, \mathbb{F})$	The space of all functions from the set X to the field $\mathbb{F}$
$\mathcal{M}_{fin}(X, \mathbb{F})$	The space of all functions from the set X to the field $\mathbb{F}$, which have finite support
$dim(V)$	The dimension of a vector space V
$[\boldsymbol{v}]_{\mathcal{B}}$	The coordinate vector of a vector $\boldsymbol{v}$ with respect to a basis $\mathcal{B}$
$Proj_{(X,Y)}$	The projection map with respect to the direct sum decomposition $X \oplus Y$
$Range(T)$	The range of a transformation T
$Ker(T)$	The kernel of the linear transformation T
$\mathcal{L}(V, W)$	The space of all linear transformations from the vector space V to the vector space W
I_X	The identity map on the set X
$\dim(V)$	The dimension of the vector space V
$\mathcal{M}_T(\mathcal{B}_V, \mathcal{B}_W)$	The matrix of the linear transformation $T : V \to W$ with respect to the bases $\mathcal{B}_V$ of V and $\mathcal{B}_W$ of W
$S \circ R$	The composition of the functions R and S
$C_A(a)$	The centralizer of the element a the algebra $\mathbb{A}$
T^{-1}	The inverse of an invertible function T
$GL(V)$	The general linear group of V consisting of the invertible operators on the vector space V
$\mathcal{M}_{I_V}(\mathcal{B}, \mathcal{B}')$	The change of basis matrix from $\mathcal{B}$ to $\mathcal{B}'$
$gcd(f, g)$	The greatest common divisor of the polynomials $f(x)$ and $g(x)$
$Ann(T, \boldsymbol{v})$	The order ideal of the vector $\boldsymbol{v}$ with respect to the operator T
$\mu_{T,\boldsymbol{v}}(x)$	The minimal polynomial of the operator T with respect to the vector $\boldsymbol{v}$
$\langle T, \boldsymbol{v} \rangle$	The T-cyclic subspace generated by the vector $\boldsymbol{v}$
$Ann(T, V)$	The annihilator ideal of the operator T on the vector space V
$\mu_T(x)$	The minimal polynomial of the operator T
$\chi_T(x)$	The characteristic polynomial of the operator T
$C(f(x))$	The companion

	matrix of the polynomial $f(x)$
$J_m(p(x))$	The generalized Jordan m-block centered at the companion matrix $C(p(x))$ of the irreducible polynomial $p(x)$
$J_m(\lambda)$	The Jordan m-block centered at the element λ of the underlying field $\mathbb{F}$
$\boldsymbol{v} \cdot \boldsymbol{w}$	The dot product of real n-vectors $\boldsymbol{v}$ and $\boldsymbol{w}$
$Trace(A)$	The trace of the square matrix A
A^{tr}	The transpose of the matrix A
$\boldsymbol{u} \perp \boldsymbol{v}$	The vectors $\boldsymbol{u}$ and $\boldsymbol{v}$ of an inner product space are orthogonal
$\boldsymbol{u}^{\perp}$	The orthogonal complement to the vector $\boldsymbol{u}$ of an inner product space
$\parallel \boldsymbol{u} \parallel$	The norm of the vector $\boldsymbol{u}$ of an inner product space.
$W^{\perp}$	The orthogonal complement to a subspace W of an inner product space
$Proj_W(\boldsymbol{v})$	The orthogonal projection of the vector $\boldsymbol{v}$ onto the subspace W of an inner product space
$Proj_{W^{\perp}}(\boldsymbol{v})$	The projection of $\boldsymbol{v}$ orthogonal to W in an inner product space
V'	The dual space of the vector space V
T'	The transpose of a linear transformation
T^*	The adjoint of an linear transformation T between inner product spaces
$\sqrt{T}$	The semi-positive square root of a semi-positive operator T on an inner product space
$Tr(T)$	The trace of an operator T
$det(T)$	The determinant of an operator T on a vector space
$det(A)$	The determinant of the square matrix A
$sgn(\sigma)$	The sign of a permutation σ
$D_k(c)$	The diagonal type elementary matrix obtained from the identity matrix by multiplying the k^{th} row by c
P_{ij}	The elementary matrix obtained from the identity matrix by exchanging the i^{th} and j^{th} rows
$T_{ij}(c)$	The elementary matrix obtained from the identity matrix by adding c times the i^{th} row to the j^{th} row
$B(V, W; X)$	The space of all bi-

	linear maps from $V \times W$ to X
$B(V^2; X)$	The space of all bilinear maps from $V^2 = V \times V$ to X
$\mathcal{M}_f(\mathcal{B}_V, \mathcal{B}_W)$	The matrix of the bilinear form f on $V \times W$ with respect to the bases $\mathcal{B}_V$ of V and $\mathcal{B}_W$ of W
$Rad_L(f)$	The left radical of a bilinear form f
$Rad_R(f)$	The right radical of a bilnear form f
$\boldsymbol{u} \perp_f \boldsymbol{v}$	The vector $\boldsymbol{u}$ is orthogonal to the vector $\boldsymbol{w}$ with respect to the bilinear form f
$\rho_{\boldsymbol{x}}$	The reflection in the non-singular vector $\boldsymbol{x}$ in an orthogonal space
$V \otimes W$	The tensor product of vector spaces V and W
$\boldsymbol{v} \otimes \boldsymbol{w}$	The tensor product of the vectors $\boldsymbol{v}$ and $\boldsymbol{w}$
$S \otimes R$	The tensor product of linear transformations S and R
$A \otimes B$	The Kronecker or tensor product of matrices A and B
$\mathcal{T}_k(V)$	The k-fold tensor product of the vector space V
$\mathcal{T}(V)$	The tensor algebra of the vector space V
$\mathbb{F}\{x, y\}$	The polynomial algebra in two non-commuting variables x, y over the field $\mathbb{F}$
$\mathcal{T}(S)$	The tensor algebra homomorphism induced by the linear transformation S
$Sym_k(V)$	The k-fold symmetric product of the vector space V
$Sym(V)$	The symmetric algebra of the vector space V
$\wedge(V)$	The exterior algebra of the vector space V
$\wedge^k(V)$	The k^{th} exterior product of the vector space V
$\boldsymbol{v}_1 \wedge \cdots \wedge \boldsymbol{v}_k$	The exterior product of vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$
$\wedge^k(S)$	The k^{th} exterior product of linear transformation S
$\wedge(S)$	The exterior algebra homomorphism induced by a linear transformation S
$\lVert \cdot \rVert_1$	The l_1 norm of $\mathbb{R}^n$ or $\mathbb{C}^n$
$\lVert \cdot \rVert_p$	The l_p norm of $\mathbb{R}^n$ or $\mathbb{C}^n$
$\lVert \cdot \rVert_2$	The l_1 norm of $\mathbb{R}^n$ or $\mathbb{C}^n$
$\lVert \cdot \rVert_\infty$	The l_∞ norm of $\mathbb{R}^n$ or $\mathbb{C}^n$
$\lVert \cdot \rVert_{p,q}$	The matrix norm induced by the l_p and l_q norms of $\mathbb{R}^n$ or $\mathbb{C}^n$
$\lVert \cdot \rVert_F$	The Frobenius matrix norm
$R_i'(A)$	The deleted row

	sum of a square complex matrix A
$C'_i(A)$	The deleted column sum of a square complex matrix A
$\Gamma_i(A)$	The i^{th} Geršgorin row disc of the square couple matrix A
$\Delta_j(A)$	The j^{th} Geršgorin column disc of the square couplex matrix A
$\chi(P, H)$	The group of transvections with center P and axis H
$\chi(P)$	The group of all transvections with center P

This page intentionally left blank

1

Vector Spaces

CONTENTS

The most basic object in linear algebra is that of a vector space. Vector spaces arise in nearly every possible mathematical context and often in concrete ones as well. In this chapter, we develop the fundamental concepts necessary for describing and characterizing vectors spaces. In the first section we define and enumerate the properties of fields. Examples of fields are the rational numbers, the real numbers, and the complex numbers. Basically, a field is determined by those properties necessary to solve all systems of linear equations. The second section is concerned with the space $\mathbb{F}^n$, where n is a natural number and $\mathbb{F}$ is any field. These spaces resemble the real vector space $\mathbb{R}^n$ and the complex space $\mathbb{C}^n$. In section three we introduce the abstract concept of a vector space, as well as subspace, and give several examples. The fourth section is devoted to the study of subspaces of a vector space V. Among other results we establish a criteria for a subset to be a subspace that substantially reduces the number of axioms which have to be demonstrated. In section five we introduce the concepts of linear independence and span. Section six deals with bases and dimension in finitely generated vector spaces. In section seven we prove that every vector space has a basis. In the final section we show, given a basis for an n-dimensional vector space V over a field $\mathbb{F}$, how to associate a vector in $\mathbb{F}^n$. This is used to translate questions of independence and spanning in V to the execution of standard algorithms in $\mathbb{F}^n$.

Throughout this chapter it is essential that you have a good grasp of the concepts introduced in elementary linear algebra. Two good sources of review are ([1]) and ([17]).

1.1 Fields

While a primary motivation for this book is the study of finite dimensional real and complex vector spaces, many of the results apply to vector spaces over an arbitrary field. When possible we will strive for the greatest generality, which means proving our results for vector spaces over an arbitrary field. This has important mathematical applications, for example, to finite group theory and error correcting codes. In this short section, we review the notion of a ***field***. Basically, a field is an algebraic system in which every linear equation in a single variable can be solved. We begin with the definition.

Definition 1.1 *A* **field** *is a set* $\mathbb{F}$ *that contains two special and distinct elements 0 and 1. It is equipped with an operation* $+ : \mathbb{F}\times\mathbb{F} \to \mathbb{F}$ *called* **addition***, which takes a pair* a, b *in* $\mathbb{F}$ *to an element* $a + b$ *in* $\mathbb{F}$*. It also has an operation* $\cdot : \mathbb{F}\times\mathbb{F} \to \mathbb{F}$ *called* **multiplication***, which takes a pair* a, b *in* $\mathbb{F}$ *to an element* $a \cdot b$*. Additionally,* $(\mathbb{F}, 0, 1, +, \cdot)$ *must satisfy the following axioms:*

(A1) For every pair of elements a, b *from* $\mathbb{F}, a + b = b + a$*.*

(A2) For every triple of elements $a, b, c \in \mathbb{F}, a + (b + c) = (a + b) + c$*.*

(A3) For every element $a \in \mathbb{F}, a + 0 = a$*.*

(A4) For every element a *in* $\mathbb{F}$ *there is an element* b *such that* $a + b = 0$*.*

(M1) For every pair of elements a, b *in* $\mathbb{F}, a \cdot b = b \cdot a$*.*

(M2) For every triple of elements a, b, c *in* $\mathbb{F}, (a \cdot b) \cdot c = a \cdot (b \cdot c)$*.*

(M3) For every $a \in \mathbb{F}, a \cdot 1 = a$*.*

(M4) For every $a \in \mathbb{F}, a \neq 0$*, there is an element* c *such that* $a \cdot c = 1$*.*

(M5) For all elements a, b, c *from* $\mathbb{F}, a \cdot (b + c) = a \cdot b + a \cdot c$*.*

Axiom (A1) says that the operation of addition is ***commutative*** and (A2) that it is ***associative***. Axiom (A3) posits the existence of a special element that acts neutrally with respect to addition; it is called ***zero***. For an element $a \in \mathbb{F}$, the element b of axiom (A4) is called the ***negative*** of a and is usually denoted by $-a$. (M1) says that multiplication is **commutative** and (M2) that it is **associative**. (M3) asserts the existence of a ***multiplicative identity***. (M4) says that every element, apart from 0, has a ***multiplicative inverse***. Finally, (M5) says that ***multiplication distributes over addition***.

Example 1.1 *The set of* **rational numbers***,* $\mathbb{Q} = \{\frac{m}{n} | m, n \in \mathbb{Z}, n \neq 0\}$*, is a field.*

Example 1.2 *All numbers that are the root of some polynomial*

$$a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

where a_i are integers is a field, known as the **field of algebraic numbers**. *It contains $\sqrt{2}$, i (a root of X^2+1), as well as the roots of X^2+X+1. However, it does not contain π or e. We denote this field by $\mathbb{A}$.*

Example 1.3 *The set of* **real numbers**, $\mathbb{R}$, *consisting of all the numbers that have a decimal expansion, is a field. This includes all the rational numbers, as well as numbers such as $\sqrt{2}, \pi, e$ which do not belong to $\mathbb{Q}$.*

Example 1.4 *The set of* **complex numbers**, *denoted by* $\mathbb{C}$, *consists of all expressions of the form $a + bi$, where a, b are real numbers and i is a number such that $i^2 = -1$. These are added and multiplied in the following way: For $a, b, c, d \in \mathbb{R}$,*

$$(a + bi) + (c + di) = (a + c) + (b + d)i, \tag{1.1}$$

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i. \tag{1.2}$$

For a real number a we will identify the complex number $a + 0i$ with a in $\mathbb{R}$ and in this way we may assume the field of real numbers is contained in the field of complex numbers.

Example 1.5 *Denote by $\mathbb{Q}[i]$ the set of all numbers $r + si$ where $r, s \in \mathbb{Q}$ and $i^2 = -1$. With the addition given by Equation* (1.1) *and multiplication by Equation* (1.2). *This is a field.*

Example 1.6 *Denote by $\mathbb{Q}[\sqrt{2}]$ the set of all numbers $r+s\sqrt{2}$, where $r, s \in \mathbb{Q}$. The addition and multiplication are those inherited from $\mathbb{R}$.*

Definition 1.2 *When $\mathbb{E}$ and $\mathbb{F}$ are fields then we say that $\mathbb{E}$ is a subfield of $\mathbb{F}$, equivalently, that $\mathbb{F}$ is an extension of $\mathbb{E}$ if $\mathbb{E} \subset \mathbb{F}$, and the operations of $\mathbb{E}$ are those of* $\mathbf{F}$ *restricted to $\mathbb{E} \times \mathbb{E}$.*

Remark 1.1 *If $\mathbb{E}$ is a subfield of $\mathbb{F}$ and $\mathbb{F}$ is a subfield of $\mathbb{K}$, then $\mathbb{E}$ is a subfield of $\mathbb{K}$.*

Example 1.7 *The rational field* $\mathbb{Q}$ *is a subfield of* $\mathbb{R}$ *and also a subfield of* $\mathbb{A}$. *Also, the field* $\mathbb{Q}[i]$ *is a subfield of* $\mathbb{A}$. $\mathbb{Q}[\sqrt{2}]$ *is a subfield of* $\mathbb{R}$ *and of* $\mathbb{A}$.

Remark 1.2 *If* $\mathbb{F}$ *is a field and* $\mathbb{E}$ *is a nonempty subset of* $\mathbb{F}$, *in order to prove* $\mathbb{E}$ *is a subfield it suffices to show i) if* $a, b \in \mathbb{E}$ *then* $a - b, ab \in \mathbb{E}$; *and ii) if* $0 \neq a \in \mathbb{E}$ *then* $a^{-1} \in \mathbb{E}$. *That addition and multiplication in* $\mathbb{F}$ *are commutative and associative and that multiplication distributes over addition is immediate from the fact that these axioms hold in* $\mathbb{F}$.

All of the examples of fields have thus far been infinite, however, finite fields exist. In particular, for every prime p, there exists a field with p elements. More generally, for every prime power p^n, there exists a field with p^n elements, denoted by $\mathbb{F}_{p^n}$ or $GF(p^n)$. Vector spaces over finite fields have important applications, for example, in the construction of error correcting codes used for all forms of digital communication, including cellphones, CDs, DVDs, and transmissions from satellites to earth.

Example 1.8 A field with three elements

The underlying set of $\mathbb{F}_3$, *the field with three elements, is* $\{0, 1, 2\}$. *The addition and multiplication tables are shown below. We omit the element 0 in the multiplication table since 0 multiplied by any element of the field is 0.*

$\oplus_3$	*0*	*1*	*2*
0	*0*	*1*	*2*
1	*1*	*2*	*0*
2	*2*	*0*	*1*

$\otimes_3$	*1*	*2*
1	*1*	*2*
2	*2*	*1*

Properties of Complex Numbers

Because of the important role that the complex numbers play in the subsequent development, we discuss this particular field in more detail.

Definition 1.3 *For a complex number* $z = a + bi$ $(a, b \in \mathbb{R})$, *the* **norm** *of* z *is defined as* $\parallel z \parallel = \sqrt{a^2 + b^2}$.

The **conjugate** *of* $z = a + bi$ *is the complex number* $\overline{z} = a - bi$.

Theorem 1.1 *i) If z, w are complex numbers, then $\| zw \| = \| z \| \cdot \| w \|$.*

ii) If z is a complex number and c is a real number, then $\| cz \| = |c| \cdot \| z \|$.

iii) If $z = a + bi$ is a complex number with $a, b \in \mathbb{R}$, then $z\bar{z} = a^2 + b^2 = \| z \|^2$.

These are fairly straightforward, and we leave them as exercises.

For later application, we will require one more result about the complex numbers, this time asserting properties of the complex conjugate.

Theorem 1.2 *i) If z and w are complex numbers, then $\overline{z + w} = \bar{z} + \bar{w}$.*

ii) If z and w are complex numbers, then $\overline{zw} = \bar{z}\bar{w}$.

iii) Let z be a complex number and c a real number. Then $\overline{cz} = c\bar{z}$.

Proof *Parts i) and iii) are left as exercises. We prove ii). Let $z = a + bi, w = c + di$ with a, b, c, d real numbers. Then $zw = (ac - bd) + (ad + bc)i$ and $\overline{zw} = (ac - bd) - (ad + bc)i$.*

On the other hand, $\bar{z} = a - bi, \bar{w} = c - di$ and $\bar{z}\bar{w} = (a - bi)(c - di) = [ac - (-b)(-d)] + [(a)(-d) + (-b)(c)]i = (ac - bd) + [-ad - bc]i = (ac - bd) - (ad + bc)i$ and so $\overline{zw} = \bar{z}\bar{w}$ as claimed.

The field of complex numbers is especially interesting and important because it is ***algebraically closed***. This means that every non-constant polynomial $f(x)$ with complex coefficients can be factored completely into linear factors. This is equivalent to the statement that every non-constant polynomial $f(x)$ with complex coefficients has a complex root.

Example 1.9 *Determine the roots of the quadratic polynomial $x^2 + 6x + 11$.*

We can use the quadratic formula, which states that the roots of the quadratic polynomial $ax^2 + bx + c$ are $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

Applying the quadratic formula to $x^2 + 6x + 11$, we obtain the roots $\frac{-6 \pm \sqrt{36 - 44}}{2} = -3 \pm \sqrt{-2}$.

The negative square root $\sqrt{-2}$ can be expressed as a purely imaginary number: $\pm\sqrt{-2} = \pm\sqrt{2}\sqrt{-1} = \pm\sqrt{2}i$ since $i^2 = -1$ in the complex numbers. Therefore, the roots of the polynomial $x^2 + 6x + 11$ are

$$-3 + \sqrt{2}i, -3 - \sqrt{2}i.$$

Notice that the roots are complex conjugates. This is always true of a real quadratic polynomial which does not have real roots. In this case, the roots are a conjugate pair of complex numbers as can be seen from the quadratic formula.

Exercises

1. Prove i) of Theorem (1.1).

2. Prove ii) and iii) of Theorem (1.1).

3. Assume that $\mathbb{C}$ is a field. Verify that its subset $\mathbb{Q}[i]$ is a field.

4. Prove i) of Theorem (1.2).

5. Prove iii) of Theorem (1.2).

6. Let $\mathbb{F}_5$ have elements $\{0, 1, 2, 3, 4\}$ and assume that addition and multiplication are given by the following tables:

$\oplus_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\otimes_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

a) How can we immediately tell from these tables that the operations of addition and multiplication are commutative?

b) How can you conclude from the addition table that 0 is an additive identity?

c) How can we conclude from the addition table that every element has an additive inverse relative to 0?

d) How can we conclude from the multiplication table that 1 is a multiplicative identity?

e) How can we conclude from the multiplication table that every non-zero element has a multiplicative inverse relative to 1?

7. Making use of the multiplication table for the field $\mathbb{F}_5$ in Exercise 6, find the solution to the linear equation $3x + 2 = 4$, where the coefficients of this equation are considered to be elements of $\mathbb{F}_5$.

8. Find the solution in field of the complex numbers to the linear equation $2x - (1 + 2i) = -ix + (2 + 2i)$.

9. In Exercises 7 and 8, which properties of the field did you use?

1.2 The Space $\mathbb{F}^n$

What You Need to Know

To make sense of the material in this section, you should be familiar with the concept of a ***field*** as well as its basic properties, in particular, that addition and multiplication are commutative and associative, the distributive law holds, and so on.

We begin with a definition:

Definition 1.4 *Let n be a positive integer. By an n*-**vector** *with entries in a field $\mathbb{F}$, we will mean a single column of length n with entries in $\mathbb{F}$:* $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$.

The entries which appear in an n-vector are called its **components**.

Two n-vectors $\boldsymbol{a} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$ *and* $\boldsymbol{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$ *are* **equal** *if and only if $a_i = b_i$ for all $i = 1, 2, \ldots, n$ and then we write $\boldsymbol{a} = \boldsymbol{b}$.*

The collection of all n-vectors with entries in $\mathbb{F}$ is denoted by $\mathbb{F}^n$ and this is referred to as "F n-space."

Note that $\begin{pmatrix} 1 \\ 2 \end{pmatrix} \neq \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}$ since the former is a 2 vector and the latter a 3 vector and equality is only defined when they are both vectors of the same size.

The remainder of this short section is devoted primarily to the ***algebra*** of $\mathbb{F}^n$. We will define two operations called ***addition*** and ***scalar multiplication*** and make explicit some of the properties of these operations. We begin with the definition of addition.

Definition 1.5 *To add (find the sum of) two $\mathbb{F}^n$vectors $\boldsymbol{u}, \boldsymbol{v}$ simply add the corresponding components. The result is a vector in $\mathbb{F}^n$:*

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ \vdots \\ a_n + b_n \end{pmatrix}.$$

The second operation involves an element c of $\mathbb{F}$ (which we refer to as a ***scalar***) and an n-vector $\boldsymbol{u}$.

Definition 1.6 *The* **scalar multiplication** *of $c \in \mathbb{F}$ and $\boldsymbol{u} \in \mathbb{F}^n$ is defined by multiplying all the components of $\boldsymbol{u}$ by c. The result is a vector in $\mathbb{F}^n$. This is denoted by $c\boldsymbol{u}$.*

$$c \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} ca_1 \\ ca_2 \\ \vdots \\ ca_n \end{pmatrix}.$$

The particular vector $(-1)\boldsymbol{u}$ (where -1 is the element of $\mathbb{F}$ such that $(-1)+1=0$) is especially important. The vector $(-1)\boldsymbol{u}$ is called the **opposite** *or* **negative** *of $\boldsymbol{u}$. We will denote this by $-\boldsymbol{u}$. Further, as a convention, we will write $\boldsymbol{u}-\boldsymbol{v}$ for $\boldsymbol{u}+(-\boldsymbol{v})$.*

Also of importance is the vector whose components are all zero:

Definition 1.7 *The* **zero vector** *in $\mathbb{F}^n$ is the n-vector all of whose components are zero. We denote it by $\mathbf{0}_n$, or just $\mathbf{0}$ when the length n is clear from the context.*

Definition 1.8 *For a given n, we will denote by $\boldsymbol{e}_i^n$ the n-vector which has only one non-zero component, a one, which occurs in the i^{th} row. When the n is understood from the context, we will usually not use the superscript.*

Example 1.10 *As an example, in $\mathbb{F}^3$ we have*

$$\boldsymbol{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \boldsymbol{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \boldsymbol{e}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

When we fix n and consider the collection of n-vectors, $\mathbb{F}^n$, then the following properties hold. These are precisely the conditions for $\mathbb{F}^n$ to be a vector space, a concept that is the subject of the next section.

Theorem 1.3 Properties of vector addition and scalar multiplication

Let $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}$ be n-vectors with entries in the field $\mathbb{F}$ (that is, elements of $\mathbb{F}^n$) and b, c be scalars (elements of $\mathbb{F}$). Then the following properties hold.

i) $(\boldsymbol{u}+\boldsymbol{v})+\boldsymbol{w}=\boldsymbol{u}+(\boldsymbol{v}+\boldsymbol{w})$. *Associative law*
ii) $\boldsymbol{u}+\boldsymbol{v}=\boldsymbol{v}+\boldsymbol{u}$. *Commutative law*
iii) $\boldsymbol{u}+\mathbf{0}=\boldsymbol{u}$. *The zero vector is an additive identity*
iv) $\boldsymbol{u}+(-\boldsymbol{u})=\mathbf{0}$. *Existence of additive inverses*
v) $b(\boldsymbol{u}+\boldsymbol{v})=b\boldsymbol{u}+b\boldsymbol{v}$. *A distributive law of scalar multiplication over vector addition*
vi) $(b+c)\boldsymbol{u}=b\boldsymbol{u}+c\boldsymbol{u}$. *A distributive law*
vii) $(bc)\boldsymbol{u}=b(c\boldsymbol{u})$. *An associative law*
viii) $1\boldsymbol{u}=\boldsymbol{u}$.
ix) $0\boldsymbol{u}=\mathbf{0}$.

Proof *Throughout let* $\boldsymbol{u}=\begin{pmatrix}u_1\\u_2\\\vdots\\u_n\end{pmatrix}, \boldsymbol{v}=\begin{pmatrix}v_1\\v_2\\\vdots\\v_n\end{pmatrix}, \boldsymbol{w}=\begin{pmatrix}w_1\\w_2\\\vdots\\w_n\end{pmatrix}.$

i) Then

$$(\boldsymbol{u}+\boldsymbol{v})+\boldsymbol{w}=\begin{pmatrix}(u_1+v_1)+w_1\\(u_2+v_2)+w_2\\\vdots\\(u_n+v_n)+w_n\end{pmatrix}$$

and

$$\boldsymbol{u}+(\boldsymbol{v}+\boldsymbol{w})=\begin{pmatrix}u_1+(v_1+w_1)\\u_2+(v_2+w_2)\\\vdots\\u_n+(v_n+w_n)\end{pmatrix}.$$

Since the addition in a field satisfies $(u_i+v_i)+w_i=u_i+(v_i+w_i)$ for all i, it follows that these vectors are identical.

In a similar fashion, ii) holds since it reduces to showing that the components of $\boldsymbol{u}+\boldsymbol{v}$ and $\boldsymbol{v}+\boldsymbol{u}$ are equal. However, the i^{th} component of $\boldsymbol{u}+\boldsymbol{v}$ is u_i+v_i, whereas the i^{th} component of $\boldsymbol{v}+\boldsymbol{u}$ is v_i+u_i which are equal since the addition in $\mathbb{F}$ is commutative.

iii) This holds since we are adding 0 to each component of $\boldsymbol{u}$ and this leaves $\boldsymbol{u}$ unchanged.

iv). The i^{th} components of $\boldsymbol{u}+(-\boldsymbol{u})$ is $u_i+(-u_i)=0$ and therefore $\boldsymbol{u}+(-\boldsymbol{u})=\mathbf{0}$.

v) The i^{th} component of $b(\boldsymbol{u}+\boldsymbol{v})$ is $b(u_i+v_i)$, whereas the i^{th} component of $b\boldsymbol{u}+b\boldsymbol{v}$ is bu_i+bv_i, and these are equal since the distributive property holds in $\mathbb{F}$.

vi) The i^{th} component of $(b+c)\boldsymbol{u}$ is $(b+c)u_i$ and the i^{th} component of $b\boldsymbol{u}+c\boldsymbol{u}$ is bu_i+cu_i, which are equal, again, since the distributive property holds in $\mathbb{F}$.

vii) The i^{th} component of $(bc)\boldsymbol{u}$ is $(bc)u_i$. The i^{th} component of $b(c\boldsymbol{u})$ is $b(cu_i)$, and these are equal since multiplication in $\mathbb{F}$ is associative.

viii) Here, each component is multiplied by 1 and so is unchanged, and therefore $\boldsymbol{u}$ is unchanged.

ix) Each component of $\boldsymbol{u}$ is multiplied by 0 and so is 0. Consequently, $0\boldsymbol{u}=\mathbf{0}$.

Exercises

In Exercises 1–3, assume the vectors are in $\mathbb{C}^3$ and perform the indicated addition.

1. $\begin{pmatrix} 1 \\ i \\ 3+i \end{pmatrix} + \begin{pmatrix} -1+2i \\ -2+i \\ 1-3i \end{pmatrix}$ 2. $\begin{pmatrix} 1-i \\ 3+2i \\ -2+5i \end{pmatrix} + \begin{pmatrix} 1+i \\ 3-2i \\ -2-5i \end{pmatrix}$

3. $\begin{pmatrix} 2-3i \\ 2+i \\ 1+4i \end{pmatrix} + \begin{pmatrix} -2-3i \\ -2+i \\ -1+4i \end{pmatrix}$

In Exercises 4–6, assume the vectors are in $\mathbb{C}^3$ and compute the indicated scalar product.

4. $(1+i)\begin{pmatrix} 2+i \\ 1-i \\ i \end{pmatrix}$ 5. $i\begin{pmatrix} 2+3i \\ -1+2i \\ -i \end{pmatrix}$ 6. $(2-i)\begin{pmatrix} i \\ 1+i \\ 2+i \end{pmatrix}$

In Exercises 7 and 8, assume the vectors are in $\mathbb{F}_5^3$ and perform the given addition.

7. $\begin{pmatrix} 2 \\ 4 \\ 1 \end{pmatrix} + \begin{pmatrix} 3 \\ 1 \\ 4 \end{pmatrix}$ 8. $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + \begin{pmatrix} 3 \\ 4 \\ 3 \end{pmatrix}$

In Exercises 9 and 10, assume the vectors are in $\mathbb{F}_5^3$ and compute the scalar product.

9. $3\begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix}$ 10. $4\begin{pmatrix} 2 \\ 4 \\ 3 \end{pmatrix}$

11. Find all vectors $\boldsymbol{v} \in \mathbb{C}^2$ such that $(1+i)\boldsymbol{v} + \begin{pmatrix} 2-i \\ 1+2i \end{pmatrix} = \begin{pmatrix} 6+i \\ 3+6i \end{pmatrix}$.

12. Find all vectors $\boldsymbol{v}$ in $\mathbb{F}_5^2$ such that $2\boldsymbol{v} + \begin{pmatrix} 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$.

1.3 Vector Spaces over an Arbitrary Field

What You Need to Know

In this section it is essential that you have mastered the concept of a ***field*** and can recall its properties. You should also be familiar with the space $\mathbb{F}^n$, where $\mathbb{F}$ is a field.

We jump right in and begin with the definition of a vector space.

Definition 1.9 *Let* $\mathbb{F}$ *be a field and* V *a nonempty set equipped with maps* $\alpha : V \times V \to V$ *called* **addition** *and* $\mu : \mathbb{F} \times V \to V$ *called* **scalar multiplication***. We will denote* $\alpha(\boldsymbol{u}, \boldsymbol{v})$ *by* $\boldsymbol{u} + \boldsymbol{v}$ *and refer to this as the* **sum** *of* $\boldsymbol{u}$ *and* $\boldsymbol{v}$*. We denote* $\mu(c, \boldsymbol{u})$ *by* $c\boldsymbol{u}$ *and refer to this as the* **scalar multiple** *of* $\boldsymbol{u}$ *by* c*.* V *is said to be a* **vector space** *over* $\mathbb{F}$ *if the following axioms are all satisfied:*

(A1) $\boldsymbol{u} + \boldsymbol{v} = \boldsymbol{v} + \boldsymbol{u}$ *for every* $\boldsymbol{u}, \boldsymbol{v} \in V$*.* **Addition is commutative***.*

(A2) $\boldsymbol{u} + (\boldsymbol{v} + \boldsymbol{w}) = (\boldsymbol{u} + \boldsymbol{v}) + \boldsymbol{w}$ *for every* $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}$ *in* V*.* **Addition is associative***.*

(A3) There is a special element $\mathbf{0}$ *called the* **zero vector** *such that* $\boldsymbol{u} + \mathbf{0} = \boldsymbol{u}$ *for every* $\boldsymbol{u} \in V$*. This is the* **existence of an additive identity***.*

(A4) For every element $\boldsymbol{u}$ *in* V *there is an element, denoted by* $-\boldsymbol{u}$*, such that* $\boldsymbol{u} + (-\boldsymbol{u}) = \mathbf{0}$*. The symbol* $-\boldsymbol{u}$ *is referred to as the opposite or negative of* $\boldsymbol{u}$*. This is the* **existence of additive inverses***.*

(M1) $a(\boldsymbol{u} + \boldsymbol{v}) = a\boldsymbol{u} + a\boldsymbol{v}$ *for every scalar* a *and vectors* $\boldsymbol{u}, \boldsymbol{v} \in V$*.* **This is a distributive axiom of scalar multiplication over vector addition***.*

(M2) $(a + b)\boldsymbol{u} = a\boldsymbol{u} + b\boldsymbol{u}$ *for every vector* $\boldsymbol{u}$ *and every pair of scalars* a, b*.* **This is another distributive axiom.**

(M3) $(ab)\boldsymbol{u} = a(b\boldsymbol{u})$ *for every vector* $\boldsymbol{u}$ *and every pair of scalars* a, b*.* **This is an associative axiom.**

(M4) $1\boldsymbol{u} = \boldsymbol{u}$*.*

In a moment, we will prove some abstract results; however, for the time being, we enumerate a few examples.

Definition 1.10 *Denote by* $\mathbb{F}[x]$ *the collection of all polynomials in the variable* x *with coefficients in the field* $\mathbb{F}$*.*

Example 1.11 *The set* $\mathbb{F}[x]$ *with the usual addition of polynomials and multiplication by constants is a vector space over* $\mathbb{F}$*.*

Definition 1.11 *Let X and Y be sets. We will denote by $\mathcal{M}(X,Y)$ the collection of all maps (functions) from X to Y.*

Example 1.12 *Let X be a nonempty set and $\mathbb{F}$ a field. For two functions g, h in $\mathcal{M}(X,\mathbb{F})$ define addition by $(g+h)(x) = g(x) + h(x)$, that is, the pointwise addition of functions. Likewise scalar multiplication is given by $(cg)(x) = cg(x)$. In this way $\mathcal{M}(X,\mathbb{F})$ becomes a vector space with zero vector the function $\mathbf{O}_{X\to\mathbb{F}}$, which satisfies $\mathbf{O}_{X\to\mathbb{F}}(x) = 0$ for all $x \in X$.*

Example 1.13 *This example generalizes Example (1.12): Let V be a vector space over the field $\mathbb{F}$ and X a set. For two functions $f, g \in \mathcal{M}(X,V)$, define addition by $(f+g)(x) = f(x)+g(x)$. Define scalar multiplication by $(cf)(x) = cf(x)$, where $c \in \mathbb{F}, f \in \mathcal{M}(X,V)$, and $x \in X$. Then $\mathcal{M}(X,V)$ is a vector space over $\mathbb{F}$ with zero vector the function $\mathbf{O}_{X\to V} : X \to V$, which satisfies $\mathbf{O}_{X\to V}(x) = \mathbf{0}_V$ for all $x \in X$, where $\mathbf{0}_V$ is the zero vector of V.*

Example 1.14 *The set of all solutions of the differential equation $\frac{d^2y}{dx^2}+y=0$ is a real vector space. Since solutions to the equation are functions with codomain $\mathbb{R}$, we use the addition and scalar multiplication introduced in Example (1.12). Note solutions exist since, in particular, sin x, cos x satisfy this differential equation.*

Example 1.15 *Let U and W be vectors spaces over a field $\mathbb{F}$. Denote by $U \times W$ the Cartesian product of U and W, $U \times W = \{(\boldsymbol{u}, \boldsymbol{w}) : \boldsymbol{u} \in U, \boldsymbol{w} \in W\}$.*

Define addition on $U \times W$ by $(\boldsymbol{u}_1, \boldsymbol{w}_1) + (\boldsymbol{u}_2, \boldsymbol{w}_2) = (\boldsymbol{u}_1 + \boldsymbol{u}_2, \boldsymbol{w}_1 + \boldsymbol{w}_2)$. Define scalar multiplication on $U \times W$ by $c(\boldsymbol{u}, \boldsymbol{w}) = (c\boldsymbol{u}, c\boldsymbol{w})$.

Set $\mathbf{0}_{U\times W} = (\mathbf{0}_U, \mathbf{0}_W)$. This makes $U \times W$ into a vector space. This is referred to as the **external direct sum** *of U and W and denoted by $U \oplus W$.*

Example 1.16 *Let I be a set and for each $i \in I$ assume U_i is a vector space over the field $\mathbb{F}$ with zero element $\mathbf{0}_i$. Let $\prod_{i\in I} U_i$ consist of all maps f from I into $\cup_{i\in I} U_i$ such that $f(i) \in U_i$ for all i.*

For $f, g \in \prod_{i\in I} U_i$ define the sum by $(f+g)(i) = f(i)+g(i)$. For $f \in \prod_{i\in I} U_i$ and a scalar c, define the scalar product cf by $(cf)(i) = cf(i)$. Finally, let $\mathbf{O}$ be the map from I to $\cup_{i\in I} U_i$ such that $\mathbf{O}(i) = \mathbf{0}_i$ for every i.

Then $\prod_{i\in I} U_i$ is a vector space with $\mathbf{O}$ as zero vector. This space is referred to as the **direct product** *of the spaces $\{U_i | i \in I\}$.*

We now come to some basic results. It would not be very desirable if there were more than one zero vector or if some vectors had more than one opposite vector. While it might seem “obvious” that the zero vector and the opposite of a vector are unique, we do not take anything for granted and prove that, indeed, these are true statements.

Theorem 1.4 Some uniqueness properties in a vector space

Let V be a vector space. Then the following hold:

i) The element $\mathbf{0}$ in V is unique. By this we mean if an element $\boldsymbol{e}$ of V satisfies $\boldsymbol{u} + \boldsymbol{e} = \boldsymbol{e} + \boldsymbol{u} = \boldsymbol{u}$ for every vector $\boldsymbol{u}$ in V, then $\boldsymbol{e} = \mathbf{0}$.

ii) The opposite (negative) of a vector $\boldsymbol{u}$ is unique, that is, if $\boldsymbol{v}$ is a vector that satisfies $\boldsymbol{u} + \boldsymbol{v} = \boldsymbol{v} + \boldsymbol{u} = \mathbf{0}$, then $\boldsymbol{v} = -\boldsymbol{u}$.

Proof *i) Suppose that $\boldsymbol{u}+\boldsymbol{e} = \boldsymbol{e}+\boldsymbol{u} = \boldsymbol{u}$ for every $\boldsymbol{u}$ in V. We already know that $\boldsymbol{u} + \mathbf{0} = \mathbf{0} + \boldsymbol{u} = \boldsymbol{u}$ for every vector $\boldsymbol{u}$ in V. Consider the vector $\mathbf{0} + \boldsymbol{e}$. Plugging $\mathbf{0}$ into $\boldsymbol{u} + \boldsymbol{e} = \boldsymbol{e} + \boldsymbol{u} = \boldsymbol{u}$, we obtain that $\mathbf{0} + \boldsymbol{e} = \mathbf{0}$. On the other hand, plugging $\boldsymbol{e}$ into $\boldsymbol{u} + \mathbf{0} = \mathbf{0} + \boldsymbol{u} = \boldsymbol{u}$, we get $\mathbf{0} + \boldsymbol{e} = \boldsymbol{e}$. Thus, $\boldsymbol{e} = \mathbf{0}$.*

ii) Suppose $\boldsymbol{u} + \boldsymbol{v} = \boldsymbol{v} + \boldsymbol{u} = \mathbf{0}$. We know that $\boldsymbol{u} + (-\boldsymbol{u}) = (-\boldsymbol{u}) + \boldsymbol{u} = \mathbf{0}$. Consider $(-\boldsymbol{u}) + (\boldsymbol{u} + \boldsymbol{v})$. By the first equation we have $(-\boldsymbol{u}) + (\boldsymbol{u} + \boldsymbol{v}) = (-\boldsymbol{u}) + \mathbf{0} = -\boldsymbol{u}$. However, by associativity, we have $(-\boldsymbol{u}) + (\boldsymbol{u}+\boldsymbol{v}) = [(-\boldsymbol{u}) + \boldsymbol{u}] + \boldsymbol{v} = \mathbf{0} + \boldsymbol{v} = \boldsymbol{v}$. Therefore, $-\boldsymbol{u} = \boldsymbol{v}$.

We have shown that the zero vector and the opposite (negative) of a vector are unique. We now determine how these "behave" with respect to scalar multiplication, which is the purpose of the next result.

Theorem 1.5 *Let V be a vector space, $\boldsymbol{u}$ a vector in V, and c a scalar. Then the following hold:*

i) $0\boldsymbol{u} = \mathbf{0}$.

ii) $c\mathbf{0} = \mathbf{0}$.

iii) If $c\boldsymbol{u} = \mathbf{0}$, then either $c = 0$ or $\boldsymbol{u} = \mathbf{0}$.

iv) $(-c)\boldsymbol{u} = -(c\boldsymbol{u})$.

Proof *i) We use the fact that $0 = 0+0$ in $\mathbb{F}$ to get $0\boldsymbol{u} = (0+0)\boldsymbol{u} = 0\boldsymbol{u}+0\boldsymbol{u}$. Now add $-(0\boldsymbol{u})$ to both sides: $-0\boldsymbol{u}+0\boldsymbol{u} = -0\boldsymbol{u}+[0\boldsymbol{u}+0\boldsymbol{u}] = [-0\boldsymbol{u}+0\boldsymbol{u}]+0\boldsymbol{u}$, the last step by associativity. This give the equality $\mathbf{0} = \mathbf{0}+0\boldsymbol{u} = 0\boldsymbol{u}$ as desired.*

ii) and iii) are left as exercises.

iv) We make use of part i) and the fact that for any element c of $\mathbb{F}, 0 = c+(-c)$ to get $\mathbf{0} = 0\boldsymbol{u} = [c + (-c)]\boldsymbol{u} = c\boldsymbol{u} + (-c)\boldsymbol{u}$. Add $-c\boldsymbol{u}$ to both sides of the equality: $-c\boldsymbol{u} + \mathbf{0} = -c\boldsymbol{u} + [c\boldsymbol{u} + (-c)\boldsymbol{u}] = [-c\boldsymbol{u} + c\boldsymbol{u}] + (-c)\boldsymbol{u}$, the last step justified by associativity. This becomes $-c\boldsymbol{u} + \mathbf{0} = \mathbf{0} + (-c)\boldsymbol{u}$ and so $-c\boldsymbol{u} = (-c)\boldsymbol{u}$.

Exercises

1. Prove part ii) of Theorem (1.5).

2. Prove part iii) of Theorem (1.5).

3. Let $\boldsymbol{v}$ be an element of a vector space V. Prove that $-(-\boldsymbol{v}) = \boldsymbol{v}$.

4. Let V be a vector space. Prove the following cancellation property: for vectors $\boldsymbol{v}, \boldsymbol{x}, \boldsymbol{y}$, if $\boldsymbol{v} + \boldsymbol{x} = \boldsymbol{v} + \boldsymbol{y}$, then $\boldsymbol{x} = \boldsymbol{y}$.

5. Let V be a vector space. Prove the following cancellation property: Assume $c \neq 0$ is a scalar and $c\boldsymbol{x} = c\boldsymbol{y}$, then $\boldsymbol{x} = \boldsymbol{y}$.

6. Let X be a set and $\mathbb{F}$ a field. Prove that $\mathcal{M}(X, \mathbb{F})$ is a vector space with the operations as given in Example (1.12).

7. Let V be a vector space over the field $\mathbb{F}$ and X a set. Prove that $\mathcal{M}(X, V)$ with the operations defined in Example (1.13) is a vector space over $\mathbb{F}$.

8. Let U and W be vector spaces over the field $\mathbb{F}$. Prove that $U \oplus W$ defined in Example (1.15) is a vector space.

9. Let $\mathbb{F}$ be a field, I a set and for each $i \in I$ assume U_i a vector space over $\mathbb{F}$ with identity element $\mathbf{0}_i$. Prove that $\prod_{i \in I} U_i$ defined in Example (1.16) is a vector space over $\mathbb{F}$ with zero vector the function $\mathbf{O} : I \to \cup_{i \in I} U_i$ defined by $\mathbf{O}(i) = \mathbf{0}_i$.

10. In this exercise $\mathbb{F}_2 = \{0, 1\}$ denotes the field with two elements. Let X be a set and denote by $\mathcal{P}(X)$ the *power set* of X consisting of all subsets of X. Define an addition on $\mathcal{P}(X)$ by $U \ominus W = (U \cup W) \setminus (U \cap W)$. Define $0 \cdot U = \emptyset$ and $1 \cdot U = U$ for $U \in \mathcal{P}(X)$. Prove that $\mathcal{P}(X)$ with these operations is a vector space over $\mathbb{F}_2 = \{0, 1\}$ with $\emptyset$ the zero vector and the negative of a subset U of X is U.

11. Let $V = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} | a, b \in \mathbb{R}^+ \right\}$. Define "addition" on V by

$$\begin{pmatrix} a_1 \\ b_1 \end{pmatrix} + \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 \\ b_1 b_2 \end{pmatrix}.$$

Further, define "scalar multiplication" for $c \in \mathbb{R}$ by $c \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a^c \\ b^c \end{pmatrix}$.

Prove that V is a vector space over $\mathbb{R}$ where $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ is the zero vector and $-\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \frac{1}{a} \\ \frac{1}{b} \end{pmatrix}$.

1.4 Subspaces of Vector Spaces

In this section, we consider subsets W of a vector space V, which are themselves vector spaces when the addition and scalar multiplication operations of V are restricted to W. We establish a criteria for a subset to be a subspace, which substantially reduces the number of axioms that have to be demonstrated.

What You Need to Know

It is important that you have mastered the concept of a ***vector space***, in particular, all the axioms used to define it. You should know the properties of the zero vector and the negative (opposite) of a vector and be able to solve a system of linear equations with real coefficients either by applying elementary equation operations or using matrices (and Gaussian elimination).

We begin this section with an example.

Example 1.17 *Let $\mathbb{F}$ be a field, $V = \mathbb{F}^3$, and $W = \left\{ \begin{pmatrix} x \\ y \\ 0 \end{pmatrix} |x, y \in \mathbb{F} \right\}$. Notice that W is a nonempty subset of V. Moreover, note that the sum of two vectors from W is in W:*

$$\begin{pmatrix} x_1 \\ y_1 \\ 0 \end{pmatrix} + \begin{pmatrix} x_2 \\ y_2 \\ 0 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \\ 0 \end{pmatrix}.$$

In a similar fashion, if $c \in \mathbb{F}$ is a scalar and $\boldsymbol{w} \in W$, then $c\boldsymbol{w} \in W$.

Clearly, the zero vector of V is contained in W. Moreover, if $\boldsymbol{v} = \begin{pmatrix} x \\ y \\ 0 \end{pmatrix} \in W$, then $-\boldsymbol{v} = \begin{pmatrix} -x \\ -y \\ 0 \end{pmatrix} \in W$.

It is fairly straightforward to show that all the properties of a vector space hold for W, where the addition is the restriction of the addition of V to $W \times W$ and the scalar multiplication is the restriction of the scalar multiplication of V to $\mathbb{F} \times W$.

When W is a subset of a vector space V and the sum of any two vectors from W are also in W, we say that "W is closed under addition." When any scalar multiple of a vector in W is in W, we say, *W is closed under scalar multiplication.* Example (1.17) motivates the following definition:

Definition 1.12 Subspace of a vector space

A nonempty subset W of a vector space V is called a **subspace** *of V if W is itself a vector space under the addition and scalar multiplication inherited from V.*

The next result gives simple criteria for a subset to be a subspace.

Theorem 1.6 Characterization of subspaces of a vector space

A nonempty subset W of a vector space V is a subspace if and only if the following two properties hold:

i) For all $\boldsymbol{u}, \boldsymbol{v} \in W$, the sum $\boldsymbol{u} + \boldsymbol{v}$ is in W (W is closed under addition).

ii) For every vector $\boldsymbol{u}$ in W and scalar c, the vector $c\boldsymbol{u}$ is in W (W is closed under scalar multiplication).

Proof *Assume that W is a subspace. By the definition of addition in a vector space for $\boldsymbol{u}, \boldsymbol{v} \in W, \boldsymbol{u} + \boldsymbol{v}$ is an element in W. In a similar fashion, for $\boldsymbol{u}$ in W and scalar $c, c\boldsymbol{u} \in W$. Thus, W is closed under addition and scalar multiplication.*

Conversely, assume that W is nonempty (it has vectors) and that i) and ii) hold. The axioms (A1) and (A2) hold since they hold in V and the addition in W is the same as the addition in V. We next show that the zero element of V belongs to W. We do know that W is nonempty so let $\boldsymbol{u} \in W$. By ii), we know for any scalar c that also $c\boldsymbol{u} \in W$. In particular, $0\boldsymbol{u} \in W$. However, by part i) of Theorem (1.5), $0\boldsymbol{u} = \boldsymbol{0}$. Consequently, $\boldsymbol{0} \in W$. Since for all $\boldsymbol{v} \in V, \boldsymbol{0} + \boldsymbol{v} = \boldsymbol{v}$, it follows that this holds in W as well and (A3) is satisfied.

We also have to show that for any vector $\boldsymbol{u} \in W$, the opposite of $\boldsymbol{u}$ belongs to V. However, by ii) we know that $(-1)\boldsymbol{u} \in W$. By part iv) of Theorem (1.5), $(-1)\boldsymbol{u} = -\boldsymbol{u}$ as required. All the other axioms (M1)–(M4) hold because they do in V.

Definition 1.13 *Let $(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k)$ be a sequence of vectors in a vector space V and $c_1, c_2, \dots, c_k$ elements of $\mathbb{F}$. An expression of the form $c_1\boldsymbol{v}_1 + \cdots + c_k\boldsymbol{v}_k$ is called a* **linear combination** *of $(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k)$.*

The next theorem states that if W is a subspace of a vector space V and $(\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_k)$ is a sequence of vectors from W, then W contains all linear combinations of $(\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_k)$.

Theorem 1.7 *Let V be a vector space, W a subspace, and $(\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_k)$ a sequence of vectors from W. If $c_1, c_2, \dots, c_k$ are scalars, then the linear combination $c_1\boldsymbol{w}_1 + c_2\boldsymbol{w}_2 + \cdots + c_k\boldsymbol{w}_k \in W$.*

Proof *The proof is by induction on k. The case $k = 1$ is just the second part of Theorem (1.6). Suppose $k = 2$. We know by the second part of Theorem (1.6) that $c_1\boldsymbol{w}_1$ and $c_2\boldsymbol{w}_2 \in W$. Then by part i) of Theorem (1.6) $c_1\boldsymbol{w}_1 + c_2\boldsymbol{w}_2 \in W$.*

Now suppose the result is true for any sequence of k vectors $(\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_k)$ and scalars $(c_1, c_2, \dots, c_k)$ and suppose we are given a sequence of vectors $(\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_k, \boldsymbol{w}_{k+1})$ in W and scalars $(c_1, c_2, \dots, c_k, c_{k+1})$. By the inductive hypothesis, $\boldsymbol{v} = c_1\boldsymbol{w}_1 + c_2\boldsymbol{w}_2 + \dots + c_k\boldsymbol{w}_k \in W$. The vectors $\boldsymbol{v}$ and $\boldsymbol{w}_{k+1}$ are in W. Now the vector $c_1\boldsymbol{w}_1 + c_2\boldsymbol{w}_2 + \dots + c_k\boldsymbol{w}_k + c_{k+1}\boldsymbol{w}_{k+1} = 1\boldsymbol{v} + c_{k+1}\boldsymbol{w}_{k+1} \in W$ by the case for $k = 2$.

We now proceed to some examples of subspaces.

Example 1.18 *If V is a vector space then V and $\{\mathbf{0}\}$ are subspaces of V. These are referred to as* **trivial subspaces**. *The subspace $\{\mathbf{0}\}$ is called the* **zero subspace**. *Often we abuse notation and write $\mathbf{0}$ for $\{\mathbf{0}\}$.*

Example 1.19 *Let $\mathbb{F}_{(n)}[x] := \{f(x) \in \mathbb{F}[x] : deg(f) \leq n\}$. Then $\mathbb{F}_{(n)}[x]$ is a subspace of $\mathbb{F}[x]$. Two typical elements of $\mathbb{F}_{(n)}[x]$ are $a_0 + a_1x + \dots + a_nx^n, b_0 + b_1x + \dots + b_nx^n$. Their sum is $(a_0 + b_0) + (a_1 + b_1)x + \dots (a_n + b_n)x^n$, which is in $\mathbb{F}_{(n)}[x]$. Also, for a scalar c, $c(a_0 + a_1x + \dots + a_nx^n) = (ca_0) + (ca_1)x + \dots + (ca_n)x^n$, which is also in $\mathbb{F}_{(n)}[x]$.*

Example 1.20 *We denote by $C(\mathbb{R}, \mathbb{R})$ the collection of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$. This is a subspace of $\mathcal{M}(\mathbb{R}, \mathbb{R})$. This depends on the following facts proved (stated) in the first calculus class:*

The sum of two continuous functions is continuous.

A scalar multiple of a continuous function is continuous.

Example 1.21 *Let $\mathbb{F}$ be field and a an element of $\mathbb{F}$. Set $W = \{f(x) \in \mathbb{F}_{(n)}[x] : f(a) = 0\}$. Suppose that $f(x), g(x) \in W$ so that $f(a) = g(a) = 0$. By the definition of $(f+g)(x)$, it follows that $(f+g)(a) = f(a)+g(a) = 0+0 = 0$. So, W is closed under addition. On the other hand, suppose $f \in W$ and c is scalar. We need to show that $cf \in W$, which means we need to show that $(cf)(a) = 0$. However, $(cf)(a) = cf(a) = c0 = 0$.*

Definition 1.14 *Let X be a set and $\mathbb{F}$ a field. The* **support** *of a function $f \in \mathcal{M}(X, \mathbb{F})$ is denoted by $spt(f)$ and is defined to be $\{x \in X | f(x) \neq 0\}$. We will say that $f \in \mathcal{M}(X, \mathbb{F})$ has* **finite support** *if $spt(f)$ is a finite set. Otherwise, it has infinite support. We will denote by $\mathcal{M}_{fin}(X, \mathbb{F})$ the collection of all functions $f : X \to \mathbb{F}$, which have finite support.*

Example 1.22 *If X is a set and $\mathbb{F}$ a field, then $\mathcal{M}_{fin}(X,\mathbb{F})$ is a subspace of $\mathcal{M}(X,\mathbb{F})$.*

Definition 1.15 *Let $\mathbb{F}$ be a field, I a nonempty set, and for i in I, let U_i be a vector space over $\mathbb{F}$ with zero element $\mathbf{0}_i$. For $f \in \prod_{i\in I} U_i$ (see Example (1.16)) define the support of f, denoted by spt(f), to be the collection of those $i \in I$ such that $f(i) \neq \mathbf{0}_i$. We say that f has finite support if spt(f) is a finite set. Denote by $\oplus_{i\in I}U_i$ the set $\{f \in \prod_{i\in I} U_i \mid spt(f) \text{ is finite } \}$.*

Example 1.23 *If $\{U_i \mid i \in I\}$ is a collection of vector spaces over a field $\mathbb{F}$ then $\oplus_{i\in I}U_i$ is a subspace of $\prod_{i\in I} U_i$. This is the* **external direct sum** *of the spaces $\{U_i|i \in I\}$.*

Remark 1.3 *If I is a finite set and $\{U_i \mid i \in I\}$ is a collection of vector spaces over a field $\mathbb{F}$ then the external direct sum and the direct product of $\{U_i \mid i \in I\}$ are identical.*

Example 1.24 *Let $\mathbb{K} \subset \mathbb{L}$ be fields. Using the addition in $\mathbb{L}$ and the restriction of the multiplication of $\mathbb{L}$ to $\mathbb{K} \times \mathbb{L}$, $\mathbb{L}$ becomes a vector space over $\mathbb{K}$. This example is used throughout field theory and, in particular, Galois theory.*

Theorem 1.8 *Suppose U and W are subspaces of the vector space V. Then $U \cap W$ is a subspace.*

Proof *By $U \cap W$, we mean the intersection, all the objects that belong to both U and W. Note that $U \cap W$ is nonempty since both U and W contain $\mathbf{0}$ and therefore $\mathbf{0} \in U \cap W$.*

We have to show that $U \cap W$ is closed under addition and scalar multiplication. Suppose $\boldsymbol{x}$ and $\boldsymbol{y}$ are vectors in $U \cap W$. Then $\boldsymbol{x}$ and $\boldsymbol{y}$ are vectors that are contained in both U and W. Since U is a subspace and $\boldsymbol{x}, \boldsymbol{y} \in U$, it follows that $\boldsymbol{x} + \boldsymbol{y} \in U$. Since W is a subspace and $\boldsymbol{x}, \boldsymbol{y} \in W$, it follows that $\boldsymbol{x} + \boldsymbol{y} \in W$. Since $\boldsymbol{x} + \boldsymbol{y}$ is in U and in W, it is in the intersection and therefore $U \cap W$ is closed under addition.

For scalar multiplication: Assume $\boldsymbol{x} \in U \cap W$ and c is a scalar. Since $\boldsymbol{x}$ is in the intersection it is in both U and W. Since it is in U and U is a subspace, $c\boldsymbol{x}$ is in U. Since $\boldsymbol{x}$ is in W and W is a subspace the scalar multiple $c\boldsymbol{x}$ is in W. Since $c\boldsymbol{x}$ is in U and $c\boldsymbol{x}$ is in W it is in the intersection. Therefore $U \cap W$ is closed under scalar multiplication.

Definition 1.16 *Let U, W be subspaces of a vector space V. The* **sum of** U *and W, denoted by $U + W$, is the set of all vectors which can be written as a sum of a vector $\boldsymbol{u}$ from U and a vector $\boldsymbol{w}$ from W,*

$$U + W := \{\boldsymbol{u} + \boldsymbol{w} | \boldsymbol{u} \in U, \boldsymbol{w} \in W\}.$$

More generally, if $U_1, U_2, \ldots, U_k$ are subspaces of V, then the **sum** *of $U_1, U_2, \ldots, U_k$ is the set of all elements of the form $\boldsymbol{u}_1 + \boldsymbol{u}_2 + \cdots + \boldsymbol{u}_k$ with $\boldsymbol{u}_i \in U_i$. This is denoted by $U_1 + U_2 + \cdots + U_k$.*

Example 1.25 *If $U_1, U_2, \ldots, U_k$ are subspaces of the vector space V, then $U_1 + U_2 + \cdots + U_k$ is a subspace of V. We prove this in the case of the sum of two subspaces and leave the general case as an exercise.*

Theorem 1.9 *If U and W are subspaces of a vector space V, then $U + W$ is a subspace of V.*

Proof *Suppose $\boldsymbol{x}, \boldsymbol{y} \in U + W$. Then there are elements $\boldsymbol{u}_1 \in U, \boldsymbol{w}_1 \in W$ so $\boldsymbol{x} = \boldsymbol{u}_1 + \boldsymbol{w}_1$ and elements $\boldsymbol{u}_2 \in U, \boldsymbol{w}_2 \in W$ so that $\boldsymbol{y} = \boldsymbol{u}_2 + \boldsymbol{w}_2$. Then*

$$\boldsymbol{x} + \boldsymbol{y} = (\boldsymbol{u}_1 + \boldsymbol{w}_1) + (\boldsymbol{u}_2 + \boldsymbol{w}_2) = (\boldsymbol{u}_1 + \boldsymbol{u}_2) + (\boldsymbol{w}_1 + \boldsymbol{w}_2).$$

Since U is a subspace $\boldsymbol{u}_1 + \boldsymbol{u}_2 \in U$, and since W is a subspace, $\boldsymbol{w}_1 + \boldsymbol{w}_2 \in W$. Therefore, $\boldsymbol{x} + \boldsymbol{y} = (\boldsymbol{u}_1 + \boldsymbol{u}_2) + (\boldsymbol{w}_1 + \boldsymbol{w}_2) \in U + W$. So $U + W$ is closed under addition.

We leave the case of scalar multiplication as an exercise.

Definition 1.17 *Let $U_1, U_2, \ldots, U_k$ be subspaces of a vector space V. We say that V is a* **direct sum** *of $U_1, U_2, \ldots, U_k$, and we write $V = U_1 \oplus U_2 \oplus \cdots \oplus U_k$ if every vector in V can be written* **uniquely** *as a sum of vectors $\boldsymbol{u}_1 + \boldsymbol{u}_2 + \cdots + \boldsymbol{u}_k$ where $\boldsymbol{u}_i \in U$ for $1 \leq i \leq k$. Put more abstractly, the following hold:*

i. If $\boldsymbol{v} \in V$ then there exists $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ with $\boldsymbol{u}_i \in U_i$ such that $\boldsymbol{v} = \boldsymbol{u}_1 + \boldsymbol{u}_2 + \cdots + \boldsymbol{u}_k$; and

ii. If $\boldsymbol{u}_i, \boldsymbol{w}_i \in U_i$ and $\boldsymbol{u}_1 + \boldsymbol{u}_2 + \cdots + \boldsymbol{u}_k = \boldsymbol{w}_1 + \boldsymbol{w}_2 + \cdots + \boldsymbol{w}_k$, then $\boldsymbol{u}_i = \boldsymbol{w}_i$ for all i.

Example 1.26 *Let* $U_1 = \left\{ \begin{pmatrix} a \\ 0 \\ 0 \end{pmatrix} \mid a \in \mathbb{F} \right\}, U_2 = \left\{ \begin{pmatrix} 0 \\ b \\ 0 \end{pmatrix} \mid b \in \mathbb{F} \right\}$, *and* $U_3 = \left\{ \begin{pmatrix} 0 \\ 0 \\ c \end{pmatrix} \mid c \in \mathbb{F} \right\}$. *Then* $\mathbb{F}^3 = U_1 \oplus U_2 \oplus U_3$.

Theorem 1.10 *Let* $U_1, U_2, \ldots, U_k$ *be subspaces of a vector space* V. *For* i *a natural number,* $1 \leq i \leq k$ *set* $W_i = \sum_{j \neq i} U_i$. *Then* $V = U_1 \oplus U_2 \oplus \cdots \oplus U_k$ *if and only if the following two conditions hold: i)* $V = U_1 + U_2 + \cdots + U_k$; *and ii)* $U_i \cap W_i = \{\mathbf{0}\}$ *for each* i.

Proof *Suppose* $V = U_1 \oplus U_2 \oplus \cdots \oplus U_k$ *and* $\boldsymbol{v} \in U_i \cap W_i$. *Then there are* $\boldsymbol{u}_j \in U_j, j \neq i$ *such that* $\boldsymbol{v} = \sum_{j \neq i} \boldsymbol{u}_j$. *Then* $\boldsymbol{u}_1 + \cdots + \boldsymbol{u}_{j-1} + (-\boldsymbol{v}) + \boldsymbol{u}_{j+1} + \cdots + \boldsymbol{u}_k = \mathbf{0}$ *is an expression for* $\mathbf{0}$ *as a sum of vectors from* U_i. *However, since* V *is the direct sum, there is a unique expression for the zero vector as a sum of vectors from the* U_i, *namely,* $\mathbf{0} = \mathbf{0} + \cdots + \mathbf{0}$. *Therefore, for* $i \neq j, \boldsymbol{u}_j = \mathbf{0}$ *and* $-\boldsymbol{v} = \mathbf{0}$.

Conversely, assume i) and ii) hold. By i) V *is the sum of* $U_1, U_2, \ldots, U_k$. *We therefore need to prove that if* $\boldsymbol{u}_i, \boldsymbol{w}_i \in U_i$ *and*

$$\boldsymbol{u}_1 + \boldsymbol{u}_2 + \cdots + \boldsymbol{u}_k = \boldsymbol{w}_1 + \boldsymbol{w}_2 + \cdots + \boldsymbol{w}_k, \tag{1.3}$$

then $\boldsymbol{u}_i = \boldsymbol{w}_i$ *for all* i.

It follows from Equation (1.3) that

$$\boldsymbol{u}_i - \boldsymbol{w}_i = (\boldsymbol{w}_1 - \boldsymbol{u}_1) + \cdots + (\boldsymbol{w}_{i-1} - \boldsymbol{u}_{i-1}) + (\boldsymbol{w}_{i+1} - \boldsymbol{u}_{i+1}) + \cdots + (\boldsymbol{w}_k - \boldsymbol{u}_k). \tag{1.4}$$

The vector on the left-hand side of Equation (1.4) belongs to U_i, *and the vector on the right-hand side of Equation (1.4) belongs to* W_i. *By ii)* $\boldsymbol{u}_i - \boldsymbol{w}_i = \mathbf{0}$ *from which it follows that* $\boldsymbol{u}_i = \boldsymbol{w}_i$ *as required.*

The following definition is exceedingly important and used extensively when we study the structure of a linear operator:

Definition 1.18 *Let* V *be a vector space and* U *a subspace of* V. *A subspace* W *is said to be a* **complement** *of* U *in* V *if* $V = U \oplus W$.

We complete the section with a construction that will be used later in a subsequent section.

Definition 1.19 *Let V be a vector space and W a subspace. We will say two vectors $\boldsymbol{u}, \boldsymbol{v} \in V$ are* **congruent modulo** *W and write $\boldsymbol{u} \equiv \boldsymbol{v}$ (mod W) if $\boldsymbol{u} - \boldsymbol{v} \in W$.*

Lemma 1.1 *Let W be a subspace of the vector space V. Then the relation "congruent modulo W" is an equivalence relation.*

Proof *We have to prove that the relation is reflexive, symmetric, and transitive.*

Reflexive: Since every subspace of V contains $\mathbf{0}$, in particular $\mathbf{0} \in W$. Since for every vector $\boldsymbol{v}, \boldsymbol{v} - \boldsymbol{v} = \mathbf{0}$, it follows that $\boldsymbol{v} \equiv \boldsymbol{v}$ (mod W) and the relation is reflexive.

Symmetric: We have to prove if $\boldsymbol{u} \equiv \boldsymbol{v}$ (mod W) then $\boldsymbol{v} \equiv \boldsymbol{u}$ (mod W). If $\boldsymbol{u} \equiv \boldsymbol{v}$ (mod W), then $\boldsymbol{u} - \boldsymbol{v} \in W$. But then $(-1)(\boldsymbol{u} - \boldsymbol{v}) = \boldsymbol{v} - \boldsymbol{u} \in W$ and, consequently, $\boldsymbol{v} \equiv \boldsymbol{u}$ (mod W) as required.

Transitive: We have to prove if $\boldsymbol{u} \equiv \boldsymbol{v}$ mod W) and $\boldsymbol{v} \equiv \boldsymbol{x}$ (mod W) then $\boldsymbol{u} \equiv \boldsymbol{x}$ (mod W). From $\boldsymbol{u} \equiv \boldsymbol{v}$ (mod W) we conclude $\boldsymbol{u} - \boldsymbol{v} \in W$. Similarly, $\boldsymbol{v} \equiv \boldsymbol{x}$ (mod W) implies that $\boldsymbol{v} - \boldsymbol{x} \in W$. Since W is a subspace, it is closed under addition. Therefore $(\boldsymbol{u} - \boldsymbol{v}) + (\boldsymbol{v} - \boldsymbol{x}) = \boldsymbol{u} - \boldsymbol{x} \in W$. Thus, $\boldsymbol{u} \equiv \boldsymbol{x}$ (mod W).

Definition 1.20 *For W a subspace of a vector space V and a vector $\boldsymbol{u}$ from V, we define the* **coset of $\boldsymbol{u}$ modulo** *W to be $\boldsymbol{u} + W = \{\boldsymbol{u} + \boldsymbol{w} | \boldsymbol{w} \in W\}$.*

Lemma 1.2 *Let W be a subspace of the vector space V and let $\boldsymbol{u} \in V$. Then the equivalence class of the relation congruent modulo W containing $\boldsymbol{u}$ is the coset $\boldsymbol{u} + W$.*

Proof *Denote the equivalence class of $\boldsymbol{u}$ for the relation congruent modulo W by $[\boldsymbol{u}]_W$. We have to show that $[\boldsymbol{u}]_W \subseteq \boldsymbol{u} + W$ and $\boldsymbol{u} + W \subseteq [\boldsymbol{u}]_W$.*

Suppose $\boldsymbol{v} \in \boldsymbol{u} + W$. Then there exists a vector $\boldsymbol{w} \in W$ such that $\boldsymbol{v} = \boldsymbol{u} + \boldsymbol{w}$. Then $\boldsymbol{u} - \boldsymbol{v} = \boldsymbol{u} - (\boldsymbol{u} + \boldsymbol{w}) = -\boldsymbol{w} \in W$, and we conclude that $\boldsymbol{u} \equiv \boldsymbol{v}$ (mod W) and therefore $\boldsymbol{v} \in [\boldsymbol{u}]_W$ and thus $\boldsymbol{u} + W \subseteq [\boldsymbol{u}]_W$.

Suppose $\boldsymbol{v} \in [\boldsymbol{u}]_W$ so that $\boldsymbol{u} \equiv \boldsymbol{v}$ (mod W). Then $\boldsymbol{u} - \boldsymbol{v} = \boldsymbol{w} \in W$. Then $\boldsymbol{v} = \boldsymbol{u} + (-\boldsymbol{w}) \in \boldsymbol{u} + W$, and so $[\boldsymbol{u}]_W \subseteq \boldsymbol{u} + W$ and we have the desired equality.

Remark 1.4 *It follows from Lemma (1.2) for any vectors* $\boldsymbol{u}, \boldsymbol{v} \in V$ *that either* $\boldsymbol{u} + W = \boldsymbol{v} + W$ *or* $(\boldsymbol{u} + W) \cap (\boldsymbol{v} + W) = \emptyset$ *since distinct equivalence classes are disjoint.*

Lemma 1.3 *Let* W *be a subspace of a vector space* V*. The following hold:*

i) If $\boldsymbol{u}_1 \equiv \boldsymbol{u}_2$ $(mod\ W)$ *and* $\boldsymbol{v}_1 \equiv \boldsymbol{v}_2$ $(mod\ W)$*, then* $\boldsymbol{u}_1 + \boldsymbol{v}_1 \equiv \boldsymbol{u}_2 + \boldsymbol{v}_2$ $(mod\ W)$.

ii) If $\boldsymbol{u} \equiv \boldsymbol{v}$ $(mod\ W)$ *and* c *is scalar, then* $c\boldsymbol{u} \equiv c\boldsymbol{v}$ $(mod\ W)$.

Proof *i) If* $\boldsymbol{u}_1 \equiv \boldsymbol{u}_2$ $(mod\ W)$*, then* $\boldsymbol{u}_1 - \boldsymbol{u}_2 \in W$*. Similarly,* $\boldsymbol{v}_1 - \boldsymbol{v}_2 \in W$*. Since* W *is a subspace* $(\boldsymbol{u}_1 - \boldsymbol{u}_2) + (\boldsymbol{v}_1 - \boldsymbol{v}_2) = (\boldsymbol{u}_1 + \boldsymbol{v}_1) - (\boldsymbol{u}_2 + \boldsymbol{v}_2) \in W$*. It then follows that* $\boldsymbol{u}_1 + \boldsymbol{v}_1 \equiv \boldsymbol{u}_2 + \boldsymbol{v}_2$ $(mod\ W)$.

ii) Suppose $\boldsymbol{u} \equiv \boldsymbol{v}$ $(mod\ W)$*. Then* $\boldsymbol{u} - \boldsymbol{v} \in W$*. Since* W *is a subspace* $c(\boldsymbol{u} - \boldsymbol{v}) = c\boldsymbol{u} - c\boldsymbol{w} \in W$*. Whence* $c\boldsymbol{u} \equiv c\boldsymbol{v}$ $(mod\ W)$.

Theorem 1.11 *Let* W *be a subspace of* V*. Denote by* V/W *the collection of cosets of* V *modulo* W*. For two cosets* $[\boldsymbol{u}]_W$ *and* $[\boldsymbol{v}]_W$ *we define their sum, denoted by* $[\boldsymbol{u}]_W + [\boldsymbol{v}]_W$*, as* $[\boldsymbol{u} + \boldsymbol{v}]_W$*. Also, for* $[\boldsymbol{u}]_W$ *and a scalar* c *define* $c \cdot [\boldsymbol{u}]_W = [c\boldsymbol{u}]_W$*. Then these operations are well defined and make* V/W *into a vector space with identity element* $[\mathbf{0}]_W$.

Proof *The operations are well defined follows from Lemma (1.3). We have to show that the axioms of a vector space hold:*

(A1) Let $\boldsymbol{u}, \boldsymbol{v} \in V$*.* $[\boldsymbol{u}]_W + [\boldsymbol{v}]_W = [\boldsymbol{u} + \boldsymbol{v}]_W = [\boldsymbol{v} + \boldsymbol{u}]_W$ *since the addition of vectors in* V *is commutative. Moreover,* $[\boldsymbol{v} + \boldsymbol{u}]_W = [\boldsymbol{v}]_W + [\boldsymbol{u}]_W$*, and therefore addition of vectors in* V/W *is commutative.*

(A2) Let $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{x} \in V$*. Then*

$$([\boldsymbol{u}]_W + [\boldsymbol{v}]_W) + [\boldsymbol{x}]_W = [\boldsymbol{u} + \boldsymbol{v}]_W + [\boldsymbol{x}]_W = [(\boldsymbol{u} + \boldsymbol{v}) + \boldsymbol{x}]_W = [\boldsymbol{u} + (\boldsymbol{v} + \boldsymbol{x})]_W,$$

since vector addition in V *is associative. However, by the definition of addition,* $[\boldsymbol{u} + (\boldsymbol{v} + \boldsymbol{x})]_W = [\boldsymbol{u}]_W + [\boldsymbol{v} + \boldsymbol{x}]_W = [\boldsymbol{u}]_W + ([\boldsymbol{v}]_W + [\boldsymbol{x}]_W)$ *and so the addition of* V/W *is associative.*

(A3) For $\boldsymbol{u} \in V, [\boldsymbol{u}]_W + [\mathbf{0}]_W = [\boldsymbol{u} + \mathbf{0}]_W = [\boldsymbol{u}]_W$*, and so* $[\mathbf{0}]_W$ *is an additive identity for* V/W.

(A4) For $\boldsymbol{u} \in V, [\boldsymbol{u}]_W + [-\boldsymbol{u}]_W = [\boldsymbol{u} + (-\boldsymbol{u})]_W = [\mathbf{0}]_W$.

(M1) For vectors $\boldsymbol{u}, \boldsymbol{v} \in V$ *and scalar* a*,* $a \cdot ([\boldsymbol{u}]_W + [\boldsymbol{v}]_W) = a \cdot [\boldsymbol{u} + \boldsymbol{v}]_W = [a \cdot (\boldsymbol{u} + \boldsymbol{v})]_W = [a \cdot \boldsymbol{u} + a \cdot \boldsymbol{v}]_W = [a \cdot \boldsymbol{u}]_W + [a \cdot \boldsymbol{v}]_W = a \cdot [\boldsymbol{u}]_W + a \cdot [\boldsymbol{v}]_W$.

(M2) For $\boldsymbol{u} \in V$ and scalars a, b we have $(a+b) \cdot [\boldsymbol{u}]_W = [(a+b) \cdot \boldsymbol{u}]_W = [a\boldsymbol{u} + b\boldsymbol{u}]_W = [a \cdot \boldsymbol{u}]_W + [b \cdot \boldsymbol{u}]_W = a \cdot [\boldsymbol{u}]_W + b \cdot [\boldsymbol{u}]_W$.

(M3) For $\boldsymbol{u} \in V$ and scalars a, b, $b \cdot (a \cdot [\boldsymbol{u}]_W) = b \cdot [a \cdot \boldsymbol{u}]_W = [b \cdot (a \cdot \boldsymbol{u})]_W = [(ba) \cdot \boldsymbol{u}]_W = (ba) \cdot [\boldsymbol{u}]_W$.

(M4) For $\boldsymbol{u} \in V, 1 \cdot [\boldsymbol{u}]_W = [1 \cdot \boldsymbol{u}]_W = [\boldsymbol{u}]_W$.

Thus, the axioms all hold and V/W is a vector space.

Definition 1.21 *If W is a subspace of V, the vector space V/W is called the* **quotient space** *of V modulo W.*

Exercises

In Exercise 1 and 2, demonstrate that the subset $W = \{f(a,b) : a, b \in \mathbb{R}\}$ is not a subspace of $\mathbb{R}_{(2)}[x]$ for the given $f(a,b)$.

1. $f(a,b) = (2a - 3b + 1) + (-2a + 5b)X + (2a + b)X^2$.

2. $f(a,b) = ab + (a - b)X + (a + b)X^2$.

3. Set $W = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3 | \ 3x - 2y + 4z = 0 \right\}$. Prove that W is a subspace of $\mathbb{R}^3$.

4. Let V be a vector space, $\mathcal{F}$ a collection of subspaces of V with the following property: If $X, Y \in \mathcal{F}$, then there exists a $Z \in \mathcal{F}$ such that $X \cup Y \subset Z$. Prove that $\cup_{U \in \mathcal{F}} U$ is a subspace of V.

5. Let V be a vector space U, W subspaces. Prove that $U + W$ is closed under scalar multiplication.

6. Let V be a vector space and assume that U, W are proper subspaces of V and that U is not a subset of W and W is not a subset of U. Prove that $U \cup W$ is closed under scalar multiplication but is not a subspace of V.

7. Give an example of a vector space V and non-trivial subspaces X, Y, Z of V such that $V = X \oplus Y = X \oplus Z$ but $Y \neq Z$. (Hint: You can find examples in $\mathbb{R}^2$.)

8. Find examples of non-trivial subspaces $X, Y, Z \subset \mathbb{R}^2$ such that $X + Y = \mathbb{R}^2$ and $X \cap Z = Y \cap Z = \{\mathbf{0}\}$. (This implies that $(X + Y) \cap Z \neq X \cap Z + Y \cap Z$.)

9. Let X be a set and $\mathbb{F}$ a field. Prove that $\mathcal{M}_{fin}(X, \mathbb{F})$ is a subspace of $\mathcal{M}(X, \mathbb{F})$.

10. Let X be a set, $\mathbb{F}$ a field, and $Y \subset X$. Prove that $\{f \in \mathcal{M}(X, \mathbb{F}) | f(y) = 0$ for all $y \in Y\}$ is a subspace of $\mathcal{M}(X, \mathbb{F})$.

11. Let X be a set, $\mathbb{F}$ a field, and x a fixed element of X. Prove that $\{f \in \mathcal{M}(X, \mathbb{F}) | f(x) = 1\}$ is not a subspace of $\mathcal{M}(X, \mathbb{F})$.

12. Let $\mathbb{F}$ be a field, I a nonempty set, and for each $i \in I, U_i$ a vector space over $\mathbb{F}$ with zero element $\mathbf{0}_i$. Prove that $\oplus_{i \in I} U_i$ is a subspace of $\prod_{i \in I} U_i$.

13. Let X, Y, Z be subspaces of a vector space V and assume that $Y \subset X$. Prove that $X \cap (Y + Z) = Y + (X \cap Z)$. This is known as the *modular law* of subspaces.

14. Let $\mathcal{M}_{odd}(\mathbb{R}, \mathbb{R})$ consists of all function $f : \mathbb{R} \to \mathbb{R}$ such that $f(-x) = f(x)$ for all $x \in \mathbb{R}$. Prove that $\mathcal{M}_{odd}(\mathbb{R}, \mathbb{R})$ is a subspace of $\mathcal{M}(\mathbb{R}, \mathbb{R})$.

1.5 Span and Independence

What You Need to Know

To make sense of this new material, you should have a good grasp of the following concepts: field, a vector space over a field $\mathbb{F}$, subspace of a vector space V, and linear combination of a finite sequence of vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k$ from a vector space V. You should know the algorithm for using elementary row operations to obtain an echelon form, respectively, the reduced echelon form, of an arbitrary real matrix. You should also know how to make use of this to determine whether a sequence of vectors from $\mathbb{R}^n$ is linearly independent or spans $\mathbb{R}^n$.

We begin with some fundamental definitions:

Definition 1.22 *Let $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$ be a sequence of vectors in V. The set of all linear combinations of $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$ is called the* **span** *of $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$ and is denoted by Span$(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$. By convention, the span of the empty sequence is the trivial subspace $\{\mathbf{0}\}$.*

If $V = Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$, then we say that $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$ **spans** *V and $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$ is a* **spanning sequence** *for V.*

More generally, for an arbitrary set S of vectors from V the span of S, Span(S), is the collection of all vectors $\boldsymbol{v}$ for which there is some finite sequence $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$ from S such that $\boldsymbol{v}$ is a linear combination of $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$.

Thus, Span(S) is the union of Span(F) taken over every finite sequence F of vectors from S.

Before we proceed to a general result we need to introduce a useful concept and prove a short lemma.

Definition 1.23 *Let $A = (\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k)$ and $B = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_l)$ be two finite sequences of vectors in a vector space V. By the* **join of the two sequences** *A and B, we mean the sequence obtained by putting the vectors of B after the vectors in A and denote this by $A\natural B$. Thus, $A\natural B = (\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k, \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_l)$.*

Lemma 1.4 *Let A and B be finite sequences from the vector space V. Then any vector in Span(A) or Span(B) is in Span$(A\sharp B)$.*

Proof *To see this, suppose $\boldsymbol{x} = a_1\boldsymbol{u}_1 + a_2\boldsymbol{u}_2 + \cdots + a_k\boldsymbol{u}_k$. Then $\boldsymbol{x} = a_1\boldsymbol{u}_1 + a_2\boldsymbol{u}_2 + \cdots + a_k\boldsymbol{u}_k + 0\boldsymbol{v}_1 + 0\boldsymbol{v}_2 + \cdots + 0\boldsymbol{v}_l \in A\sharp B$.*

Similarly, if $\boldsymbol{y} = b_1\boldsymbol{v}_1 + b_2\boldsymbol{v}_2 + \cdots + b_l\boldsymbol{v}_l$, then $\boldsymbol{y} = 0\boldsymbol{u}_1 + 0\boldsymbol{u}_2 + \cdots + 0\boldsymbol{u}_k + b_1\boldsymbol{v}_1 + b_2\boldsymbol{v}_2 + \cdots + b_l\boldsymbol{v}_l \in$ Span$(A\sharp B)$.

Thus, Span(A), Span$(B) \subset$ Span$(A\sharp B)$.

Theorem 1.12 *Let S be sequence from V.*

i) Span(S) is a subspace of V.

ii) If W is a subspace of V and W contains S, then W contains Span(S).

Proof *We first prove i) in the case that S is finite.*

We have to show Span(S) is closed under addition and closed under scalar multiplication.

Span(S) **is closed under addition***: We need to show if $\boldsymbol{u}, \boldsymbol{v} \in$ Span(S) then $\boldsymbol{u} + \boldsymbol{v} \in$ Span(S). We can write $\boldsymbol{u} = a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_k\boldsymbol{v}_k, \boldsymbol{v} = b_1\boldsymbol{v}_1 + b_2\boldsymbol{v}_2 + \cdots + b_k\boldsymbol{v}_k$ for some scalars $a_i, b_i \in \mathbb{F}, 1 \leq i \leq k$.*

Now $\boldsymbol{u} + \boldsymbol{v} = (a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_k\boldsymbol{v}_k) + (b_1\boldsymbol{v}_1 + b_2\boldsymbol{v}_2 + \cdots + b_k\boldsymbol{v}_k)$. By associativity and commutativity of addition this is equal to

$$(a_1 + b_1)\boldsymbol{v}_1 + (a_2 + b_2)\boldsymbol{v}_2 + \cdots + (a_k + b_k)\boldsymbol{v}_k,$$

an element of Span$(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$.

Span(S) **is closed under scalar multiplication***: We must show if $\boldsymbol{u} \in$ Span(S), and $c \in \mathbb{F}$ then $c\boldsymbol{u} \in S$. We can write $\boldsymbol{u} = a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_k\boldsymbol{v}_k$. Then $c\boldsymbol{u}$ is equal to $(ca_1)\boldsymbol{v}_1 + (ca_2)\boldsymbol{v}_2 + \cdots + (ca_k)\boldsymbol{v}_k \in$ Span(S) by vector space axiom (M3). This completes the finite case.*

The infinite case

Let $\mathcal{F} = \{$Span$(A) | A \subset S, |A|$ is finite $\}$. Then Span$(S) = \cup_{W \in \mathcal{F}} F$. Now suppose $F_1, F_2 \in \mathcal{F}$, say, $F_1 =$ Span(A_1) and $F_2 =$ Span(A_2). Set $A' = A_1 \sharp A_2$ and $F' =$ Span(A'). By Lemma (1.4), $F_1 \cup F_2 \subset F'$. It then follows by Exercise 1.4.9 that Span(S) is a subspace.

ii) This follows from Theorem (1.7).

Remark 1.5 *The two parts of Theorem (1.12) imply that Span(S) is the "minimal" subspace of V which contains S, that is, if W is a subspace containing S and $W \subset$ Span(S), then $W =$ Span(S).*

Some important consequences of Theorem (1.12) are the following:

Corollary 1.1 *i) If W is a subspace of a vector space V, then $Span(W) = W$.*

ii) If S is a subset of a vector space V, then $Span(Span(S)) = Span(S)$.

Theorem 1.13 *Let $S = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_k)$ be a sequence of (distinct) vectors. Assume for some i the vector $\boldsymbol{v}_i$ is a linear combination of $S \setminus (\boldsymbol{v}_i) = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_{i-1}, \boldsymbol{v}_{i+1}, \dots, \boldsymbol{v}_k)$. Then $Span(S) = Span(S \setminus (\boldsymbol{v}_i))$.*

Proof *By relabeling the vectors if necessary, we assume that $\boldsymbol{v}_k$ is a linear combination of $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_{k-1}$, say,*

$$\boldsymbol{v}_k = a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_{k-1}\boldsymbol{v}_{k-1} \tag{1.5}$$

We need to show that $Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k) = Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_{k-1})$. Since $Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_{k-1}) \subset Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k)$ we only have to show that $Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k)$ is contained in $Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_{k-1})$.

Suppose $\boldsymbol{u} \in Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k)$ so that

$$\boldsymbol{u} = c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_k\boldsymbol{v}_k. \tag{1.6}$$

Substituting Equation (1.5) into Equation (1.6), we get $\boldsymbol{u} = c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_{k-1}\boldsymbol{v}_{k-1} + c_k(a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_{k-1}\boldsymbol{v}_{k-1})$.

After distributing in the last term and rearranging, we get $\boldsymbol{u} = (c_1 + c_k a_1)\boldsymbol{v}_1 + (c_2 + c_k a_2)\boldsymbol{v}_2 + \cdots + (c_{k-1} + c_k a_{k-1})\boldsymbol{v}_{k-1}$ an element of $Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_{k-1})$.

We now come to our second fundamental concept:

Definition 1.24 *A finite sequence of vectors, $(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k)$ from a vector space V is* **linearly dependent** *if there are scalars $c_1, c_2, \dots, c_k$, not all zero, such that $c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_k\boldsymbol{v}_k = \mathbf{0}$.*

The sequence $(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k)$ is **linearly independent** *if it is not linearly dependent. This means if $c_1, c_2, \dots, c_k$ are scalars such that $c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_k\boldsymbol{v}_k = \mathbf{0}$ then $c_1 = c_2 = \cdots = c_k = 0$.*

Remark 1.6 *The term "linearly dependent" suggests that at least one of the vectors depends on the others. We will show below that this is, indeed, true and, in fact, equivalent to the standard definition given above. The reason the above definition is chosen over the more intuitive formulation is that it admits a fairly straightforward algorithm that can be performed once to determine whether a finite sequence of vectors is linearly dependent, whereas in the latter case one would have to perform an algorithm checking whether each vector is a linear combination of the remaining vectors, which is much more work.*

Remark 1.7 *Any finite sequence of vectors that contains a repeated vector is linearly dependent. Therefore, if a finite sequence of vectors is linearly independent, the vectors are distinct. In this case we can speak of a finite set of linearly independent vectors. We make use of this in extending the definition of linear independence and linear dependence to infinite sets of vectors.*

Definition 1.25 *An infinite set of vectors is* **linearly dependent** *if it contains a finite subset that is linearly dependent. Otherwise, S is* **linearly independent**.

Example 1.27 *The sequence* $(2 + 4x - 5x^2 - x^3, 1 - x^3, x - x^3, x^2 - x^3)$ *is linearly dependent since*

$$(2 + 4x - 5x^2 - x^3) + (-2)(1 - x^3) + (-4)x - x^3) + 5(x^2 - x^3) = 0.$$

Example 1.28 *The sequence* $(1, x, x^2, \ldots, x^n)$ *is linearly independent in* $\mathbb{F}_{(n)}[x]$.

The following result gives useful criteria for a finite sequence of vectors to be linearly dependent.

Theorem 1.14 *Let $k \geq 2$ and S be the sequence $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$.*

i) S is linearly dependent if and only if for some j the vector $\boldsymbol{v}_j$ is a linear combination of the sequence obtained from S when $\boldsymbol{v}_j$ is deleted.

ii) Assume $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i)$ is linearly independent for some $i \geq 1$ (note that this implies, in particular, that $\boldsymbol{v}_1 \neq \mathbf{0}$). Then S is linearly dependent if and only there is a $j > i$ such that $\boldsymbol{v}_j$ is a linear combination of the sequence $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{j-1})$.

Proof *i) Assume S is linearly dependent. Then there are scalars $c_1, c_2, \ldots, c_k$ not all zero, such that $c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_k\boldsymbol{v}_k = \mathbf{0}$. Suppose $c_j \neq 0$. Then $c_j\boldsymbol{v}_j = (-c_1)\boldsymbol{v}_1 + (-c_2)\boldsymbol{v}_2 + \cdots + (-c_{j-1})\boldsymbol{v}_{j-1} + (-c_{j+1})\boldsymbol{v}_{j+1} + \cdots + (-c_k)\boldsymbol{v}_k$. Dividing both sides by c_j, we obtain*

$$\boldsymbol{v}_j = \sum_{i \neq j} \left(-\frac{c_i}{c_j}\right) \boldsymbol{v}_i. \tag{1.7}$$

We conclude from Equation (1.7) that $\boldsymbol{v}_j \in Span(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{j-1}, \boldsymbol{v}_{j+1}, \ldots, \boldsymbol{v}_k)$.

Conversely, suppose $\boldsymbol{v}_j$ *is in Span*$(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{j-1}, \boldsymbol{v}_{j+1}, \ldots \boldsymbol{v}_k)$. *Then there are scalars* $c_1, c_2, \ldots, c_{j-1}, c_{j+1}, \ldots, c_k$ *such that*

$$\boldsymbol{v}_j = c_1\boldsymbol{v}_1 + \cdots + c_{j-1}\boldsymbol{v}_{j-1} + c_{j+1}\boldsymbol{v}_{j+1} + \cdots + c_k\boldsymbol{v}_k. \tag{1.8}$$

Subtracting $\boldsymbol{v}_j$ *from both sides, we obtain*

$$\mathbf{0} = c_1\boldsymbol{v}_1 + \cdots + c_{j-1}\boldsymbol{v}_j + (-1)\boldsymbol{v}_j + c_{j+1}\boldsymbol{v}_{j+1} + \cdots + c_k\boldsymbol{v}_k.$$

Since the coefficient of $\boldsymbol{v}_j$ *is* $-1 \neq 0$, *it follows that* $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)$ *is linearly dependent.*

ii) Suppose for some $j > i$ *that* $\boldsymbol{v}_j$ *is a linear combination of the sequence* $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{j-1})$. *Then by the first part it follows that* $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_j)$ *is linearly dependent, whence* $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)$ *is linearly dependent.*

On the other hand, suppose that $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$ *is linearly dependent. Let* $c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \ldots c_k\boldsymbol{v}_k = \mathbf{0}$ *be a non-trivial dependence relation. Choose* j *maximal so that* $c_j \neq 0$. *We claim that* $j > i$. *For otherwise,* $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_j)$ *is linearly dependent and a subsequence of* $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i)$ *from which it follows that* $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i)$ *is linearly dependent, contrary to the hypothesis. Thus,* $j > i$ *as claimed. With this choice of* j, *we have* $c_1\boldsymbol{v}_1 + \ldots c_j\boldsymbol{v}_j = \mathbf{0}$. *Subtracting* $c_j\boldsymbol{v}_j$ *from both sides, we obtain* $c_1\boldsymbol{v}_1 + \ldots c_{j-1}\boldsymbol{v}_{j-1} = -c_j\boldsymbol{v}_j$. *Dividing by* $-c_j$, *this becomes* $(-\frac{c_1}{c_j})\boldsymbol{v}_1 + (-\frac{c_2}{c_j})\boldsymbol{v}_2 + \cdots + (-\frac{c_j-1}{c_j})\boldsymbol{v}_{j-1} = \boldsymbol{v}_j$ *which proves that* $\boldsymbol{v}_j$ *is a linear combination of the sequence* $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{j-1})$.

The next result is extremely important. The first part will be used in the subsequent section to show the existence of bases in a finitely generated vector space. The second part will be the foundation for the notion of the coordinate vector.

Theorem 1.15 *Let* $S = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$ *be a linearly independent sequence of vectors in a vector space* V.

i) If $\boldsymbol{v}$ *is not in the span of* S, *then we get a linearly independent sequence by adjoining* $\boldsymbol{v}$ *to* S, *that is,* $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k, \boldsymbol{v})$ *is linearly independent.*

ii) Any vector $\boldsymbol{u}$ *in the span of* S *is expressible in one and only one way as a linear combination of* $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k$.

Proof *i) Suppose to the contrary that* $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k, \boldsymbol{v})$ *is linear dependent. Then there are scalars* $c_1, c_2, \ldots, c_k, c$ *not all zero such that* $c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \ldots c_k\boldsymbol{v}_k + c\boldsymbol{v} = \mathbf{0}$. *Suppose* $c = 0$. *Then some* $c_j \neq 0$, *and we have a non-trivial dependence relation on* $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)$, *contrary to the hypothesis. Thus,* $c \neq 0$. *But then* $c\boldsymbol{v} = (-c_1)\boldsymbol{v}_1 + \cdots + (-c_k)\boldsymbol{v}_k$ *from which we get* $\boldsymbol{v} = (-\frac{c_1}{c})\boldsymbol{v}_1 + \cdots + (-\frac{c_k}{c})\boldsymbol{v}_k$ *and therefore* $\boldsymbol{v} \in$ *Span*$(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$, *also contrary to our hypothesis. Thus,* $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k, \boldsymbol{v})$ *is linearly independent.*

ii) Suppose $\boldsymbol{u} = a_1\boldsymbol{v}_1 + \cdots + a_k\boldsymbol{v}_k = b_1\boldsymbol{v}_1 + \dots b_k\boldsymbol{v}_k$*. Subtracting the second expression from the first then, after rearranging and regrouping terms, we obtain* $(a_1 - b_1)\boldsymbol{v}_1 + \cdots + (a_k - b_k)\boldsymbol{v}_k = \boldsymbol{0}$*. Since* $(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k)$ *is linearly independent,* $a_1 - b_1 = a_2 - b_2 = \cdots = a_k - b_k = 0$ *from which we conclude that* $a_i = b_i$ *for* $1 \leq i \leq k$*.*

Exercises

1. Let X, Y be sequences or subsets of a vector space V. Assume $X \subset Span(Y)$ and $Y \subset Span(X)$. Prove that $Span(X) = Span(Y)$.

2. Let $\boldsymbol{u}, \boldsymbol{v}$ be vectors in the space V over the field $\mathbb{F}$ and c a scalar. Prove that $Span(\boldsymbol{u}, \boldsymbol{v}) = Span(\boldsymbol{u}, c\boldsymbol{u} + \boldsymbol{v})$.

3. Let $\boldsymbol{u}, \boldsymbol{v}$ be vectors in the space V over the field $\mathbb{F}$ and c a non-zero scalar. Prove that $Span(\boldsymbol{u}, \boldsymbol{v}) = Span(c\boldsymbol{u}, \boldsymbol{v})$.

4. Let c_{12}, c_{13}, and c_{23} be scalars and $\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3$ vectors. Prove that

$$Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3) = Span(\boldsymbol{v}_1, c_{12}\boldsymbol{v}_1 + \boldsymbol{v}_2, c_{13}\boldsymbol{v}_1 + c_{23}\boldsymbol{v}_2 + \boldsymbol{v}_3).$$

5. Prove if S consists of a single vector $\boldsymbol{v}$ then S is linearly dependent if and only if $\boldsymbol{v} = \boldsymbol{0}$.

6. Let $\boldsymbol{u}, \boldsymbol{v}$ be non-zero vectors. Prove that $(\boldsymbol{u}, \boldsymbol{v})$ is linearly dependent if and only if the vectors are scalar multiples of one another.

7. Prove if one of the vectors of a sequence $S = (\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k)$ is the zero vector then S is linearly dependent.

8. Remark (1.7) asserted that if a sequence contains repeated vectors then it is linearly dependent. Prove this.

9. Prove if a sequence S contains a subsequence S_0, which is linearly dependent, then S is linearly dependent.

10. Prove that a subsequence of a linearly independent sequence of vectors is linearly independent.

11. Assume that $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$ is linearly independent and that $(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_l)$ is linearly independent. Prove that $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k, \boldsymbol{v}_1, \dots, \boldsymbol{v}_l)$ is linearly independent if and only if $Span(\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k) \cap Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_l) = \{\boldsymbol{0}\}$.

12. Let $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$ be a sequence of vectors in a vector space V and $\boldsymbol{v}, \boldsymbol{w}$ vectors from V. Assume that $\boldsymbol{w} \in Span(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k, \boldsymbol{v}), \boldsymbol{w} \notin Span(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$. Prove that $\boldsymbol{v} \in Span(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k, \boldsymbol{w})$.

13. Let V be a vector space and assume that $(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3)$ is a linearly independent sequence from V, $\boldsymbol{w}$ is a vector from V, and $(\boldsymbol{v}_1 + \boldsymbol{w}, \boldsymbol{v}_2 + \boldsymbol{w}, \boldsymbol{v}_3 + \boldsymbol{w})$ is linearly dependent. Prove that $\boldsymbol{w} \in Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3)$.

1.6 Bases and Finite-Dimensional Vector Spaces

In this section, we introduce the concepts of basis and dimension. We will prove that every vector space that can be spanned by a finite sequence of vectors (referred to as a finitely generated vector space) has a basis and that every basis for such a space has the same number of vectors.

What You Need to Know

It is essential that you have a good grasp of the following concepts: vector space over a field $\mathbb{F}$, subspace of a vector space V, linear combination of vectors, span of a sequence or set of vectors, linear dependence and linear independence of a sequence or set of vectors. It is also important that you understand Theorem (1.15). Finally, given a sequence of vectors $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$ from $\mathbb{R}^n$ you will need to know how to find a basis for $Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$.

We begin with an important definition:

Definition 1.26 *Let V be a nonzero vector space over a field $\mathbb{F}$. A subset $\mathcal{B}$ of V is said to be a* **basis** *if the following are satisfied: 1) $\mathcal{B}$ is linearly independent; and 2) $Span(\mathcal{B}) = V$, that is, $\mathcal{B}$ spans V.*

It is our goal in this section and the following to prove that all vector spaces have bases. In this section, we will limit our treatment to those vector spaces that have a finite basis (finite dimensional vector spaces) while the next section is devoted to spaces which do not have a finite basis.

The spaces that we will treat presently are those that can be spanned by a finite number of vectors. We give a formal name to such spaces:

Definition 1.27 *A vector space V is* **finitely generated** *if it is possible to find a finite sequence of vectors $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$ such that $V = Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$.*

Example 1.29 *The spaces $\mathbb{F}^n$ and $\mathbb{F}_{(n)}[X]$ are finitely generated.*

The spaces $\mathbb{F}[X], F(\mathbb{R}), C(\mathbb{R}), C^1(\mathbb{R})$ are not finitely generated. Also, if X is an infinite set, then $\mathcal{M}_{fin}(X, \mathbb{F})$ and $\mathcal{M}(X, \mathbb{F})$ are not finitely generated.

We now come to an elegant theorem, which will imply the existence of bases in a finitely generated vector space.

Theorem 1.16 *(***Exchange Theorem***) Assume V can be generated by n vectors. Then any sequence of vectors of length greater than n is linearly dependent.*

Proof *Let $X = (\boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ be a spanning sequence of V, and $Y = (\boldsymbol{y}_1, \dots, \boldsymbol{y}_n, \boldsymbol{y}_{n+1})$ a sequence of length $n+1$. We prove Y is linearly dependent.*

Since $\boldsymbol{y}_1 \in Span(X)$, it follows that $(\boldsymbol{y}_1)\sharp X$ is linearly dependent. Since $\boldsymbol{y}_1 \neq \mathbf{0}$ it follows from part ii) of Theorem (1.14) that some $\boldsymbol{x}_i$ is a linear combination of the preceding vectors in the sequence $(\boldsymbol{y}_1, \boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$. By reordering the vectors of X, if necessary, we can assume that $\boldsymbol{x}_n$ is a linear combination of $Z_1 = (\boldsymbol{y}_1, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-1})$. Since we are assuming that $\boldsymbol{x}_n \in Span(Z_1)$, it follows that $Span(Z_1) = Span(X) = V$.

Now consider the sequence $(\boldsymbol{y}_2)\sharp Z_1$. Since $\boldsymbol{y}_2 \in Span(Z_1)$, it follows that $(\boldsymbol{y}_2)\sharp Z_1$ is linearly dependent. Again by ii) of Theorem (1.14) some vector in the sequence is a linear combination of the preceding vectors. Since $(\boldsymbol{y}_2, \boldsymbol{y}_1)$ is linearly independent, there must be some j with $1 \leq j \leq n-1$ such that $\boldsymbol{x}_j$ is a linear combination of the preceding vectors $(\boldsymbol{y}_2, \boldsymbol{y}_1, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{j-1})$. By relabeling, if necessary, we can assume that $\boldsymbol{x}_{n-1}$ is a linear combination of $Z_2 = (\boldsymbol{y}_2, \boldsymbol{y}_1, \dots, \boldsymbol{x}_{j-1}, \boldsymbol{x}_{j+1}, \dots, \boldsymbol{x}_n)$. By the same reasoning as before, Z_2 is a spanning set.

We can continue in this way, replacing vectors from X with vectors from Y, obtaining at each step a spanning sequence. After n iterations we get that $Z_n = (\boldsymbol{y}_n, \boldsymbol{y}_{n-1}, \dots, \boldsymbol{y}_2, \boldsymbol{y}_1)$ is a spanning sequence. But then $\boldsymbol{y}_{n+1} \in Span(Z_n)$ from which it follows that Y is linearly dependent as claimed.

The following corollary immediately follows from Theorem (1.16). It has many far-reaching consequences.

Corollary 1.2 *Assume the sequence $(\boldsymbol{x}_1, \dots, \boldsymbol{x}_m)$ from the vector space V is linearly independent and the sequence $(\boldsymbol{y}_1, \dots, \boldsymbol{y}_n)$ spans V. Then $m \leq n$.*

Theorem 1.17 *Let V be a finitely generated vector space, say, $V = Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n)$. Then V has a basis with at most n elements.*

Proof *By the exchange theorem, no linearly independent sequence has more than n vectors. Choose a linearly independent sequence $\mathcal{B} = (\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_m)$ with m as large as possible. Such sets exist because m must be less than or equal to n.*

We claim that $Span(\mathcal{B}) = V$. Suppose to the contrary that $Span(\mathcal{B}) \neq V$ and let $\boldsymbol{v} \in V \setminus Span(\mathcal{B})$. By i) of Theorem (1.15) the sequence $\mathcal{B} \cup (\boldsymbol{v})$ is linearly independent, which contradicts the maximality of m. Thus, $\mathcal{B}$ is linearly independent and spans V, from which it follows that $\mathcal{B}$ is a basis.

Remark 1.8 *It is not difficult to show that every spanning sequence can be contracted to a basis. This can be used to develop an algorithm for constructing a basis starting from a spanning sequence.*

By the same proof as Theorem (1.17), we can conclude a stronger statement.

Theorem 1.18 *Let V be a vector space and assume there is an integer n such that every linearly independent sequence from V has at most n vectors. Then V has a basis with at most n vectors.*

Because of the similarity to Theorem (1.17) we omit the proof.

Suppose now that V is a finitely generated vector space and has a spanning set with n vectors. If W is a subspace of V, then any linearly independent sequence of W is a linearly independent sequence of V, and therefore its length is bounded by n. Consequently, the theorem applies to W:

Theorem 1.19 *Assume that V can be generated by a sequence of n vectors. Then every subspace W of V has a basis with n or fewer vectors.*

A natural question arises: Can there be bases with different numbers of vectors? The next theorem says that every basis must have the same number of elements.

Theorem 1.20 *If a vector space V has a basis with n elements, then every basis has n elements.*

Proof *Let $\mathcal{B}$ be a basis with n elements and $\mathcal{B}'$ any other basis. Since $\mathcal{B}'$ is an independent sequence and $\mathcal{B}$ spans, it follows from Corollary (1.2) that $\mathcal{B}'$ has at most n elements, in particular, it is finite. So let us suppose that $\mathcal{B}'$, specifically, has m elements. We have just argued that $m \leq n$.*

On the other hand, since $\mathcal{B}'$ is a basis we have $Span(\mathcal{B}') = V$. Because $\mathcal{B}$ is a basis, it is linearly independent. Thus, by the Corollary (1.2) , $n \leq m$. Therefore, we conclude that $m = n$.

Definition 1.28 *Let V be a finitely generated vector space. The common length of all the bases of V, is the* **dimension** *of V. If this common number is n then we write $dim(V) = n$.*

Example 1.30 *1. $dim(\mathbb{F}^n) = n$. The sequence of vectors $(\boldsymbol{e}_1^n, \boldsymbol{e}_2^n, \dots, \boldsymbol{e}_n^n)$ is a basis.*

2. $dim(\mathbb{F}_{(n)}[X]) = n + 1$. The sequence of vectors $(1, x, x^2, \dots, x^n)$ is a basis. There are $n + 1$ vectors in this sequence.

The same arguments used to prove the invariance of the size of basis in a finitely generated vector can be used to prove the next result:

Theorem 1.21 *Let V be a vector space of dimension n. Let $S = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m)$ be a sequence of vectors from V. Then the following hold:*

i) If S is linearly independent, then $m \leq n$.

ii) If S spans V, then $m \geq n$.

Suppose now that V is an n-dimensional vector space. Then V is finitely generated and therefore every subspace W of V has a basis and is also finite dimensional. Since a basis of W consists of linearly independent vectors from V we can conclude the following:

Theorem 1.22 *Let W be a subspace of an n-dimensional vector space V. Then the following hold:*

i) $dim(W) \leq n$.

ii) A subspace W of V has dimension n if and only if $W = V$.

You may have noticed in elementary linear algebra that in the space $\mathbb{R}^n$ it was sufficient to check that a sequence $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ is a basis if and only if it is linearly independent if and only if it spans. This is true in general, a result to which we now turn.

Theorem 1.23 *Let V be an n-dimensional vector space and $S = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ be a sequence of vectors from V. Then the following hold:*

i) If S is linearly independent then S spans V and S is a basis of V.

ii) If S spans V then S is linearly independent and S is a basis of V.

Proof *i) Suppose S does not span. Then there is a vector $\boldsymbol{v} \in V, \boldsymbol{v} \notin Span(S)$. But then $S \natural (\boldsymbol{v})$ is linearly independent. However, by Theorem (1.16), it is not possible for an independent sequence to have length $n+1$ and we have a contradiction. Therefore, S spans V and is a basis.*

ii) This is proved similarly and is left as a exercise.

Recall, we previously stated that any spanning sequence in a finitely generated vector space V can be contracted to a basis and any linearly independent set can be expanded to a basis. We state and prove these formally:

Theorem 1.24 *Let V be an n-dimensional vector space and $S = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m)$ a sequence of vectors from V.*

i) If S is linearly independent and $m < n$, then S can be expanded to a basis.

ii) If S spans V and $m > n$, then some subsequence of S is a basis of V.

Proof *i) Let $\mathcal{B} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$ be a linearly independent sequence containing S with k as large as possible. Note that since $m < n$ and S does not span V and there exists a vector $\boldsymbol{v} \in V \setminus Span(S)$. By i) of Theorem (1.15), $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m, \boldsymbol{v})$ is linearly independent and therefore $k > m$. We now claim that $\mathcal{B}$ is a basis. If not, since $\mathcal{B}$ is linearly independent, it must be the case that $\mathcal{B}$ is not a spanning sequence, that is, $Span(\mathcal{B}) \neq V$. However, if $\boldsymbol{w} \in V \setminus Span(\mathcal{B})$, then $\mathcal{B}\sharp(\boldsymbol{w})$ is linearly independent by i) of Theorem (1.15), which contradicts the maximality of the length of $\mathcal{B}$.*

ii) This is left as an exercise.

Theorem 1.25 *Let V be a finite dimensional vector space and U a subspace of V. Then U has a complement in V.*

Proof *This is left as an exercise.*

We complete the section with one more result, which gives a characterization of a basis. We will make use of this result in a subsequent section on coordinates. With the introduction of coordinates with respect to a basis, we will be able to transfer various questions in an abstract vector space to corresponding questions in the space $\mathbb{F}^n$.

Theorem 1.26 *A sequence $\mathcal{B} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$ from the vector space V is a basis of V if and only if for each vector $\boldsymbol{v}$ in V there are unique scalars $c_1, c_2, \ldots, c_k$ such that $\boldsymbol{v} = c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_k\boldsymbol{v}_k$.*

Proof *Suppose $\mathcal{B}$ is a basis and $\boldsymbol{v} \in V$. Since $Span(\mathcal{B}) = V$, there are scalars $c_1, \ldots, c_k$ such that $c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \ldots c_k\boldsymbol{v}_k = \boldsymbol{v}$. By Theorem (1.15), the scalars $c_1, c_2, \ldots, c_k$ are unique.*

Conversely, assume that for every vector $\boldsymbol{v}$ there are unique scalars $c_1, \ldots, c_k$ such that $\boldsymbol{v} = c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_k\boldsymbol{v}_k$. This implies that $\mathcal{B}$ spans V. On the other hand, the hypothesis applies to $\mathbf{0}$. Therefore, there are unique scalars $c_1, \cdots, c_k$ such that $c_1\boldsymbol{v}_1 + \cdots + c_k\boldsymbol{v}_k = \mathbf{0}$. However, $\mathbf{0} = 0\boldsymbol{v}_1 + \cdots + 0\boldsymbol{v}_k$. By the uniqueness assumption, $c_i = 0$ for all $i = 1, 2, \ldots, n$. Therefore $\mathcal{B}$ is linearly independent and it follows that $\mathcal{B}$ is a basis.

Example 1.31 *We have seen that when $\mathbb{K} \subset \mathbb{L}$ is an extension of fields then we can make $\mathbb{L}$ into a vector space over $\mathbb{K}$ by defining addition to be the addition of elements in $\mathbb{L}$ and the scalar multiplication the restriction to $\mathbb{K} \times \mathbb{L}$ of the multiplication in $\mathbb{L}$. The situation where $\mathbb{L}$ is finite dimensional over $\mathbb{K}$ plays an important role in Galois theory. The dimension is usually referred to as the degree of $\mathbb{L}$ over $\mathbb{K}$.*

A particular example is given by $\mathbb{Q} \subset \mathbb{Q}[\sqrt{5}]$. In this case, the degree is 2 and $(1, \sqrt{5})$ is a basis for $\mathbb{Q}[\sqrt{5}]$ over $\mathbb{Q}$.

Exercises

1. Let V be a four-dimensional vector space.

a) Explain why it is not possible to span V with three vectors.

b) Explain why V cannot have a linearly independent set with five vectors.

2. Assume that U and W are distinct subspaces ($U \neq W$) of a four-dimensional vector space V and $dim(U) = dim(W) = 3$. Prove that $dim(U \cap W) = 2$ and $U + W = V$. (Do not invoke Exercise 6).

3. Assume that U and W are subspaces of a vector space V and that $U \cap W = \{\mathbf{0}\}$. Assume that $(\boldsymbol{u}_1, \boldsymbol{u}_2)$ is a basis for U and $(\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}_3)$ is a basis for W. Prove that $(\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}_3)$ is a basis for $U + W$.

4. Prove the second part of Theorem (1.23).

5. Prove the second part of Theorem (1.24).

6. Let V be a finite dimensional vector space and U, W subspaces. Prove that $dim(U + W) + dim(U \cap W) = dim(U) + dim(W)$.

7. Let $dim(V) = 5$. Assume that X and Y are linearly independent sequences of length 3. Prove that $Span(X) \cap Span(Y) \neq \{\mathbf{0}\}$.

8. Assume $dim(V) = n, dim(U) = k, dim(W) = n - k$ and $U + W = V$. Prove that $U \cap W = \{\mathbf{0}\}$ and $V = U \oplus W$.

9. In $\mathbb{F}^6$, give an example of two independent and disjoint sequences of vectors $(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3)$ and $(\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}_3)$ such that:

(a) $Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3) = Span(\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}_3)$.

(b) $dim[Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3) \cap Span(\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}_3)] = 2$.

(c) $dim[Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3) \cap Span(\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}_3)] = 1$.

10. a) Determine how many bases exist for the two-dimensional space $\mathbb{F}_3^2$ over the field $\mathbb{F}_3$.

b) Determine how many bases exist for the two-dimensional space $\mathbb{F}_5^2$ over the field $\mathbb{F}_5$.

c) Let p be a prime. Determine how many bases exist for the two-dimensional space $\mathbb{F}_p^2$ over the field $\mathbb{F}_p$.

11. Prove Theorem (1.25).

12. Assume $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)$ is a spanning sequence of V and W is a proper subspace of V. Prove there exists an i such that $\boldsymbol{v}_i \notin W$.

13. Assume V is an n-dimensionalvector space and X, Y are k-dimensionalsubspaces of V. Prove there exists an $n-k$ dimensional subspace Z of V such that $V = X \oplus Z = Y \oplus Z$.

1.7 Bases and Infinite-Dimensional Vector Spaces

In this section, we complete the proof that every vector space has a basis by extending the result to spaces which are not finitely generated. The key to the proof is Zorn's lemma, which is equivalent to the axiom of choice. We will also show that the cardinalities of any two bases are equal.

What You Need to Know

To make any sense of what we are doing in this section, you will need to have mastered these concepts: vector space over a field $\mathbb{F}$, subspace of a vector space V, linear combination of vectors, span of a sequence or set of vectors, linear dependence, and linear independence of a sequence or set of vectors.

You will also need some familiarity with the concept of a partially ordered set (POSET) and related concepts such as a chain in a POSET, a maximal element in a POSET, and an upper bound for a subset of a POSET. Also, we will make use of results from set theory, specifically the Schroeder–Bernstein theorem. A reasonably good treatment of partially ordered sets, the axiom of choice, Zorn's lemma and the Schroeder–Bernstein theorem can be found in a beginning book on set theory such as *Naive Set Theory* by Paul Halmos ([9]).

We will now show that an arbitrary vector space V has a basis.

Theorem 1.27 *Let V be a vector space over a field $\mathbb{F}$. Assume $I \subset V$ is an independent set and $S \subset V$ is a spanning set. Then there exists $J \subset S$ such that $I \cup J$ is a basis of V.*

Proof *We first deal with the case that I spans V. In this situation, I is a basis and so we can set $J = \emptyset$. Therefore, we may assume that $Span(I) \neq V$. We now create a POSET in the following way:*

Let $\mathcal{X}$ consist of all subsets J of S such that $I \cup J$ is linearly independent. For $J, J' \in X$, we write $J \leq J'$ if and only if $J \subset J'$. We first claim that $\mathcal{X} \neq \{\emptyset\}$. To see this, note that since I is not a basis, it must be the case that $Span(I) \neq V$. On the other hand, if $S \subset Span(I)$, then $V = Span(S) \subset Span(Span(I)) = Span(I)$, a contradiction. Therefore, there exists a vector $\boldsymbol{s} \in S \setminus Span(I)$. We claim that $I \cup \{\boldsymbol{s}\}$ is linearly independent.

Suppose to the contrary that $I \cup \{\boldsymbol{s}\}$ is linearly dependent. Then there is a finite subset K of $I \cup \{\boldsymbol{s}\}$ that is linearly dependent. Among all such subsets, let K_0 be one that is minimal under inclusion. Now if $\boldsymbol{s} \notin K_0$, then $K_0 \subset I$, in which case I is linearly dependent, which contradicts our hypothesis. Therefore $\boldsymbol{s} \in K_0$. Suppose $K_0 = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k, \boldsymbol{s})$ with $\boldsymbol{v}_i \in I$ for $1 \leq i \leq k$. Since K_0 is linearly dependent, there are scalars $c_1, \ldots, c_k, c$ such that

$$c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \dots c_k\boldsymbol{v}_k + c\boldsymbol{s} = \mathbf{0}.$$

Since K_0 is minimal among subsets of $I \cup \{\boldsymbol{s}\}$, which are linearly dependent, all the c_i and c are non-zero. But then we have

$$\boldsymbol{s} = \left(-\frac{c_1}{c}\right)\boldsymbol{v}_1 + \left(-\frac{c_2}{c}\right)\boldsymbol{v}_2 + \cdots + \left(-\frac{c_k}{c}\right)\boldsymbol{v}_k,$$

which implies that $\boldsymbol{s} \in Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k) \subset Span(I)$, a contradiction. Thus, $I \cup \{\boldsymbol{s}\}$ is linearly independent and $\{\boldsymbol{s}\} \in \mathcal{X}$.

We next show that every chain in $\mathcal{X}$ has an upper bound in $\mathcal{X}$. Thus, let $\mathcal{C} = \{J_\alpha | \alpha \in A\}$ be a chain in $\mathcal{X}$. Recall that this means if $\alpha, \beta \in A$ then either $J_\alpha \subset J_\beta$ or $J_\beta \subset J_\alpha$.

Set $J = \cup_{\alpha \in A} J_\alpha$. Clearly, for all $\beta \in A, J_\beta \subset J$ so J is a candidate for an upper bound for $\mathcal{C}$, but we need to know that $J \in \mathcal{X}$. We therefore must prove that $I \cup J$ is linearly independent.

Suppose to the contrary that $I \cup J$ is linearly dependent. Then there is a finite subset K of $I \cup J$, which is linearly dependent. Set $K \cap J = (\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n)$. By the definition of J for each i, there is an $\alpha_i \in A$ such that $\boldsymbol{v}_i \in J_{\alpha_i}$. Since it is easy to see that any finite chain contains an upper bound, there is $k \leq n$ such that $J_{\alpha_i} \subset J_{\alpha_k}$. In particular, $K \cap J \subset J_{\alpha_k}$, and consequently, $K \subset I \cup J_{\alpha_k}$. However, this implies that $I \cup J_{\alpha_k}$ is linearly dependent, which contradicts the assumption that $J_{\alpha_k} \in \mathcal{X}$. Thus, $I \cup J$ is linearly independent as claimed.

We can now invoke Zorn's lemma so that $\mathcal{X}$ contains maximal elements. Thus, let $M \subset S$ be a maximal element of $\mathcal{X}$. We claim that $I \cup M$ is a basis of V. Since $M \in \mathcal{X}$, we know that $I \cup M$ is linearly independent. Therefore, it only remains to show that $I \cup M$ spans V. However, if $Span(I \cup M) \neq V$, then by the argument used at the beginning of the proof there must exist a vector $\boldsymbol{s} \in S$, which is not in $Span(I \cup M)$ and then $(I \cup M) \cup \{\boldsymbol{s}\}$ is linearly independent. But it then follows that $M \cup \{\boldsymbol{s}\}$ is linearly independent, contained in S, and $I \cup [M \cup \{\boldsymbol{s}\}]$ is linearly independent. That is, $M \cup \{\boldsymbol{s}\}$ is in $\mathcal{X}$. However, this contradicts the assumption that M is a maximal element of $\mathcal{X}$. Thus, it must be the case that $Span(I \cup M) = V$ and $I \cup M$ is a basis of V. This completes the proof.

As an immediate corollary, we have:

Corollary 1.3 *Let V be a vector space which is not finitely generated. Then the following hold:*

i) Assume I is an independent subset of V. Then there exists a basis $\mathcal{B}$ of V such that $I \subset \mathcal{B}$. Put another way, every linearly independent subset of a vector space can be extended to a basis.

ii) Assume that S is a spanning set of V. Then there exists a basis $\mathcal{B}$ of V

such that $\mathcal{B} \subset S$. Put another way, any spanning set of a vector space V can be contracted to a basis.

iii) Bases exist in V.

Proof *i) Set $S = V$. Then S is a clearly a spanning set. By Theorem (1.27), there exists a subset $J \subset S = V$ such that $\mathcal{B} = I \cup J$ is a basis of V.*

ii) Let I be the empty set. By Theorem (1.27), there exists a subset J of S such that $I \cup J = \emptyset \cup J = J$ is a basis of V.

iii) Take $I = \emptyset$ and apply i) or take $S = V$ and apply ii) to get a basis in V.

The result from the last section that all bases in a finite dimensional vector space have the same number of elements can be extended to arbitrary spaces in the following sense: If $\mathcal{B}, \mathcal{B}'$ are bases of a vector space V, then there exists a bijection $f : \mathcal{B} \to \mathcal{B}'$. This means the sets $\mathcal{B}$ and $\mathcal{B}'$ have the same cardinality. In what follows below, we will write $\mathcal{B} \preceq \mathcal{B}'$ if there exists an injective function $f : \mathcal{B} \to \mathcal{B}'$.

Theorem 1.28 *Let V be a vector space with bases $\mathcal{B}$ and $\mathcal{B}'$. Then there exists a bijective function $f : \mathcal{B} \to \mathcal{B}'$.*

Proof *If either $\mathcal{B}$ or $\mathcal{B}'$ is finite, then both are finite and have the same number of elements by Theorem (1.20). Therefore, we may assume that both $\mathcal{B}$ and $\mathcal{B}'$ are infinite. We show that $card(\mathcal{B}) \preceq card(\mathcal{B}')$ and $card(\mathcal{B}') \preceq card(\mathcal{B})$.*

Thus, let $\mathcal{B} = \{\boldsymbol{v}_b | b \in B\}$ so that $\mathcal{B}$ and B are sets of the same cardinality. Since $\mathcal{B}'$ is basis, each $\boldsymbol{v}_b \in Span(\mathcal{B}')$. This means that there is a finite subset of vectors $\Omega_b \subset \mathcal{B}'$ such that $\boldsymbol{v}_b \in Span(\Omega_b)$. Set $\Omega = \cup_{b \in B} \Omega_b$. Since $Span(\Omega_b) \subset Span(\Omega)$ and $\boldsymbol{v}_b \in Span(\Omega_b)$, we have for all $b \in B, \boldsymbol{v}_b \in Span(\Omega)$. On the other hand, since $\mathcal{B}$ is a basis, in particular, it is a spanning set. It follows that $Span(\Omega)$ contains a spanning set. But then $Span(\Omega) = Span(Span(\Omega)) = V$ and consequently, Ω is a spanning set. However, Ω is a subset of the basis $\mathcal{B}'$. This implies that $\Omega = \mathcal{B}'$. Thus,

$$\mathcal{B}' = \cup_{b \in B} \Omega_b.$$

Since each Ω_b is finite and B is infinite it follows that $card(\cup_{b \in B} \Omega_b) \preceq card(B) = card(\mathcal{B})$. Therefore, $card(\mathcal{B}') \preceq card(\mathcal{B})$.

By the exact argument, we also have $card(\mathcal{B}) \preceq card(\mathcal{B}')$. It now follows from the Schroeder–Bernstein theorem that $card(\mathcal{B}) = card(\mathcal{B}')$.

Exercises

1. Let X be a set and $\mathbb{F}$ a field. For $Y \subset X$, let $\chi_Y : X \to \mathbb{F}$ be the characteristic function of Y, that is, the function defined by

$$\chi_Y(x) = \begin{cases} 1 & : x \in Y \\ 0 & : x \notin Y. \end{cases}$$

When $Y = \{y\}, y \in X$ let χ_y denote $\chi_{\{y\}}$. Prove that $\{\chi_x | x \in X\}$ is a basis of $\mathcal{M}_{fin}(X, \mathbb{F})$.

2. Show that the cardinality of a basis of $\mathbb{R}$ considered as a vector space over $\mathbb{Q}$ is the same as the cardinality of $\mathbb{R}$.

3. Let V be an infinite dimensional vector space and U a subspace of V. Prove that U has a complement in V.

4. Assume V is an infinite dimensional vector space and n is a natural number. Prove that V has a subspace U such that $dim(V/U) = n$.

1.8 Coordinate Vectors

In this section, we consider a finite dimensional vector space V over a field $\mathbb{F}$ with a basis $\mathcal{B} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ and show how to associate with each vector $\boldsymbol{v} \in V$ an element of $\mathbb{F}^n$.

What You Need to Know

It goes without saying that you need to be familiar with the concepts of a vector space and subspace. More specifically, essential to the understanding of the material in this section are the following: linear combination of a sequence of vectors, a linearly dependent (independent) sequence of vectors, the span of a sequence of vectors, a sequence of vectors S spans a subspace of a vector space, basis of a vector space, and the dimension of a finitely generated vector space.

Recall the following, which was proved for finite dimensional vector spaces in Section (1.6):

Theorem (1.26) A sequence $\mathcal{B} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$ of a vector space V is a basis of V if and only if for each vector $\boldsymbol{v}$ in V there are unique scalars $c_1, c_2, \ldots, c_k$ such that $\boldsymbol{v} = c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_k\boldsymbol{v}_k$.

Example 1.32 *Set* $\boldsymbol{v}_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \boldsymbol{v}_2 = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}, \boldsymbol{v}_3 = \begin{pmatrix} 3 \\ 2 \\ 2 \end{pmatrix}$. *The sequence* $(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3)$ *is a basis of* $\mathbb{R}^3$. *We can write* $\begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$ *uniquely as a linear combination of* $\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3$ *as follows,*

$$\begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} = \boldsymbol{v}_1 + \boldsymbol{v}_2 - \boldsymbol{v}_3.$$

Such an expression is very important and a useful tool for both theory and computation. We therefore give it a name:

Definition 1.29 *Let* $\mathcal{B} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ *be a basis for the vector space* V *and let* $\boldsymbol{v}$ *be a vector in* V. *If* $\boldsymbol{v} = c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_n\boldsymbol{v}_n$, *then the vector* $\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}$, *denoted by* $[\boldsymbol{v}]_{\mathcal{B}}$, *is called the* **coordinate vector** *of* $\boldsymbol{v}$ **with respect to** $\mathcal{B}$.

Remark 1.9 *In general, if $\mathcal{B} \neq \mathcal{B}'$, then $[\boldsymbol{v}]_{\mathcal{B}} \neq [\boldsymbol{v}]_{\mathcal{B}'}$. In particular, this is the case if $\mathcal{B}'$ is obtained from $\mathcal{B}$ by permuting its vectors. This is why we have emphasized that a basis of a finite dimensional vector space is not simply a set of independent vectors that span the vector space V but also has a specific order (and so is a sequence of vectors).*

Example 1.33 *Let $\mathcal{B} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3)$ be the basis of Example (1.32) and $\boldsymbol{v} = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$. then $[\boldsymbol{v}]_{\mathcal{B}} = \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}$.*

On the other hand, if $\mathcal{B}' = (\boldsymbol{v}_1 - \boldsymbol{v}_2, \boldsymbol{v}_2, \boldsymbol{v}_3)$, then $[\boldsymbol{v}]_{\mathcal{B}'} = \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix}$.

If $\mathcal{B}^* = (\boldsymbol{v}_2, \boldsymbol{v}_3, \boldsymbol{v}_1)$, then $[\boldsymbol{v}]_{\mathcal{B}^*} = \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$.

Example 1.34 *Let $f_1(x) = \frac{1}{2}(x-1)(x-2), f_2(x) = -x(x-2)$ and $f_3(x) = \frac{1}{2}x(x-1)$. Then $\mathcal{B} = (f_1, f_2, f_3)$ is a basis for $\mathbb{R}_{(2)}[x]$, the vector space of all polynomials of degree at most two. This basis is quite special: For an arbitrary polynomial $g(x) \in \mathbb{R}_{(2)}[x]$,*

$$[g]_{\mathcal{B}} = \begin{pmatrix} g(0) \\ g(1) \\ g(2) \end{pmatrix}.$$

As a concrete example, let $g(x) = x^2 - x + 1$. Then $g(0) = 1, g(1) = 1, g(2) = 3$. We check:

$$f_1(x) + f_2(x) + 3f_3(x) = \frac{1}{2}(x-1)(x-2) - x(x-2) + \frac{3}{2}x(x-1) = x^2 - x + 1 = g(x).$$

Therefore, $[g]_{\mathcal{B}} = \begin{pmatrix} 1 \\ 1 \\ 3 \end{pmatrix}$, as predicted.

Theorem 1.29 *Let V be a finite dimensional vector space with basis $\mathcal{B} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$. Suppose $\boldsymbol{w}, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ are vectors in V. Then $\boldsymbol{w}$ is a linear combination of $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ if and only if $[\boldsymbol{w}]_{\mathcal{B}}$ is a linear combination of $[\boldsymbol{u}_1]_{\mathcal{B}}, [\boldsymbol{u}_2]_{\mathcal{B}}, \ldots, [\boldsymbol{u}_k]_{\mathcal{B}}$. More precisely, $\boldsymbol{w} = c_1\boldsymbol{u}_1 + c_2\boldsymbol{u}_2 + \cdots + c_k\boldsymbol{u}_k$ if and only if $[\boldsymbol{w}]_{\mathcal{B}} = c_1[\boldsymbol{u}_1]_{\mathcal{B}} + c_2[\boldsymbol{u}_2]_{\mathcal{B}} + \cdots + c_k[\boldsymbol{u}_k]_{\mathcal{B}}$.*

Proof *Suppose*

$$[\boldsymbol{w}]_{\mathcal{B}} = \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix}, [\boldsymbol{u}_1]_{\mathcal{B}} = \begin{pmatrix} u_{11} \\ u_{21} \\ \vdots \\ u_{n1} \end{pmatrix}, \dots [\boldsymbol{u}_k]_{\mathcal{B}} = \begin{pmatrix} u_{1k} \\ u_{2k} \\ \vdots \\ u_{nk} \end{pmatrix}. \tag{1.9}$$

Equation (1.9) can be interpreted to mean

$$\begin{aligned} \boldsymbol{w} &= w_1\boldsymbol{v}_1 + w_2\boldsymbol{v}_2 + \cdots + w_n\boldsymbol{v}_n \\ \boldsymbol{u}_1 &= u_{11}\boldsymbol{v}_1 + u_{21}\boldsymbol{v}_2 + \cdots + u_{n1}\boldsymbol{v}_n \\ &\vdots \\ \boldsymbol{u}_k &= u_{1k}\boldsymbol{v}_1 + u_{2k}\boldsymbol{v}_2 + \cdots + u_{nk}\boldsymbol{v}_n. \end{aligned}$$

Now suppose $\boldsymbol{w} = c_1\boldsymbol{u}_1 + \cdots + c_k\boldsymbol{u}_k$. *Then* $\boldsymbol{w} =$

$$c_1(u_{11}\boldsymbol{v}_1 + u_{21}\boldsymbol{v}_2 + \cdots + u_{n1}\boldsymbol{v}_n) + \cdots + c_k(u_{1k}\boldsymbol{v}_1 + u_{2k} + \cdots + u_{nk}\boldsymbol{v}_n) =$$

$$(c_1u_{11} + c_2u_{12} + \cdots + c_ku_{1k})\boldsymbol{v}_1 + \cdots + (c_1u_{n1} + c_2u_{n2} + \cdots + c_ku_{nk})\boldsymbol{v}_n.$$

Thus,

$$[\boldsymbol{w}]_{\mathcal{B}} = \begin{pmatrix} c_1u_{11} + c_2u_{12} + \cdots + c_ku_{1k} \\ c_1u_{21} + c_2u_{22} + \cdots + c_ku_{2k} \\ \vdots \\ c_1u_{n1} + c_2u_{n2} + \cdots + c_ku_{nk} \end{pmatrix} = c_1\begin{pmatrix} u_{11} \\ u_{21} \\ \vdots \\ u_{n1} \end{pmatrix} + c_2\begin{pmatrix} u_{12} \\ u_{22} \\ \vdots \\ u_{32} \end{pmatrix} + \cdots + c_k\begin{pmatrix} u_{1k} \\ u_{2k} \\ \vdots \\ u_{nk} \end{pmatrix}$$

$$= c_1[\boldsymbol{u}_1]_{\mathcal{B}} + c_2[\boldsymbol{u}_2]_{\mathcal{B}} + \cdots + c_k[\boldsymbol{u}_k]_{\mathcal{B}}.$$

It is straightforward to reverse the argument.

By taking $\boldsymbol{w}$ to be the zero vector, $\mathbf{0}_V$, we get the following:

Theorem 1.30 *Let* V *be a finite dimensional vector space with basis* $\mathcal{B} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n)$. *Let* $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ *be vectors in* V. *Then* $(\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k)$ *is linearly independent if and only if* $([\boldsymbol{u}_1]_{\mathcal{B}}, [\boldsymbol{u}_2]_{\mathcal{B}}, \dots, [\boldsymbol{u}_k]_{\mathcal{B}})$ *is linearly independent. In fact,* $c_1\boldsymbol{u}_1 + \cdots + c_k\boldsymbol{u}_k = \mathbf{0}_V$ *is a dependence relation of* $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$ *if and only if* $c_1[\boldsymbol{u}_1]_{\mathcal{B}} + \cdots + c_k[\boldsymbol{u}_k]_{\mathcal{B}} = \mathbf{0}_n$ *is a dependence relation in* $\mathbb{F}^n$.

Exercises

1. a) Verify that $\mathcal{F} = (1+x, 1+x^2, 1+2x-2x^2)$ is a basis of $\mathbb{F}_{(2)}[x]$.

b) Compute the coordinate vectors $[1]_{\mathcal{F}}, [x]_{\mathcal{F}}, [x^2]_{\mathcal{F}}$.

2. Suppose $\mathcal{B}_1 = (\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3)$ and $\mathcal{B}_2 = (\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3)$ are bases for the three-dimensional vector space V. Let $[\boldsymbol{u}_j]_{\mathcal{B}_2} = \boldsymbol{c}_j$. Suppose $\boldsymbol{x} \in V$ and $[\boldsymbol{x}]_{\mathcal{B}_1} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$. Prove that $[\boldsymbol{x}]_{\mathcal{B}_2} = a_1\boldsymbol{c}_1 + a_2\boldsymbol{c}_2 + a_n\boldsymbol{c}_n$.

3. Let $f_1(x) = -\frac{1}{6}(x-1)(x-2)(x-3), f_2(x) = \frac{1}{2}x(x-2)(x-3), f_3(x) = -\frac{1}{2}x(x-1)(x-3), f_4(x) = \frac{1}{6}x(x-1)(x-2)$.

a) Prove that $\mathcal{F} = (f_1, f_2, f_3, f_4)$ is a basis for $\mathbb{R}_{(3)}[x]$.

b) If $g(X) \in \mathbb{R}_{(3)}[x]$, prove that $[g]_{\mathcal{F}} = \begin{pmatrix} g(0) \\ g(1) \\ g(2) \\ g(3) \end{pmatrix}$.

4. Let $\mathcal{F} = (f_1, f_2, f_3, f_4)$ be the basis of $\mathbb{R}_{(3)}[x]$ from Exercise 3. Compute the coordinate vectors of the *standard basis*, $(1, x, x^2, x^3)$ with respect to $\mathcal{F}$.

5. Let $\mathcal{B}$ be a basis for the finite dimensional vector space V over the field $\mathbb{F}$ and let $(\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k)$ be a sequence of vectors in V. Prove that $Span(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k) = V$ if and only if $Span([\boldsymbol{u}_1]_{\mathcal{B}}, \dots, [\boldsymbol{u}_k]_{\mathcal{B}}) = \mathbb{F}^n$.

6. Let $\mathcal{B}$ be a basis for the n-dimensional vector space V over the field $\mathbb{F}$ and let $(\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n)$ be a sequence of vectors in V. Prove that $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ is a basis for V if and only if $([\boldsymbol{u}_1]_{\mathcal{B}}, \dots, [\boldsymbol{u}_n]_{\mathcal{B}})$ is a basis for $\mathbb{F}^n$.

This page intentionally left blank

2

Linear Transformations

CONTENTS

It is typical in the study of algebra to begin with the definition of its basic objects and investigate their properties. Then it is customary to introduce maps (functions, transformations) between these objects that preserve the algebraic character of the object. The relevant types of maps when the objects are vector spaces are ***linear transformations***. In this chapter, we introduce and begin to develop the theory of linear transformations between vector spaces. In the first section, we define the concept of a linear transformation and give examples. In the second section, we define the ***kernel*** of a linear transformation. We then obtain a criterion for a linear transformation to be injective (one-to-one) in terms of the kernel. In section three, we prove some fundamental theorems about linear transformations, referred to as *isomorphism theorems*. In section four we consider a linear transformation T from an n-dimensional vector space V to an m-dimensional vector space W and show how, using a fixed pair of bases for V and W, respectively, to obtain an $m \times n$ matrix M for the linear transformation. This is used to define addition and multiplication of matrices. In the fifth section, we introduce the notion of an ***algebra*** over a field $\mathbb{F}$ as well as an isomorphism of algebras. We show that for a finite-dimensional vector space V over a field $\mathbb{F}$ the space $\mathcal{L}(V, V)$ of linear operators on V is an algebra over $\mathbb{F}$. We will also introduce the space $M_{nn}(\mathbb{F})$ of $n \times n$ matrices with entries in the field $\mathbb{F}$ and show that this is an algebra isomorphic to $\mathcal{L}(V, V)$ when $dim(V) = n$. In the final section, we study linear transformations that are bijective. We investigate the relationship between two matrices, which arise as the matrix of the same transformation but with respect to different bases for the domain and codomain. This gives rise to the notion of a ***change of basis*** matrix. When the transformation is an operator on a space V this motivates the definition of ***similarity*** of operators and matrices.

2.1 Introduction to Linear Transformations

In this section, we introduce the concept of a linear transformation from one vector space to another and investigate some basic properties.

What You Need to Know

To comprehend the new material of this section, you should have mastered the following concepts: Vector space, dimension of a vector space, finite-dimensional vector space, basis of a vector space, and linear combination of vectors. You should also know what is meant by a function from a set X to a set Y and related concepts such as the domain, codomain, the image of an element, and the range of a function. Consult, if necessary, a good introductory textbook on mathematical proof such as ([20]) or ([6]).

In mathematics, the terms function, transformation, and map are used interchangeably and are synonyms. However, in different areas of mathematics one term predominates while in another area a different usage may be more common. So, in calculus, we typically use the term *function.* In abstract algebra, which deals with groups and rings, we more often use the term *map.* In linear algebra, the common usage is the term *transformation.*

Before plunging into the material we first review some concepts related to the notion of a function.

Definition 2.1 *Let $f : X \to Y$ be a function of a set X into a set Y. The set X is called the* **domain** *of f and Y is the* **codomain***. For an element $x \in X$ the element $f(x)$ of Y is referred to as the* **image** *of x. The* **range** *of f, denoted by Range(f), is the set of all images, Range$(f) := \{f(x)|x \in X\}$. This is also referred to as the* **image of** *f.*

Intuitively, a linear transformation between vector spaces should preserve the algebraic properties of vector spaces, specifically the addition and scalar multiplication. The formal definition follows:

Definition 2.2 *Let V and W be vector spaces over the field $\mathbb{F}$. A* **linear transformation** *$T : V \to W$ is a function (map, transformation), which satisfies the following two conditions:*

i. for every $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V, T(\boldsymbol{v}_1 + \boldsymbol{v}_2) = T(\boldsymbol{v}_1) + T(\boldsymbol{v}_2)$; and

ii. for every $\boldsymbol{v} \in V$ and scalar $c \in \mathbb{F}, T(c\boldsymbol{v}) = cT(\boldsymbol{v})$.

We will denote the collection of all linear maps from V to W by $\mathcal{L}(V, W)$.

Example 2.1 *1. Let V and W be a vectors spaces. For all $\boldsymbol{v} \in V$, define $T(\boldsymbol{v}) = \mathbf{0}_W$. This is the* **zero map** *from V to W and is denoted by $\mathbf{0}_{V \to W}$.*

2. Define $D : \mathbb{F}[x] \to \mathbb{F}[x]$ by

$$D(a_0 + a_1x + \cdots + a_nx^n) = a_1 + 2a_2x + \cdots + na_nx^{n-1}.$$

The map D is called a **derivation** *of $\mathbb{F}[x]$.*

3. Let V and W be vector spaces over the field $\mathbb{F}$. Let $\mathcal{B} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ be a basis for V, $(\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_n)$ a sequence of n vectors in W. Define $T : V \to W$ by $T(a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_n\boldsymbol{v}_n) = a_1\boldsymbol{w}_1 + a_2\boldsymbol{v}_2 + \cdots + a_n\boldsymbol{w}_n$. That this is a linear transformation will be established below in Theorem (2.5).

4. Let F be the collection of functions from $\mathbb{F}$ to $\mathbb{F}$ and $a \in \mathbb{F}$. Define $E_a : F \to \mathbb{F}$ by $E_a(f) = f(a)$. This is called **evaluation at** *a.*

5. Let V be a vector space. Define $I_V : V \to V$ by $I_V(\boldsymbol{v}) = \boldsymbol{v}$ for all $\boldsymbol{v} \in V$. This is the **identity map** *on V.*

6. Let V be a vector space and W a subspace of V. Recall that V/W is the quotient space of V modulo W. Define a map $\pi_{V/W} : V \to V/W$ by $\pi_{V/W}(\boldsymbol{u}) = [\boldsymbol{u}]_W = \boldsymbol{u} + W$. This is a linear transformation called the **quotient map** *of V modulo W.*

Theorem 2.1 *Let $T : V \to W$ be a transformation. Then T is linear if and only if for every pair of vectors $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$ and scalars $c_1, c_2 \in \mathbb{F}$, $T(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2) = c_1T(\boldsymbol{v}_1) + c_2T(\boldsymbol{v}_2)$.*

Proof *Suppose T is a linear transformation and $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V, c_1, c_2 \in \mathbb{F}$. Then $T(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2) = T(c_1\boldsymbol{v}_1) + T(c_2\boldsymbol{v}_2)$ by the first property of a linear transformation. But then $T(c_1\boldsymbol{v}_1) = c_1T(\boldsymbol{v}_1), T(c_2\boldsymbol{v}_2) = c_2T(\boldsymbol{v}_2)$ by the second property, from which it follows that $T(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2) = c_1T(\boldsymbol{v}_1) + c_2T(\boldsymbol{v}_2)$.*

On the other hand, suppose T satisfies the given property. Then, when we take $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V, c_1 = c_2 = 1$, we get $T(\boldsymbol{v}_1 + \boldsymbol{v}_2) = T(\boldsymbol{v}_1) + T(\boldsymbol{v}_2)$, which is the first condition.

Taking $\boldsymbol{v}_1 = \boldsymbol{v}, \boldsymbol{v}_2 = \mathbf{0}, c_1 = c, c_2 = 0$, we get $T(c\boldsymbol{v}) = cT(\boldsymbol{v})$.

Example 2.2 *Let V be a vector space and assume $V = X \oplus Y$ for subspaces X and Y of V. For every $\boldsymbol{v} \in V$, there are unique vectors $\boldsymbol{x} \in X, \boldsymbol{y} \in Y$ such that $\boldsymbol{v} = \boldsymbol{x} + \boldsymbol{y}$. Denote by $Proj_{(X,Y)}(\boldsymbol{v})$ the vector $\boldsymbol{x}$. Then $Proj_{(X,Y)}$ is a linear transformation from V to V. The proof of this is the subject of the next theorem.*

Theorem 2.2 *$Proj_{(X,Y)} : V \to V$ is a linear transformation.*

Proof *Suppose $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$ and c_1, c_2 are scalars. We need to show that $Proj_{(X,Y)}(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2) = c_1 Proj_{(X,Y)}(\boldsymbol{v}_1) + c_2 Proj_{(X,Y)}(\boldsymbol{v}_2)$.*

Let $\boldsymbol{x}_1, \boldsymbol{x}_2 \in X$ and $\boldsymbol{y}_1, \boldsymbol{y}_2 \in Y$ such that

$$\boldsymbol{v}_1 = \boldsymbol{x}_1 + \boldsymbol{y}_1, \boldsymbol{v}_2 = \boldsymbol{x}_2 + \boldsymbol{y}_2. \tag{2.1}$$

By the definition of $Proj_{(X,Y)}$ we have

$$Proj_{(X,Y)}(\boldsymbol{v}_1) = \boldsymbol{x}_1, Proj_{(X,Y)}(\boldsymbol{v}_2) = \boldsymbol{x}_2. \tag{2.2}$$

By (2.1) we have

$$c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 = c_1(\boldsymbol{x}_1 + \boldsymbol{y}_1) + c_2(\boldsymbol{x}_2 + \boldsymbol{y}_2) = (c_1\boldsymbol{x}_1 + c_2\boldsymbol{x}_2) + (c_1\boldsymbol{y}_1 + c_2\boldsymbol{y}_2). \tag{2.3}$$

Since X is a subspace of $V, c_1\boldsymbol{x}_1 + c_2\boldsymbol{x}_2 \in X$ and since Y is a subspace, $c_1\boldsymbol{y}_1 + c_2\boldsymbol{y}_2 \in Y$. By the definition of $Proj_{(X,Y)}$, (2.2), and (2.3) it follows that $Proj_{(X,Y)}(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2) = c_1\boldsymbol{x}_1 + c_2\boldsymbol{x}_2 = c_1 Proj_{(X,Y)}(\boldsymbol{v}_1) + c_2 Proj_{(X,Y)}(\boldsymbol{v}_2)$ as we needed to show.

Definition 2.3 *Assume that $V = X \oplus Y$, the direct sum of the subspaces X and Y. The mapping $Proj_{(X,Y)}$ is called the* **projection map with respect to X and Y**. *It is also called the* **projection map of V onto X relative to Y**.

Remark 2.1 *The ordering of X and Y makes a difference in the definition of $Proj_{(X,Y)}$ and, in fact, $Proj_{(X,Y)} \neq Proj_{(Y,X)}$. Also, the choice of a complement to X makes a difference: If $V = X \oplus Y = X \oplus Z$ with $Y \neq Z$ then $Proj_{(X,Y)} \neq Proj_{(X,Z)}$.*

Theorem 2.3 *Let $T : V \to W$ be a linear transformation. Then the following hold:*

i) $T(\mathbf{0}_V) = \mathbf{0}_W$; and

ii) $T(\boldsymbol{u} - \boldsymbol{v}) = T(\boldsymbol{u}) - T(\boldsymbol{v})$.

Proof *i) Since $\mathbf{0}_V + \mathbf{0}_V = \mathbf{0}_V$, we get*

$$T(\mathbf{0}_V) = T(\mathbf{0}_V + \mathbf{0}_V) = T(\mathbf{0}_V) + T(\mathbf{0}_V).$$

Adding the negative of $T(\mathbf{0}_V)$, to both sides we get

$$\mathbf{0}_W = T(\mathbf{0}_V) + (-T(\mathbf{0}_V)) = [T(\mathbf{0}_V) + T(\mathbf{0}_V)] + (-T(\mathbf{0}_V)) =$$
$$T(\mathbf{0}_V) + [T(\mathbf{0}_V) + (-T(\mathbf{0}_V))] = T(\mathbf{0}_V) + \mathbf{0}_W = T(\mathbf{0}_V).$$

ii) $T(\boldsymbol{u} - \boldsymbol{v}) = T((1)\boldsymbol{u} + (-1)\boldsymbol{v}) = (1)T(\boldsymbol{u}) + (-1)T(\boldsymbol{v}) = T(\boldsymbol{u}) - T(\boldsymbol{v})$ *by Theorem (2.1).*

We next show that the range of a linear transformation $T : V \to W$ is a subspace of W.

Theorem 2.4 *Let* $T : V \to W$ *be a linear transformation. Then Range*(T) *is a subspace of* W.

Proof *Suppose that* $\boldsymbol{w}_1, \boldsymbol{w}_2$ *are in Range*(T) *and* c_1, c_2 *are scalars. We need to show that* $c_1\boldsymbol{w}_1 + c_2\boldsymbol{w}_2 \in$ *Range*(T)*. Now we have to remember what it means to be in Range*(T)*. A vector* $\boldsymbol{w}$ *is in Range*(T) *if there is a vector* $\boldsymbol{v} \in V$ *such that* $T(\boldsymbol{v}) = \boldsymbol{w}$*. Since we are assuming that* $\boldsymbol{w}_1, \boldsymbol{w}_2$ *are in Range*(T)*, there are vectors* $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$ *such that* $T(\boldsymbol{v}_1) = \boldsymbol{w}_1, T(\boldsymbol{v}_2) = \boldsymbol{w}_2$*. Since* V *is a vector space and* $\boldsymbol{v}_1, \boldsymbol{v}_2$ *are in* V *and* c_1, c_2 *are scalars, it follows that* $c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2$ *is a vector in* V*. Now* $T(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2) = c_1T(\boldsymbol{v}_1) + c_2T(\boldsymbol{v}_2) = c_1\boldsymbol{w}_1 + c_2\boldsymbol{w}_2$ *by our criteria for a linear transformation, Theorem 2.1). So,* $c_1\boldsymbol{w}_1 + c_2\boldsymbol{w}_2$ *is the image of the element* $c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2$ *and hence in Range*(T) *as required.*

Lemma 2.1 *Let* $T : V \to W$ *be a linear transformation. Let* $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k$ *be vectors in* V *and* $c_1, c_2, \ldots, c_k$ *be scalars. Then*

$$T(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_k\boldsymbol{v}_k) = c_1T(\boldsymbol{v}_1) + c_2T(\boldsymbol{v}_2) + \cdots + c_kT(\boldsymbol{v}_k). \tag{2.4}$$

Proof *When* $k = 1$*, this is just the second property of a linear transformation and there is nothing to prove. When* $k = 2$ *the result follows from Theorem (2.1).*

The general proof is by mathematical induction on k*. Assume for all* k*-sequences of vectors* $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$ *from* V *and scalars* $(c_1, c_2, \ldots, c_k)$ *that* $T(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_k\boldsymbol{v}_k) = c_1T(\boldsymbol{v}_1) + c_2T(\boldsymbol{v}_2) + \cdots + c_kT(\boldsymbol{v}_k)$.

We must show that this can be extended to $(k + 1)$*-sequences of vectors and scalars. Let* $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k, \boldsymbol{v}_{k+1})$ *be a sequence of vectors from* V *and* $(c_1, c_2, \ldots, c_k, c_{k+1})$ *scalars. Set* $\boldsymbol{u} = c_1\boldsymbol{v}_1 + \cdots + c_k\boldsymbol{v}_k$ *and* $\boldsymbol{w} = c_{k+1}\boldsymbol{v}_{k+1}$*. Then* $T(c_1\boldsymbol{v}_1 + \cdots + c_k\boldsymbol{v}_k + c_{k+1}\boldsymbol{v}_{k+1}) = T(\boldsymbol{u} + \boldsymbol{w}) = T(\boldsymbol{u}) + T(\boldsymbol{w})$ *by the additive property of linear transformations. Thus,*

$$T(c_1\boldsymbol{v}_1 + \cdots + c_k\boldsymbol{v}_k + c_{k+1}\boldsymbol{v}_{k+1}) = T(c_1\boldsymbol{v}_1 + \cdots + c_k\boldsymbol{v}_k) + T(c_{k+1}\boldsymbol{v}_{k+1}).$$

By the inductive hypothesis, $T(c_1\boldsymbol{v}_1+c_2\boldsymbol{v}_2+\cdots+c_k\boldsymbol{v}_k)=c_1T(\boldsymbol{v}_1)+c_2T(\boldsymbol{v}_2)+\cdots+c_kT(\boldsymbol{v}_k)$. *By the scalar property of a linear transformation,* $T(\boldsymbol{w})=T(c_{k+1}\boldsymbol{v}_{k+1})=c_{k+1}T(\boldsymbol{v}_{k+1})$ *and combining these gives the result.*

Theorem 2.5 *Let* V *be an* n*-dimensional vector space over the field* $\mathbb{F}$ *with basis* $\mathcal{B}_V=(\boldsymbol{v}_1,\boldsymbol{v}_2,\ldots,\boldsymbol{v}_n)$ *and* W *a vector space over* $\mathbb{F}$. *Let* $(\boldsymbol{w}_1,\boldsymbol{w}_2,\ldots,\boldsymbol{w}_n)$ *be a sequence of vectors from* W. *Define a function* $T:V\rightarrow W$ *as follows:*

$$T(c_1\boldsymbol{v}_1+c_2\boldsymbol{v}_2+\cdots+c_n\boldsymbol{v}_n)=c_1\boldsymbol{w}_1+c_2\boldsymbol{w}_2+\cdots+c_n\boldsymbol{w}_n. \qquad (2.5)$$

Then T *is a linear transformation. Moreover, every linear transformation from* V *to* W *is defined in this way.*

Proof *It follows from Lemma (2.1) that any linear transformation* T *is defined in this way, so it remains to show that every such* T *is a linear transformation.*

Let c *be a scalar and* $\boldsymbol{v}$ *an arbitrary vector. We need to show that* $T(c\boldsymbol{v})=cT(\boldsymbol{v})$. *Since* $\mathcal{B}$ *is a basis for* V, *there are unique scalars* $c_1,c_2,\ldots,c_n$ *such that* $\boldsymbol{v}=c_1\boldsymbol{v}_1+\ldots c_n\boldsymbol{v}_n$. *Then* $c\cdot\boldsymbol{v}=c\cdot(c_1\boldsymbol{v}_1+\ldots c_n\boldsymbol{v}_n)=(cc_1)\boldsymbol{v}_1+(cc_2)\boldsymbol{v}_2+\ldots(cc_n)\boldsymbol{v}_n$. *By the definition of* T *we have*

$$\begin{aligned}T(c\boldsymbol{v}) &= T((cc_1)\boldsymbol{v}_1+(cc_2)\boldsymbol{v}_2+\ldots(cc_n)\boldsymbol{v}_n)\\ &= (cc_1)\boldsymbol{w}_1+\ldots(cc_n)\boldsymbol{w}_n\\ &= c\cdot(c_1\boldsymbol{w}_1)+\cdots+c\cdot(c_n\boldsymbol{w}_n)\\ &= c\cdot[c_1\boldsymbol{w}_1+\ldots c_n\boldsymbol{w}_n]\\ &= cT(c_1\boldsymbol{v}_1+\ldots c_n\boldsymbol{v}_n)=cT(\boldsymbol{v}).\end{aligned}$$

Now let $\boldsymbol{u},\boldsymbol{v}\in V$. *We must show that* $T(\boldsymbol{u}+\boldsymbol{v})=T(\boldsymbol{u})+T(\boldsymbol{v})$. *Since* $\mathcal{B}$ *is a basis for* V, *there are unique scalars* $(b_1,\ldots,b_n)$ *and* $(c_1,c_2,\ldots,c_n)$ *such that* $\boldsymbol{u}=b_1\boldsymbol{v}_1+\cdots+b_n\boldsymbol{v}_n, \boldsymbol{v}=c_1\boldsymbol{v}_1+\cdots+c_n\boldsymbol{v}_n$. *Then*

$$\boldsymbol{u}+\boldsymbol{v}=(b_1\boldsymbol{v}_1+\cdots+b_n\boldsymbol{v}_n)+(c_1\boldsymbol{v}_1+\cdots+c_n\boldsymbol{v}_n)=$$
$$(b_1+c_1)\boldsymbol{v}_1+\cdots+(b_n+c_n)\boldsymbol{v}_n.$$

As a consequence,

$$\begin{aligned}T(\boldsymbol{u}+\boldsymbol{v}) &= T([b_1+c_1]\boldsymbol{v}_1+\cdots+[b_n+c_n]\boldsymbol{v}_n)\\ &= (b_1+c_1)\boldsymbol{w}_1+\cdots+(b_n+c_n)\boldsymbol{w}_n\\ &= [b_1\boldsymbol{w}_1+c_1\boldsymbol{w}_1]+\cdots+[b_n\boldsymbol{w}_n+c_n\boldsymbol{w}_n\\ &= [b_1\boldsymbol{w}_1+\ldots b_n\boldsymbol{w}_n]+[c_1\boldsymbol{w}_1+\cdots+c_n\boldsymbol{w}_n]\\ &= T(\boldsymbol{u})+T(\boldsymbol{v})\end{aligned}$$

as required.

Putting Lemma (2.1) and Theorem (2.5) together we obtain the following:

Theorem 2.6 *Let V be a finite-dimensional vector space over a field $\mathbb{F}$ with basis $\mathcal{B}_V, W$ an $\mathbb{F}$-vector space, and $(\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_n)$ a sequence of vectors from W. Then there exists a unique linear transformation $T : V \to W$ such that $T(\boldsymbol{v}_j) = \boldsymbol{w}_j$ for $j = 1, 2, \dots, n$.*

Proof *By Lemma (2.1) the only possibility for T is given by $T(c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n) = c_1\boldsymbol{w}_1 + \cdots + c_n\boldsymbol{w}_n$. By Theorem (2.5), T is well defined and a linear transformation.*

It is possible to extend Theorem (2.6) to infinite-dimensional vector spaces. We leave this as an exercise.

Theorem 2.7 *Let V and W be $\mathbb{F}$-vector spaces and $\mathcal{B}$ a basis for V. Then every function $f : \mathcal{B} \to W$ can be extended in a unique way to a linear transformation T from V to W.*

Proof *Since every element of V is a linear combination of finitely many elements of $\mathcal{B}$, it follows from Lemma (2.1) that there is at most one extension. We leave the existence of a linear transformation as an exercise (with extensive hints).*

The significance of Theorem (2.7) is that when $\mathcal{B}$ is a basis of the vector space V then V is ***universal*** among all pairs (f, W) where W is an $\mathbb{F}$-vector space and $f : \mathcal{B} \to W$ is a map. The notion of a universal mapping problem will be more fully developed in the chapter on tensor products.

Let V and W be vector spaces over a field $\mathbb{F}$. We introduce operations of scalar multiplication and addition on the set $\mathcal{L}(V, W)$ in such a way that it becomes a vector space over $\mathbb{F}$.

Definition 2.4 *1) Let $T \in \mathcal{L}(V, W)$ and $c \in \mathbb{F}$. Define $(cT) : V \to W$ by $(cT)(\boldsymbol{v}) = c \cdot T(\boldsymbol{v})$. This is referred to as the* **scalar multiplication** *of T by c.*

2) Let $S, T \in \mathcal{L}(V, W)$. Define $(S+T) : V \to W$ by $(S+T)(\boldsymbol{v}) = S(\boldsymbol{v}) + T(\boldsymbol{v})$. This is the **sum** *of the transformations S and T.*

Lemma 2.2 *i) Let $T \in \mathcal{L}(V,W)$ and c be an element of $\mathbb{F}$. Then $(cT) \in \mathcal{L}(V,W)$.*

ii). Let $S,T \in \mathcal{L}(V,W)$. Then $S+T \in \mathcal{L}(V,W)$.

Proof *i) Let $\boldsymbol{u},\boldsymbol{v} \in V$. Then*

$$(cT)(\boldsymbol{u}+\boldsymbol{v}) = \cdot T(\boldsymbol{u}+\boldsymbol{v}) = c\cdot(T(\boldsymbol{u})+T(\boldsymbol{v})) =$$
$$c\cdot T(\boldsymbol{u}) + c\cdot T(\boldsymbol{v}) = (cT)(\boldsymbol{u}) + (cT)(\boldsymbol{v}).$$

Let $\boldsymbol{u} \in V$ and b a scalar. Then

$$(cT)(b\boldsymbol{u}) = c\cdot T(b\boldsymbol{u}) = c\cdot(b\cdot T(\boldsymbol{u})) = (cb)\cdot T(\boldsymbol{u}) =$$
$$(bc)\cdot T(\boldsymbol{u}) = b\cdot(c\cdot T(\boldsymbol{u})) = b\cdot(cT)(\boldsymbol{u}).$$

This proves that $cT \in \mathcal{L}(V,W)$.

ii) We leave this as an exercise.

Corollary 2.1 *Let V,W be vector spaces over the field $\mathbb{F}$. Then $\mathcal{L}(V,W)$ with the given definitions of addition and scalar multiplication is a vector space.*

Exercises

1. Define $T: \mathbb{F}^3 \to \mathbb{F}_{(2)}[x]$ by $T\begin{pmatrix} a \\ b \\ c \end{pmatrix} = (a+b-2c)+(a-b)x+(a-c)x^2$. Prove that T is a linear transformation.

2. Define $T: \mathbb{F}_{(3)}[x] \to \mathbb{F}^2$ by $T(a_3x^3+a_2x^2+a_1x+a_0) = \begin{pmatrix} a_2a_3 \\ a_0+a_1 \end{pmatrix}$. Show that T is **not** a linear transformation.

3. Define $T: \mathbb{F}^2 \to \mathbb{F}^3$ by $T\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 2a-3b \\ -a+2b \\ 4a+5b \end{pmatrix}$. Prove that T is a linear transformation.

4. Let V be the real two-dimensional vector space of Exercise 11 of Section (1.3). Define $T: \mathbb{R}^2 \to V$ by $T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} e^x \\ e^y \end{pmatrix}$. Prove that T is a linear transformation.

5. Let $S: U \to V$ and $T: V \to W$ be linear transformations. Prove that $T \circ S$ is a linear transformation.

6. Prove part ii) of Lemma (2.2).

In Exercicses 7–8, let V be a vector space over a field F and assume that $V = X \oplus Y$. Set $P_1 = Proj_{(X,Y)}$ and $P_2 = Proj_{(Y,X)}$.

7. Prove the following hold:

a) $P_1 \circ P_1 = P_1, P_2 \circ P_2 = P_2$;
b) $P_1 + P_2 = I_V$; and
c) $P_1 \circ P_2 = P_2 \circ P_1 = \mathbf{0}_{V \to V}$.

8. Let U be a vector space over $\mathbb{F}$ and $T : U \to V$ a map. Assume that $P_1 \circ T$ and $P_2 \circ T$ are linear transformations. Prove that T is a linear transformation.

9. Assume $P_1, P_2 \in \mathcal{L}(V, V)$ satisfy

a) $P_1 + P_2 = I_V$; and
b) $P_1 P_2 = P_2 P_1 = 0_{V \to V}$.

Set $X = Range(P_1), Y = Range(P_2)$. Prove that $V = X \oplus Y$.

10. Assume $dim(V) = n, dim(W) = m$ with $n > m$ and let $T : V \to W$ be a linear transformation. Prove that there exists a nonzero vector $\boldsymbol{v} \in V$ such that $T(\boldsymbol{v}) = \mathbf{0}_W$.

11. Let V be a vector space and W a subspace of V. Prove that the map $\pi_{V/W} : V \to V/W$ given by $\pi_{V/W}(\boldsymbol{v}) = [\boldsymbol{v}]_W = \boldsymbol{v} + W$ is a linear transformation.

12. Let $T : V \to W$ be a linear transformation of vector spaces. Assume $(\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_m)$ is a spanning sequence of W and $\boldsymbol{w}_j \in Range(T)$ for all j. Prove that $Range(T) = W$ so that T is surjective (onto).

13. Let $T : V \to W$ be a linear transformation and $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ a basis for V. Prove that $Range(T) = Span(T(\boldsymbol{v}_1), T(\boldsymbol{v}_2), \ldots, T(\boldsymbol{v}_n))$.

14. Let V be an n-dimensional vector space over $\mathbb{F}$ with basis $\mathcal{B}_V = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ and let W be an m-dimensional space over $\mathbb{F}$ with basis $\mathcal{B}_W = (\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_m)$. Define a map $E_{ij} : V \to W$ by $E_{ij}(c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n) = c_j\boldsymbol{w}_i$. Prove that $\{E_{ij} : 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis for $\mathcal{L}(V, W)$ and therefore $dim(\mathcal{L}(V, W)) = mn$.

15. Prove Theorem (2.7). (See the hints in the appendix at the end of the book.)

16. Assume $T : V \to W$ is a linear transformation, $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)$ a sequence of vectors from V, and set $\boldsymbol{w}_i = T(\boldsymbol{v}_i), i = 1, \ldots, k$. Assume $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k)$ is linearly independent. Prove that $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)$ is linearly independent.

2.2 The Range and Kernel of a Linear Transformation

In this section, we introduce the notion of the kernel of a linear transformation. The kernel of a linear transformation, like the range, is a subspace. We obtain a criterion for a linear transformation to be injective (one-to-one) in terms of the kernel. We demonstrate how the dimensions of the kernel and range are related in the fundamental rank-nullity theorem.

What You Need to Know

For the material of this section to be meaningful, you should understand the following concepts: vector space over a field, subspace of a vector space, span of a sequence or set of vectors, a sequence of vectors spans a subspace of a vector space, a sequence of vectors is linearly dependent/independent, a sequence of vectors is a basis of a vector space, dimension of a vector space, range of a function (map, transformation), surjective function, injective function, and linear transformation. The following are algorithms you should be able to perform: Solve a linear system of equations with coefficients in a field $\mathbb{F}$; given a finite spanning sequence for a subspace of a vector space, find a basis for the subspace and compute the dimension of the subspace.

In order to avoid being repetitious, we will adopt the convention that when we say $T : V \to W$ is a linear transformation it is understood that V and W are vector spaces over a common field.

We begin with a definition:

Definition 2.5 *Let $T : V \to W$ be a linear transformation. The* **kernel** *of T, denoted by $Ker(T)$, consists of all vectors in V which go to the zero vector of W, $Ker(T) := \{\boldsymbol{v} \in V | T(\boldsymbol{v}) = \mathbf{0}_W\}$.*

Recall, we defined the ***range*** of T, denoted by $Range(T)$, to be the set of all images of T: $Range(T) = \{T(\boldsymbol{v})|\boldsymbol{v} \in V\}$. When $T : V \to W$ is a linear transformation, we proved in Theorem (2.4) that $Range(T)$ is a subspace. We now show that $Ker(T)$ is a subspace of V.

Theorem 2.8 *Let $T : V \to W$ be a linear transformation. Then $Ker(T)$ is a subspace of V.*

Proof *Suppose that $\boldsymbol{v}_1, \boldsymbol{v}_2$ are in $Ker(T)$ and c_1, c_2 are scalars. Since we are assuming that $\boldsymbol{v}_1, \boldsymbol{v}_2$ are in $Ker(T)$ this means that $T(\boldsymbol{v}_1) = T(\boldsymbol{v}_2) = \mathbf{0}_W$. Applying T to $c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2$: $T(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2) = c_1T(\boldsymbol{v}_1) + c_2T(\boldsymbol{v}_2) = c_1\mathbf{0}_W + c_2\mathbf{0}_W = \mathbf{0}_W + \mathbf{0}_W = \mathbf{0}_W$. So, $c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2$ is in $Ker(T)$ as required.*

Example 2.3 *1. Let $D : \mathbb{R}_{(3)}[x] \to \mathbb{R}_{(2)}[x]$ be the derivative. Then $Ker(D) = \mathbb{R}$, $Range(D) = \mathbb{R}_{(2)}[x]$.*

2. Let D^2 be the map from the space of twice differentiable functions to $F[\mathbb{R}]$ given by $D^2(f) = \frac{d^2f}{dx^2}$. What is the kernel of $D^2 + I$?

It is the set of all functions that satisfy the second-order differential equation

$$\frac{d^2 f(x)}{dx^2} + f(x) = 0.$$

3. Let V be a four-dimensional vector space with a basis $(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3, \boldsymbol{v}_4)$ and W a three-dimensional vector space with basis $(\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}_3)$ both over the field $\mathbb{F}$. Suppose $T : V \to W$ is a linear transformation and $T(\boldsymbol{v}_1) = \boldsymbol{w}_1, T(\boldsymbol{v}_2) = \boldsymbol{w}_2, T(\boldsymbol{v}_3) = \boldsymbol{w}_3$ and $T(\boldsymbol{v}_4) = c_1\boldsymbol{w}_1 + c_2\boldsymbol{w}_2 + c_3\boldsymbol{w}_3$. Then $Ker(T) = Span(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + c_3\boldsymbol{v}_3 - \boldsymbol{v}_4)$.

Since the range and the kernel of a linear transformation are subspaces, they have dimensions. For future reference, we give names to these dimensions:

Definition 2.6 *Let V and W be vector spaces over the field $\mathbb{F}$ and $T : V \to W$ be a linear transformation. We will refer to the dimension of the range of T as the* **rank of** *T and denote this by $rank(T)$. Thus, $rank(T) = dim(Range(T))$. The dimension of the kernel of T is called the* **nullity of** *T. We denote this by $nullity(T)$. Thus, $nullity(T) = dim(Ker(T))$.*

The next result relates the rank and nullity of a linear transformation when the domain is a finite-dimensional vector space.

Theorem 2.9 (Rank and nullity theorem for linear transformations)

Let V be an n-dimensional vector space and $T : V \to W$ be a linear transformation. Then $n = dim(V) = rank(T) + nullity(T)$.

Proof *Let $k = nullity(T)$. Choose a basis $(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k)$ for $Ker(T)$. Extend this to a basis $(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n)$ for V. We claim two things:*

1) $(T(\boldsymbol{v}_{k+1}), \dots, T(\boldsymbol{v}_n))$ is linearly independent; and 2) $(T(\boldsymbol{v}_{k+1}), \dots, T(\boldsymbol{v}_n))$ spans $Range(T)$.

If both of these are true, then the result will follow since $(T(\boldsymbol{v}_{k+1}), \dots, T(\boldsymbol{v}_n))$ is then a basis for $Range(T)$ and we will have $rank(T) = n - k$ as required. So let us prove the two claims.

1) The first thing we must demonstrate is that

$$Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k) \cap Span(\boldsymbol{v}_{k+1}, \boldsymbol{v}_{k+2}, \dots, \boldsymbol{v}_n) = \{\boldsymbol{0}_V\}.$$

Since $(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n)$ is a basis, in particular, it is linearly independent. Suppose then that $c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \dots c_k\boldsymbol{v}_k = c_{k+1}\boldsymbol{v}_{k+1} + \dots + c_n\boldsymbol{v}_n$ is a vector in the intersection. It follows from this that $c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \dots + c_k\boldsymbol{v}_k - c_{k+1}\boldsymbol{v}_{k+1} - \dots - c_n\boldsymbol{v}_n = \mathbf{0}_V$. Since $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n$ is a basis, we must have $c_1 = c_2 = \dots = c_n = 0$ and therefore $c_1\boldsymbol{v}_1 + \dots + c_k\boldsymbol{v}_k = \mathbf{0}_V$ as claimed.

Suppose now that $c_{k+1}T(\boldsymbol{v}_{k+1}) + \dots + c_nT(\boldsymbol{v}_n) = \mathbf{0}_W$. Since $c_{k+1}T(\boldsymbol{v}_{k+1}) + \dots + c_nT(\boldsymbol{v}_n)$ is the image of $\boldsymbol{u} = c_{k+1}\boldsymbol{v}_{k+1} + \dots + c_n\boldsymbol{v}_n$, the vector $\boldsymbol{u}$ is in $Ker(T)$. But then $c_{k+1}\boldsymbol{v}_{k+1} + \dots + c_n\boldsymbol{v}_n$ is in $Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k)$ and so is in the intersection, $Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k) \cap Span(\boldsymbol{v}_{k+1}, \dots, \boldsymbol{v}_n)$, which we just proved is the trivial subspace $\{\mathbf{0}_V\}$. Therefore, $c_{k+1}\boldsymbol{v}_{k+1} + \dots + c_n\boldsymbol{v}_n = \mathbf{0}_V$. Since the sequence $(\boldsymbol{v}_{k+1}, \dots, \boldsymbol{v}_n)$ is linearly independent it follows that $c_{k+1} = c_{k+2} = \dots = c_n = 0$. Therefore, the sequence $(T(\boldsymbol{v}_{k+1}), T(\boldsymbol{v}_{k+2}), \dots, T(\boldsymbol{v}_n))$ is linearly independent as claimed.

2) Since every vector in V is a linear combination of $(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n)$ it follows that the typical element of the Range(T) is $T(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \dots + c_n\boldsymbol{v}_n) = c_1T(\boldsymbol{v}_1) + c_2T(\boldsymbol{v}_2) + \dots + c_kT(\boldsymbol{v}_k) + c_{k+1}T(\boldsymbol{v}_{k+1}) + \dots c_nT(\boldsymbol{v}_n)$. However, since $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k \in Ker(T)$ this is equal to $c_{k+1}T(\boldsymbol{v}_{k+1}) + \dots c_nT(\boldsymbol{v}_n)$, which is just an element of $Span(T(\boldsymbol{v}_{k+1}), \dots T(\boldsymbol{v}_n))$ as claimed.

Before proceeding to some further results, we review the concept of an injective (one-to-one) function and surjective (onto) function.

Definition 2.7 *Let $f : X \to Y$ be a function. Then f is said to be* **injective** *or* **one-to-one** *if whenever $x \neq x'$, then $f(x) \neq f(x')$. Equivalently, if $f(x) = f(x')$ then $x = x'$. The function f is said to be* **surjective** *or* **onto** *if $Y =$ Range(f). Finally, f is* **bijective** *if it both injective and surjective.*

There is a beautiful criterion for a linear transformation to be injective, which we establish in our next theorem.

Theorem 2.10 *Assume $T : V \to W$ is a linear transformation. Then T is injective if and only if $Ker(T) = \{\mathbf{0}_V\}$.*

Proof *Suppose T is one-to-one. Then there is at most one vector $\boldsymbol{v} \in V$ such that $T(\boldsymbol{v}) = \mathbf{0}_W$. Since $\mathbf{0}_V$ maps to $\mathbf{0}_W$, it follows that $Ker(T) = \{\mathbf{0}_V\}$.*

On the other hand, suppose $Ker(T) = \{\mathbf{0}_V\}$, $\boldsymbol{v}_1, \boldsymbol{v}_2$ are vectors in V, and $T(\boldsymbol{v}_1) = T(\boldsymbol{v}_2)$. We need to prove that $\boldsymbol{v}_1 = \boldsymbol{v}_2$. Since $T(\boldsymbol{v}_1) = T(\boldsymbol{v}_2)$, it follows that $T(\boldsymbol{v}_1) - T(\boldsymbol{v}_2) = \mathbf{0}_W$. But $T(\boldsymbol{v}_1) - T(\boldsymbol{v}_2) = T(\boldsymbol{v}_1 - \boldsymbol{v}_2)$ and consequently $\boldsymbol{v}_1 - \boldsymbol{v}_2 \in Ker(T)$. But then $\boldsymbol{v}_1 - \boldsymbol{v}_2 = \mathbf{0}_V$, whence $\boldsymbol{v}_1 = \boldsymbol{v}_2$ as desired.

Example 2.4 *(1) Let $E : \mathbb{R}_{(2)}[x] \to \mathbb{R}^3$ be the transformation given by $E(f) = \begin{pmatrix} f(1) \\ f(2) \\ f(3) \end{pmatrix}$. This transformation is one-to-one.*

(2) Consider the transformation $T : \mathbb{R}_{(2)}[x] \to \mathbb{R}^2$ given by $T(f) = \begin{pmatrix} f(1) \\ f(2) \end{pmatrix}$. Now, Ker(T) = Span((x − 1)(x − 2)).

The first part of the next theorem indicates how an injective transformation acts on a linearly independent set. The second part gives a criterion for a transformation to be injective in terms of the image of a basis under the transformation.

Theorem 2.11 *i) Let $T : V \to W$ be an injective linear transformation and $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$ a linearly independent sequence from V. Then $(T(\boldsymbol{v}_1), \ldots, T(\boldsymbol{v}_k))$ is linearly independent.*

ii) Assume that $T : V \to W$ is a linear transformation and $\mathcal{B} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ is a basis for V. If $(T(\boldsymbol{v}_1), T(\boldsymbol{v}_2), \ldots, T(\boldsymbol{v}_n))$ is linearly independent then T is injective.

Proof *i) Consider a dependence relation on $(T(\boldsymbol{v}_1), \ldots, T(\boldsymbol{v}_k))$: Suppose for the scalars $c_1, c_2, \ldots, c_k$ that $c_1T(\boldsymbol{v}_1) + c_2T(\boldsymbol{v}_2) + \ldots c_kT(\boldsymbol{v}_k) = \mathbf{0}_W$. We need to show that $c_1 = c_2 = \cdots = c_k = 0$. Because T is a linear transformation, we have*

$$\begin{aligned} T(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_k\boldsymbol{v}_k) &= c_1T(\boldsymbol{v}_1) + c_2T(\boldsymbol{v}_2) + \cdots + c_kT(\boldsymbol{v}_k) \\ &= \mathbf{0}_W. \end{aligned}$$

This implies that the vector $c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_k\boldsymbol{v}_k$ is in $Ker(T)$. However, by hypothesis, $Ker(T) = \{\mathbf{0}_V\}$. Therefore, $c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_k\boldsymbol{v}_k = \mathbf{0}_V$. But we are also assuming that $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$ is linearly independent. Consequently, $c_1 = c_2 = \cdots = c_k = 0$ as required.

ii) Let $\boldsymbol{u} \in Ker(T)$. We must show that $\boldsymbol{u} = \mathbf{0}_V$. Since $\mathcal{B}$ is a basis there are scalars $c_1, c_2, \ldots, c_n$ such that $\boldsymbol{u} = c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_n\boldsymbol{v}_n$. Since $\boldsymbol{u} \in Ker(T), T(\boldsymbol{u}) = \mathbf{0}_W$, by our properties of linear transformations, we can conclude that

$$\begin{aligned} T(\boldsymbol{u}) &= T(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_n\boldsymbol{v}_n) \\ &= c_1T(\boldsymbol{v}_1) + c_2T(\boldsymbol{v}_2) + \cdots + c_nT(\boldsymbol{v}_n) \\ &= \mathbf{0}_W. \end{aligned}$$

However, we are assuming that $(T(\boldsymbol{v}_1), T(\boldsymbol{v}_2), \dots, T(\boldsymbol{v}_n))$ is linearly independent. Consequently $c_1 = c_2 = \cdots = c_n$. Therefore, $\boldsymbol{u} = c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_n\boldsymbol{v}_n = \mathbf{0}_V$ as required.

In some of the examples above, you may have noticed that when $T : V \to W$ is a linear transformation and $dim(V) = dim(W)$ then T injective appears to imply T is surjective and vice versa. This is, indeed, true and the subject of the next theorem.

Theorem 2.12 ("Half is good enough for linear transformations")

Let V and W be n-dimensional vector spaces and $T : V \to W$ be a linear transformation.

i) If T is injective, then T is surjective.
ii) If T is surjective, then T is injective.

Proof *i) Suppose T is injective. Let $(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n)$ be a basis for V. By Theorem (2.11), the sequence $(T(\boldsymbol{v}_1), T(\boldsymbol{v}_2), \dots, T(\boldsymbol{v}_n))$ is linearly independent in W. Since W has dimension n, by Theorem (1.23), $(T(\boldsymbol{v}_1), T(\boldsymbol{v}_2), \dots, T(\boldsymbol{v}_n))$ is a basis for W. Since $Span(T(\boldsymbol{v}_1), T(\boldsymbol{v}_2), \dots, T(\boldsymbol{v}_n)) = Range(T)$, we conclude that T is surjective.*

ii) Assume now that T is surjective. Then $(T(\boldsymbol{v}_1), \dots, T(\boldsymbol{v}_n))$ spans W. By Theorem (1.23), the sequence $(T(\boldsymbol{v}_1), \dots, T(\boldsymbol{v}_n))$ is linearly independent, and then by Theorem (2.11) T is injective.

We give a special name to bijective linear transformations and also to the vector spaces which are connected by such transformations.

Definition 2.8 *If the linear transformation $T : V \to W$ is bijective then we say that T is an* **isomorphism**. *If V and W are vector spaces and there exists an isomorphism $T : V \to W$, we say that V and W are* **isomorphic**.

The next theorem validates the intuition that vector spaces like $\mathbb{F}^4, \mathbb{F}_{(3)}[x]$ are alike (and the tendency to treat them as if they are identical).

Theorem 2.13 *Two finite-dimensional vector spaces V and W are isomorphic if and only if $dim(V) = dim(W)$.*

Proof *If $T : V \to W$ is an isomorphism, then it takes a basis of V to a basis of W and therefore $dim(V) = dim(W)$.*

On the other hand, if $dim(V) = dim(W)$, choose bases $(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n)$ in V and $(\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_n)$ in W and define $T(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \dots c_n\boldsymbol{v}_n) = c_1\boldsymbol{w}_1 + c_2\boldsymbol{w}_2 + \cdots + c_n\boldsymbol{w}_n$.

T is a linear transformation. Suppose some vector $\boldsymbol{u} = c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \dots c_n\boldsymbol{v}_n \in Ker(T)$. Then $c_1\boldsymbol{w}_1 + c_2\boldsymbol{w}_2 + \cdots + c_n\boldsymbol{w}_n = \boldsymbol{0}_W$. However, since $(\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_n)$ is a basis for W, it is linearly independent and it follows that $c_1 = c_2 = \cdots = c_n = 0$. Therefore, $\boldsymbol{u} = \boldsymbol{0}_V$ and thus $Ker(T) = \{\boldsymbol{0}_V\}$. Consequently, T is injective. Since the dimensions are equal by Theorem (2.12), T is an isomorphism.

Example 2.5 *Assume the field $\mathbb{F}$ has at least three elements. If 0, 1, and a are distinct elements of $\mathbb{F}$, then the transformation which takes $f \in \mathbb{F}_{(2)}[x]$ to $\begin{pmatrix} f(0) \\ f(1) \\ f(a) \end{pmatrix}$ is an isomorphism.*

Exercises

1. Let $T : \mathbb{R}^6 \to \mathbb{R}_{(4)}[x]$ be a linear transformation and assume that the following vectors are a basis for $Range(T)$:

$$(1 + x^2 + x^4, x + x^3, 1 + x + 2x^2).$$

What is the rank and nullity of T?

2. Let $a \neq b \in \mathbb{F}$. Define a linear transformation $T : \mathbb{F}_{(3)}[x] \to \mathbb{F}^2$ by $T(f) = \begin{pmatrix} f(a) \\ f(b) \end{pmatrix}$. Describe the kernel of T (find a basis) and determine the rank and nullity of T.

3. Let $T : \mathbb{R}_{(3)}[x] \to \mathbb{R}^4$ be the linear transformation given by

$$T(a + bx + cx^2 + dx^3) = \begin{pmatrix} a + 2b + 2d \\ a + 3b + c + d \\ a + b - c + d \\ a + 2b + 2d \end{pmatrix}.$$

Determine bases for the range and kernel of T and use these to compute the rank and nullity of T.

4. Show that the linear transformation $T : \mathbb{F}^4 \to \mathbb{F}_{(2)}[x]$ given by $T\left(\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}\right) = (a - d) + (b - d)x + (c - d)x^2$ is surjective. Then explain why T is not an isomorphism.

5. Show that the linear transformation $T : \mathbb{F}^3 \to \mathbb{F}_{(3)}[x]$ given by $T\begin{pmatrix} a \\ b \\ c \end{pmatrix} = (a + b) + (b + c)x + (a - 2b - 2c)x^2 + (a + 2b + c)x^3$ is injective. Explain why T is not an isomorphism.

6. Determine whether the map $T : \mathbb{F}_{(2)}[x] \to \mathbb{F}^3$ given by $T(a + bx + cx^2) = \begin{pmatrix} a - b + c \\ a + b + c \\ a + 2b + 4c \end{pmatrix}$ is an isomorphism.

7. Assume that $S : U \to V$ and $T : V \to W$ are both surjective functions. Prove that $T \circ S$ is surjective.

8. Assume that $S : U \to V$ and $T : V \to W$ are both injective functions. Prove that $T \circ S$ is injective.

9. Assume that $S : U \to V$ and $T : V \to W$ are both isomorphisms. Prove that $T \circ S$ is an isomorphism.

10. Assume V and W are finite-dimensional vector spaces and $T : V \to W$ is an isomorphism. Prove that the inverse function $T^{-1} : W \to V$ is a linear transformation.

11. Let V and W be finite-dimensional vector spaces and $T : V \to W$ a linear transformation. Prove that if T is surjective then $dim(V) \geq dim(W)$.

12. Let V and W be finite-dimensional vector spaces and $T : V \to W$ a linear transformation. Prove that if T is injective then $dim(V) \leq dim(W)$.

13. Let V and W be finite-dimensional vector spaces and $T : V \to W$ be a surjective linear transformation. Prove that there is a linear transformation $S : W \to V$ such that $T \circ S = I_W$.

14. Let V and W be finite-dimensional vector spaces and $T : V \to W$ be an injective linear transformation. Prove that there is a linear transformation $S : W \to V$ such that $S \circ T = I_V$.

15. Let V be a finite-dimensional vector space and assume that $T_1, T_2 \in \mathcal{L}(V, V)$ and $Ker(T_1) = Ker(T_2)$. Define a map $R : Range(T_1) \to Range(T_2)$ by $S(T_1(\boldsymbol{v})) = T_2(\boldsymbol{v})$. Prove that R is well-defined and a linear transformation. (Well defined means if $\boldsymbol{v} \in Range(T_1)$ then $S(\boldsymbol{v})$ does not depend on the choice of $\boldsymbol{u} \in V$ such that $\boldsymbol{v} = T_1(\boldsymbol{u})$.)

16. Let V be an n-dimensional vector space over a field $\mathbb{F}$ and T an operator on V. Prove that $Ker(T^n) = Ker(T^{n+1})$ and $Range(T^n) = Range(T^{n+1})$.

17. Let V be an n-dimensional vector space over a field $\mathbb{F}$ and T an operator on V. Prove that $V = Range(T^n) \oplus Ker(T^n)$.

18. Let V be a finite-dimensional vector space over a field $\mathbb{F}$ and T an operator on V. Prove that $Range(T^2) = Range(T)$ if and only if $Ker(T^2) = Ker(T)$.

In Exercises 19 and 20 assume V is a vector space over $\mathbb{F}$ of dimension n and $T : V \to V$ is a linear operator of rank k.

19. a) Let V be an n-dimensional vector space, $S, T \in \mathcal{L}(V, V)$, and $rank(T) = k$. Assume $TS = \mathbf{0}_{V \to V}$. Prove that $rank(S) \leq n - k$. b) Prove that there exists S of rank $n - k$ such that $TS = \mathbf{0}_{V \to V}$.

20. a) Let V be an n-dimensional vector space, $S, T \in \mathcal{L}(V, V)$, and $rank(T) = k$. Assume $ST = \mathbf{0}_{V \to V}$. Prove that $rank(S) \leq n - k$. b) Prove that there exists S of rank $n - k$ such that $TS = \mathbf{0}_{V \to V}$.

21. Assume T is a linear operator on V and $T^2 = \mathbf{0}_{V \to V}$. Prove that $rank(T) \leq \frac{dim(V)}{2}$.

22. Assume V is a vector space with basis $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{2m})$. Give an example of a linear operator T on V of rank m such that $T^2 = \mathbf{0}_{V \to V}$.

2.3 The Correspondence and Isomorphism Theorems

In this section, we prove some fundamental theorems about linear transformations. In particular, we relate the range of a transformation to the quotient space of the domain by the kernel of the transformation.

What You Need to Know

For the material of this section to be meaningful, you should understand the following concepts: vector space over a field, subspace of a vector space, span of a sequence or set of vectors, a sequence of vectors spans a subspace of a vector space, a sequence of vectors is linearly dependent/independent, a sequence of vectors is a basis of a vector space, dimension of a vector space, range of a function (map, transformation), surjective function, injective function, bijective function, linear transformation, kernel of a linear transformation, quotient of a vector space by a subspace, and isomorphism of vector spaces.

Let V be a vector space and U a subspace. We will denote by $Sub(V, U)$ the collection of all subspaces of V that contain U. We also set $Sub(V) = Sub(V, \{\mathbf{0}\})$.

Definition 2.9 *Let $f : A \to B$ be a function and C a subset of B. The* **preimage** *of C is $f^{-1}(C) := \{a \in A | f(a) \in C\}$. In other words, $f^{-1}(C)$ consists of all elements of the domain A which map into C.*

Theorem 2.14 *Let $T : V \to W$ be a linear transformation. Then the following hold:*
i) If X is a subspace of V, then $T(X)$ is a subspace of W.
ii) If Y is a subspace of W, then $T^{-1}(Y)$ is a subspace of V containing $Ker(T)$.
iii) Assume X_1, X_2 are subspaces of V both containing $Ker(T)$. If $T(X_1) = T(X_2)$, then $X_1 = X_2$.

Proof *i) Since $T_{|X} : X \to W$ (T restricted to X) is a linear transformation, this follows from Theorem (2.4) since $T(X)$ is the range of $T_{|X}$.*

ii) Let $\pi_{W/Y} : W \to W/Y$ be the map given by $\pi_{W/Y}(\boldsymbol{w}) = \boldsymbol{w} + Y = [\boldsymbol{w}]_Y$. Then $\pi_{W/Y}$ is a linear transformation. Set $S = \pi_{W/Y} \circ T : V \to W/Y$. Since S is the composition of linear transformations, it is a linear transformation. Note that $Y = Ker(\pi_{W/Y})$. Suppose $T(\boldsymbol{x}) \in Y$. Then $S(\boldsymbol{x}) = \pi_{W/Y}(\boldsymbol{x}) = \mathbf{0}_{W/Y}$. On the other hand, if $\boldsymbol{x} \in Ker(S)$, then $\pi_{W/Y}(T(\boldsymbol{x})) = T(\boldsymbol{x}) + Y = Y$, and, consequently, $T(\boldsymbol{x}) \in Y$. It therefore follows that $T^{-1}(Y) = Ker(S)$. It now *follows from Theorem (2.8) that $T^{-1}(Y)$ is a subspace of V. Moreover, since $\mathbf{0}_W \in Y, Ker(T) = T^{-1}(\{\mathbf{0}_W\}) \subset T^{-1}(Y)$.*

iii) We need to show that $X_1 \subset X_2$ and $X_2 \subset X_1$. Suppose $\boldsymbol{x}_1 \in X_1$. Then $T(\boldsymbol{x}_1) \in T(X_1) = T(X_2)$. Then there exists $\boldsymbol{x}_2 \in X_2$ such that $T(\boldsymbol{x}_1) = T(\boldsymbol{x}_2)$. Then $T(\boldsymbol{x}_1 - \boldsymbol{x}_2) = T(\boldsymbol{x}_1) - T(\boldsymbol{x}_2) = \mathbf{0}_W$. Therefore $\boldsymbol{x}_1 - \boldsymbol{x}_2$ is in $Ker(T)$. Set $\boldsymbol{x}_1 - \boldsymbol{x}_2 = \boldsymbol{v} \in Ker(T)$. Then $\boldsymbol{x}_1 = \boldsymbol{x}_2 + \boldsymbol{v}$. However, since $Ker(T) \subset X_2$, it follows that $\boldsymbol{x}_2 + \boldsymbol{v} \in X_2$. Thus, $\boldsymbol{x}_1 \in X_2$. Since $\boldsymbol{x}_1$ is arbitrary, we conclude that $X_1 \subset X_2$. In exactly the same way, $X_2 \subset X_1$ and we have equality.

When $T : V \to W$ is surjective we can say quite a bit more:

Theorem 2.15 *(***Correspondence Theorem***) Let $T : V \to W$ be a surjective linear transformation. Then the following hold:*
i) If Y is subspace of W, then $T(T^{-1}(Y)) = Y$.
ii) The map $T : Sub(V, Ker(T)) \to Sub(W)$ is bijective and therefore gives a one-to-one correspondence.

Proof *i) Suppose $\boldsymbol{x} \in T^{-1}(Y)$. Then by the definition of $T^{-1}(Y)$, $T(\boldsymbol{x}) \in Y$, and, consequently, $T(T^{-1}(Y)) \subset Y$. On the other hand, since T is surjective, if $\boldsymbol{y} \in Y$, then there exists $\boldsymbol{x} \in V$ such that $T(\boldsymbol{x}) = \boldsymbol{y}$. Since $\boldsymbol{y} \in Y$ clearly $\boldsymbol{x} \in T^{-1}(Y)$. Then $\boldsymbol{y} = T(\boldsymbol{x}) \in T(T^{-1}(Y))$. Since $\boldsymbol{y}$ is arbitrary in Y we conclude that $Y \subset T(T^{-1}(Y))$.*

ii) In part iii) of Theorem (2.14), we proved that map induced by T from $Sub(V, Ker(T)) \to Sub(W)$ is injective. By i) above, it is surjective and, consequently, bijective.

The next theorem will set us up for proving the first isomorphism theorem. More specifically, we prove that when $T : V \to W$ is a linear transformation and X is a subspace of $Ker(T)$, there is a natural way to induce a linear transformation on the quotient space V/X.

Theorem 2.16 *Let $T : V \to W$ be a linear transformation and assume that $X \subset Ker(T)$. Define $\widehat{T} : V/X \to W$ by $\widehat{T}([\boldsymbol{u}]_X) = T(\boldsymbol{u})$. Then $\widehat{T}$ is well defined and a linear transformation.*

Proof *When we say that $\widehat{T}$ is well defined, it means the image, $T([\boldsymbol{u}]_X)$, which is defined on an equivalence class of V modulo X, does not depend on the choice of a representative of the equivalence class. Thus, we have to prove if $\boldsymbol{u} \equiv \boldsymbol{v} \pmod{X}$ then $T(\boldsymbol{u}) = T(\boldsymbol{v})$. If $\boldsymbol{u} \equiv \boldsymbol{v}$, then $\boldsymbol{u} - \boldsymbol{v} \in X \subset Ker(T)$. Then $\mathbf{0}_W = T(\boldsymbol{u} - \boldsymbol{v}) = T(\boldsymbol{u}) - T(\boldsymbol{v})$ from which it follows that $T(\boldsymbol{u}) = T(\boldsymbol{v})$ as required.*

We now prove that $\widehat{T}$ is a linear transformation. We need to prove

1. $\widehat{T}([\boldsymbol{u}]_X + [\boldsymbol{v}]_X) = \widehat{T}([\boldsymbol{u}]_X) + \widehat{T}([\boldsymbol{v}]_X)$; *and*

2. $\widehat{T}(c \cdot [\boldsymbol{u}]_X) = c \cdot \widehat{T}([\boldsymbol{u}]_X)$.

1. $\widehat{T}([\boldsymbol{u}]_X + [\boldsymbol{v}]_X) = \widehat{T}([\boldsymbol{u}+\boldsymbol{v}]_X) = T(\boldsymbol{u}+\boldsymbol{v}) = T(\boldsymbol{u}) + T(\boldsymbol{v}) = \widehat{T}([\boldsymbol{u}]_X) + \widehat{T}([\boldsymbol{v}]_X)$.

2. $\widehat{T}(c \cdot [\boldsymbol{u}]_X) = \widehat{T}([c \cdot \boldsymbol{u}]_X) = T(c \cdot \boldsymbol{u}) = c \cdot T(\boldsymbol{u}) = c \cdot \widehat{T}([\boldsymbol{u}]_X)$.

As a consequence of Theorem (2.16), we can now prove the following:

Theorem 2.17 *(***First Isomorphism Theorem***)* *Let $T : V \to W$ be a linear transformation. Define $\widehat{T} : V/Ker(T) \to W$ by $\widehat{T}([\boldsymbol{u}]_{Ker(T)}) = T(\boldsymbol{u})$. Then $\widehat{T}$ is well defined and an isomorphism of $V/Ker(T)$ onto $Range(T)$.*

Proof *That $\widehat{T}$ is well defined and a linear transformation follows from Theorem (2.16). Clearly $Range(\widehat{T}) = Range(T)$, so when considered as a transformation with codomain $Range(T), \widehat{T}$ is surjective. It remains to show that $\widehat{T}$ is injective. Suppose $\widehat{T}([\boldsymbol{u}]_{Ker(T)}) = \boldsymbol{0}_W$. Then $T(\boldsymbol{u}) = \boldsymbol{0}_W$. It then follows that $\boldsymbol{u} \in Ker(T)$, and, consequently, $[\boldsymbol{u}]_{Ker(T)} = Ker(T) = \boldsymbol{0}_{V/Ker(T)}$. Thus, $\widehat{T}$ is injective and therefore an isomorphism.*

If there is a first isomorphism theorem, then there must be a second. It follows:

Theorem 2.18 (Second Isomorphism Theorem) *Let V be a vector space with subspaces $W \subseteq X$. Then the quotient spaces V/X and $(V/W)/(X/W)$ are isomorphic.*

Proof *Let $T : V \to V/X$ denote the linear transformation given by $T(\boldsymbol{u}) = [\boldsymbol{u}]_X$. Since $W \subset X$, we get an induced transformation $\widehat{T} : V/W \to V/X$ given by $\widehat{T}([\boldsymbol{u}]_W) = T(\boldsymbol{u}) = [\boldsymbol{u}]_X$. Since T is surjective, $\widehat{T}$ is surjective. We determine $Ker(\widehat{T})$: Suppose $[\boldsymbol{u}]_W \in Ker(\widehat{T})$. Then $\widehat{T}([\boldsymbol{u}]_W) = T(\boldsymbol{u}) = [\boldsymbol{u}]_X = \boldsymbol{0}_{V/X} = X$. Therefore, $[\boldsymbol{u}]_W \in Ker(\widehat{T})$ if and only if $\boldsymbol{u} \in X$ and, consequently, $Ker(\widehat{T}) = X/W$. By the First Isomorphism Theorem, V/X is isomorphic to $(V/W)/Ker(\widehat{T}) = (V/W)/(X/W)$ as desired.*

Our final result is often referred to as the **Third Isomorphism Theorem.**

Theorem 2.19 *Let X and W be subspaces of the vector space V. Then $(X + W)/W$ is isomorphic to $X/(X \cap W)$.*

Proof *Let T be the map from $X+W$ to $(X+W)/W$ given by $T(\boldsymbol{u}) = [\boldsymbol{u}]_W$. Let T' denote the restriction of this map to X. We claim first that T' is surjective. Let $[\boldsymbol{u}]_W$ be an arbitrary element of $(X+W)/W$. Then there exists $\boldsymbol{x} \in X$ and $\boldsymbol{w} \in W$ such that $\boldsymbol{u} = \boldsymbol{x} + \boldsymbol{w}$. But then $[\boldsymbol{u}]_W = [\boldsymbol{x}]_W$ from which it follows that $T'(\boldsymbol{x}) = T(\boldsymbol{u}) = [\boldsymbol{u}]_W$. This proves the claim.*

It now follows from the First Isomorphism Theorem that $(X+W)/W$ is isomorphic to $X/Ker(T')$. We determine $Ker(T')$. Suppose $\boldsymbol{x} \in X$ and $T'(\boldsymbol{x}) = [\boldsymbol{x}]_W = \mathbf{0}_{(X+W)/W}$. Then $\boldsymbol{x} \in W$. Since $\boldsymbol{x} \in X$, it follows that $\boldsymbol{x} \in X \cap W$. Consequently, $Ker(T') = X \cap W$. Thus, $X/(X \cap W)$ is isomorphic to $(X+W)/W$ as required.

Exercises

1. Let V be a vector space with subspace W. Suppose $X_1 + W = V = X_2 + W$. Prove that $X_1/(X_1 \cap W)$ is isomorphic to $X_2/(X_2 \cap W)$.

2. Let V be a vector space with subspace W. Suppose X_1, X_2 are complements to W in V. Prove that X_1 and X_2 are isomorphic.

3. Let V be a vector space over the field $\mathbb{F}$ and consider $\mathbb{F}$ to be a vector space over $\mathbb{F}$ of dimension one. Let $f \in \mathcal{L}(V, \mathbb{F}), f \neq \mathbf{0}_{V \to \mathbb{F}}$. Prove that $V/Ker(f)$ is isomorphic to $\mathbb{F}$ as a vector space.

4. Let V be a vector space and $U \neq V, \{\mathbf{0}\}$ a subspace of V. Assume $T \in \mathcal{L}(V,V)$ satisfies the following: a) $T(\boldsymbol{u}) = \boldsymbol{u}$ for all $\boldsymbol{u} \in U$; and b) $T(\boldsymbol{v}) + U = \boldsymbol{v} + U$ for all $\boldsymbol{v} \in V$. Set $S = T - I_V$. Prove that $S^2 = \mathbf{0}_{V \to V}$.

5. Let V be a vector space and assume $S \in \mathcal{L}(V,V)$ is not $\mathbf{0}_{V \to V}$ but $S^2 = \mathbf{0}_{V \to V}$. Set $T = S + I_V$ and $U = Ker(S)$. Prove the following:

a) Let $\boldsymbol{v} \in V$. Then $T(\boldsymbol{v}) = \boldsymbol{v}$ if and only if $\boldsymbol{v} \in U$.

b) $T(\boldsymbol{v}) + U = \boldsymbol{v} + U$ for all $\boldsymbol{v} \in V$.

6. Let U, V be vector spaces with respective subspaces X and Y. Prove that $(U \oplus V)/(X \oplus Y)$ is isomorphic to $(U/X) \oplus (V/Y)$. Here $U \oplus V$ refers to the external direct sum of U and W.

7. Let V be a vector space and $T \in \mathcal{L}(V,V)$ an isomorphism. The ***graph*** of T is the subset $\Gamma := \{(\boldsymbol{v}, T(\boldsymbol{v}))|\boldsymbol{v} \in V\}$. Prove the following:

a) Γ is a subspace of $V \oplus V$; and

b) $(V \oplus V)/\Gamma \cong V$.

8. Let U and W be subspaces of the vector space V and assume that $dim(V/U) = m, dim(V/W) = n$. Prove that $dim(V/(U \cap W)) \leq m + n$.

2.4 Matrix of a Linear Transformation

In this section, we consider a linear transformation T from an n-dimensional vector space V to an m-dimensional vector space W and show how, using a fixed pair of bases from V and W, respectively, to obtain an $m \times n$ matrix M for the linear transformation. In this way we obtain a correspondence between $\mathcal{L}(V, W)$ and the set $M_{mn}(\mathbb{F})$ of all $m \times n$ matrices. This is then used to define addition and multiplication of matrices.

What You Need to Know

For the material of this section to be meaningful, you should understand the following concepts: vector space over a field, subspace of a vector space, span of a sequence or set of vectors, what it means for a sequence of vectors to span a subspace of a vector space, what it means for a sequence of vectors to be linearly dependent/independent, what it means for a sequence of vectors to be a basis of a vector space, the dimension of a vector space, the range of a function (map, transformation), surjective function, injective function, bijective function, linear transformation, and coordinate vector of a vector in a finite-dimensional vector space. The following are algorithms you should be able to perform: Solve a linear system of equations with coefficients in a field $\mathbb{F}$; given a finite spanning sequence for a subspace of a vector space, find a basis for the subspace and compute the dimension of the subspace; and compute the coordinate vector of a vector $\boldsymbol{v}$ in a finite-dimensional vector space V with respect to a basis $\mathcal{B}$ of V.

The notion of a matrix is probably familiar to the reader from elementary linear algebra, however for completeness we introduce this concept as well as some of the related concepts terminology we will use in later sections.

Definition 2.10 *Let $\mathbb{F}$ be a field. A* **matrix** *over $\mathbb{F}$ is defined to be a rectangular array whose entries are elements of $\mathbb{F}$. The sequences of numbers which go across the matrix are called* **rows** *and the sequences of numbers that are vertical are called the* **columns** *of the matrix. If there are m rows and n columns, then it is said to be an m by n matrix and we write this as $m \times n$.*

The numbers which occur in the matrix are called its **entries**. *The one which is found at the intersection of the i^{th} row and the j^{th} column is called the ij^{th} entry, often written as $(i, j)-$entry.*

Of particular importance is the $n \times n$ matrix whose (i, j)-entry is 0 if $i \neq j$ and 1 if $i = j$. This is the $n \times n$ **identity matrix**. *It is denote d by I_n.*

Definition 2.11 *Assume A is an $m \times n$ matrix with $(i, j)-$entry a_{ij}. The* **transpose** *of A, denoted by A^{tr}, is the $n \times m$ matrix whose $(k, l)-$entry is a_{lk}.*

Example 2.6 *Let* $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$. *Then* $A^{tr} = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$.

Let $T : V \to W$ be a linear transformation from an n-dimensional vector space V to an m-dimensional vector space $W, \mathcal{B}_V = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ be a basis for V, and $\mathcal{B}_W = (\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_m)$ be a basis for W.

Then the image $T(\boldsymbol{v}_j)$ of each of the basis vectors $\boldsymbol{v}_j$ can be written in a unique way as a linear combination of $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m)$. Thus, let $a_{ij}, 1 \leq i \leq m$ be the scalars such that $T(\boldsymbol{v}_j) = a_{1j}\boldsymbol{w}_1 + a_{2j}\boldsymbol{w}_2 + \cdots + a_{mj}\boldsymbol{w}_m$, which is the same thing as

$$[T(\boldsymbol{v}_j)]_{\mathcal{B}_W} = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}.$$

Let A be the $m \times n$ matrix whose j^{th} column is $\boldsymbol{a}_j = [T(\boldsymbol{v}_j)]_{\mathcal{B}_W} = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{nj} \end{pmatrix}$ and hence has entries $a_{ij}, 1 \leq i \leq m, 1 \leq j \leq n$. Thus,

$$A = (\boldsymbol{a}_1\ \boldsymbol{a}_2\ \ldots\ \boldsymbol{a}_n) = ([T(\boldsymbol{v}_1)]_{\mathcal{B}_W}\ [T(\boldsymbol{v}_2)]_{\mathcal{B}_W}\ \ldots\ [T(\boldsymbol{v}_n)]_{\mathcal{B}_W}).$$

Now suppose $\boldsymbol{v} \in V$ and $[\boldsymbol{v}]_{\mathcal{B}_V} = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}$, which means that $\boldsymbol{v} = c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_n\boldsymbol{v}_n$. Note that this is the unique expression of $\boldsymbol{v}$ as a linear combination of the basis $\mathcal{B}_V = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$.

By Lemma (2.1)

$$\begin{aligned} T(\boldsymbol{v}) &= T(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_n\boldsymbol{v}_n) \\ &= c_1T(\boldsymbol{v}_1) + c_2T(\boldsymbol{v}_2) + \ldots c_nT(\boldsymbol{v}_n). \end{aligned} \tag{2.6}$$

From (2.6) and Theorem (1.29) it follows that

$$\begin{aligned} [T(\boldsymbol{v})]_{\mathcal{B}_W} &= c_1[T(\boldsymbol{v}_1)]_{\mathcal{B}_W} + c_2[T(\boldsymbol{v}_2)]_{\mathcal{B}_W} + \cdots + c_n[T(\boldsymbol{v}_n)]_{\mathcal{B}_W} \\ &= c_1\boldsymbol{a}_1 + c_2\boldsymbol{a}_2 + \cdots + c_n\boldsymbol{a}_n. \end{aligned}$$

Thus, we can compute the coordinate vector of $T(\boldsymbol{v})$ with respect to $\mathcal{B}_W$ from the coordinate vector of $\boldsymbol{v}$ with respect to $\mathcal{B}_V$ by multiplying the components of $[\boldsymbol{v}]_{\mathcal{B}_V}$ by the corresponding columns of the matrix A.

The matrix $A = (\boldsymbol{a}_1\ \boldsymbol{a}_2\ \dots\ \boldsymbol{a}_n) = ([T(\boldsymbol{v}_1)]_{\mathcal{B}_W}\ [T(\boldsymbol{v}_2)]_{\mathcal{B}_W}\ \dots\ [T(\boldsymbol{v}_n)]_{\mathcal{B}_W})$ is a powerful tool for both computation and theoretic purposes and the subject of the following definition.

Definition 2.12 *Let $T : V \to W$ be a linear transformation from an n-dimensional vector space V to an m-dimensional vector space W, $\mathcal{B}_V = (\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n)$ be a basis for V, and $\mathcal{B}_W = (\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_m)$ a basis for W.*

Let A be the $m \times n$ matrix whose j^{th} column is $\boldsymbol{a}_j = [T(\boldsymbol{v}_j)]_{\mathcal{B}_W} = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{nj} \end{pmatrix}$.

$$A = (\boldsymbol{a}_1\ \boldsymbol{a}_2\ \dots\ \boldsymbol{a}_n) = ([T(\boldsymbol{v}_1)]_{\mathcal{B}_W}\ [T(\boldsymbol{v}_2)]_{\mathcal{B}_W}\ \dots\ [T(\boldsymbol{v}_n)]_{\mathcal{B}_W}).$$

Then A is the **matrix of T with respect to the bases $\mathcal{B}_V$ and $\mathcal{B}_W$**. *We will denote this by $\mathcal{M}_T(\mathcal{B}_V, \mathcal{B}_W)$.*

Remark 2.2 *Let V be an n-dimensional vector space with basis $\mathcal{B}_V = (\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n)$, W an m-dimensional vector space with a basis $\mathcal{B}_W = (\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_m)$. Let $A = (\boldsymbol{a}_1\ \boldsymbol{a}_2\ \dots\ \boldsymbol{a}_n)$ be an arbitrary $m \times n$ matrix. Set* $\boldsymbol{u}_j = a_{1j}\boldsymbol{w}_1 + a_{2j}\boldsymbol{w}_2 + \dots + a_{mj}\boldsymbol{w}_m$ *so that* $[\boldsymbol{u}_j]_{\mathcal{B}_W} = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix} = \boldsymbol{a}_j$. *By Theorem (2.5), there exists a unique linear transformation $T : V \to W$ such that $T(\boldsymbol{v}_j) = \boldsymbol{u}_j$. It is then the case that $\mathcal{M}_T(\mathcal{B}_V, \mathcal{B}_W) = A$. Consequently, every $m \times n$ matrix A is the matrix of some linear transformation from V to W with respect to the bases $\mathcal{B}_V$ and $\mathcal{B}_W$.*

Recall that we have defined operations of addition and scalar multiplication on $\mathcal{L}(V, W)$ in such a way that it becomes a vector space. On the other hand, we presently do not have a definition of addition or scalar multiplication of matrices. We will use the definition for transformations and Remark (2.2) to define addition and scalar multiplication of matrices.

Suppose $A = (\boldsymbol{a}_1\ \boldsymbol{a}_2\ \dots\ \boldsymbol{a}_n)$ is the matrix of $T : V \to W$ with respect to bases $\mathcal{B}_V$ and $\mathcal{B}_W$ and $c \in \mathbb{F}$ is scalar. Then

$$[(cT)(\boldsymbol{v}_j)]_{\mathcal{B}_W} = [c \cdot T(\boldsymbol{v}_j)]_{\mathcal{B}_W} = c[T(\boldsymbol{v}_j)]_{\mathcal{B}_W} = c\boldsymbol{a}_j.$$

It therefore follows that the matrix of cT is the matrix obtained from A by multiplying each entry of A by the scalar c. This motivates our definition of scalar multiplication of a matrix:

Definition 2.13 *Let A be an $m \times n$ matrix and $c \in \mathbb{F}$ a scalar. Then cA is the matrix obtained from A by multiplying each of its entries by c*

$$c\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = \begin{pmatrix} ca_{11} & ca_{12} & \dots & ca_{1n} \\ ca_{21} & ca_{22} & \dots & ca_{2n} \\ \vdots & \vdots & \dots & \vdots \\ ca_{m1} & ca_{m2} & \dots & ca_{mn} \end{pmatrix}.$$

As an immediate consequence of the definition, we have the following:

Theorem 2.20 *Let $\mathcal{B}_V, \mathcal{B}_W$ be bases for V and W, respectively. Let $T \in \mathcal{L}(V, W)$ and $c \in \mathbb{F}$. Then $\mathcal{M}_{cT}(\mathcal{B}_V, \mathcal{B}_W) = c\mathcal{M}_T(\mathcal{B}_V, \mathcal{B}_W)$.*

Now, let $T, S \in \mathcal{L}(V, W)$ and let $A = (\boldsymbol{a}_1\ \boldsymbol{a}_2\ \dots\ \boldsymbol{a}_n) = \mathcal{M}_T(\mathcal{B}_V, \mathcal{B}_W), B = (\boldsymbol{b}_1\ \boldsymbol{b}_2\ \dots\ \boldsymbol{b}_n) = \mathcal{M}_S(\mathcal{B}_V, \mathcal{B}_W)$. We compute the matrix of $T+S$ with respect to the bases $\mathcal{B}_V$ and $\mathcal{B}_W$.

Since $(T+S)(\boldsymbol{v}_j) = T(\boldsymbol{v}_j) + S(\boldsymbol{v}_j)$, we therefore have

$$[(T+S)(\boldsymbol{v}_j)]_{\mathcal{B}_W} = [T(\boldsymbol{v}_j) + S(\boldsymbol{v}_j)]_{\mathcal{B}_W} = [T(\boldsymbol{v}_j)]_{\mathcal{B}_W} + [S(\boldsymbol{v}_j)]_{\mathcal{B}_W} = \boldsymbol{a}_j + \boldsymbol{b}_j.$$

It follows that the matrix of $T+S$ is obtained from the matrices of T and S by adding the corresponding columns and, hence, the corresponding entries. We use this to define the sum of two matrices.

Definition 2.14 *Let* $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ \vdots & \dots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}, B = \begin{pmatrix} b_{11} & \dots & b_{1n} \\ b_{21} & \dots & b_{2n} \\ \vdots & \dots & \vdots \\ b_{m1} & \dots & b_{mn} \end{pmatrix}.$ *Then the* **sum** *of A and B is the matrix obtained by adding the corresponding entries of A and B:*

$$A + B = \begin{pmatrix} a_{11} + b_{11} & \dots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & \dots & a_{2n} + b_{2n} \\ \vdots & \dots & \vdots \\ a_{m1} + b_{m1} & \dots & a_{mn} + b_{mn} \end{pmatrix}.$$

An immediate consequence of the definition is:

Theorem 2.21 *Let $\mathcal{B}_V, \mathcal{B}_W$ be bases for V and W, respectively. Let $T, S \in \mathcal{L}(V, W)$. Then $\mathcal{M}_{T+S}(\mathcal{B}_V, \mathcal{B}_W) = \mathcal{M}_T(\mathcal{B}_V, \mathcal{B}_W) + \mathcal{M}_S(\mathcal{B}_V, \mathcal{B}_W)$.*

We as yet also do not have a definition for multiplication of matrices. We begin by defining the product of an $m \times n$ matrix and an n-vector ($n \times 1$ matrix) and then extend to a product of an $m \times n$ matrix and an $n \times p$ matrix. The definition will be motivated by the relationship between the coordinate vector $[\boldsymbol{v}]_{\mathcal{B}_V}$, the coordinate vector $[T(\boldsymbol{v})]_{\mathcal{B}_W}$, and the matrix of T with respect to $\mathcal{B}_V$ and $\mathcal{B}_W$.

Definition 2.15 *Let A be an $m \times n$ matrix with columns $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n$ and let $\boldsymbol{c} = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}$ be an n-vector. Then the* **product** *of A and $\boldsymbol{c}$ is defined to be*

$$A\boldsymbol{c} = c_1\boldsymbol{a}_1 + c_2\boldsymbol{a}_2 + \cdots + c_n\boldsymbol{a}_n.$$

An immediate consequence of defining the product this way is the following:

Theorem 2.22 *Let V be an n-dimensional vector space with basis $\mathcal{B}_V, W$ an m-dimensional vector space with basis $\mathcal{B}_W$, and $T : V \to W$ a linear transformation. Then for an arbitrary vector $\boldsymbol{v} \in V$*

$$[T(\boldsymbol{v})]_{\mathcal{B}_W} = \mathcal{M}_T(\mathcal{B}_V, \mathcal{B}_W)[\boldsymbol{v}]_{\mathcal{B}_V}.$$

It remains to define a general product of matrices. The definition is again motivated by the properties of the matrix of a linear transformation. We have previously seen in Exercise 15 of Section (2.1) if $T : V \to W$ and $S : W \to X$ are linear transformations then the composition $S \circ T : V \to X$ is a linear transformation. Ideally, if $\mathcal{B}_V, \mathcal{B}_W$, and $\mathcal{B}_X$ are bases for V, W, and X, respectively, then

$$\mathcal{M}_{S \circ T}(\mathcal{B}_V, \mathcal{B}_X) = \mathcal{M}_S(\mathcal{B}_W, \mathcal{B}_X)\mathcal{M}_T(\mathcal{B}_V, \mathcal{B}_W).$$

We therefore investigate the relationship between $\mathcal{M}_S(\mathcal{B}_W, \mathcal{B}_X), \mathcal{M}_T(\mathcal{B}_V, \mathcal{B}_W)$, and $\mathcal{M}_{S \circ T}(\mathcal{B}_V, \mathcal{B}_X)$.

Toward that end, we compute the coordinate vector of $(S \circ T)(\boldsymbol{v}_j)$ with respect to the basis $\mathcal{B}_X$. Let us set $\mathcal{M}_T(\mathcal{B}_V, \mathcal{B}_W) = A$ and $\mathcal{M}_S(\mathcal{B}_W, \mathcal{B}_X) = B$. By the definition of composition

$$(S \circ T)(\boldsymbol{v}_j) = S(T(\boldsymbol{v}_j)).$$

Taking coordinate vectors, we get

$$[(S \circ T)(\boldsymbol{v}_j)]_{\mathcal{B}_X} = [S(T(\boldsymbol{v}_j))]_{\mathcal{B}_X}.$$

By Theorem (2.22), it follows that

$$[S(T(\boldsymbol{v}_j)]_{\mathcal{B}_X} = B[T(\boldsymbol{v}_j)]_{\mathcal{B}_W}.$$

By the definition of $\mathcal{M}_T(\mathcal{B}_V, \mathcal{B}_W)$, it follows that

$$[T(\boldsymbol{v}_j)]_{\mathcal{B}_W} = \boldsymbol{a}_j,$$

and therefore the j^{th} column of $\mathcal{M}_{S\circ T}(\mathcal{B}_V, \mathcal{B}_X)$ is $B\boldsymbol{a}_j$. This is the motivation for the following:

Definition 2.16 *Let A be an $m \times n$ matrix with columns $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n$ and B a $p \times m$ matrix. Then the* **product of** B **and** A *is defined to be the $p \times n$ matrix whose j^{th} column is $B\boldsymbol{a}_j$. Thus,*

$$BA = (B\boldsymbol{a}_1 \ B\boldsymbol{a}_2 \ \dots \ B\boldsymbol{a}_n).$$

As a consequence of this definition, we have:

Theorem 2.23 *Let V be an n-dimensional vector space with basis $\mathcal{B}_V, W$ an m-dimensional vector space with basis $\mathcal{B}_W$, and X a p-dimensional vector space with basis $\mathcal{B}_X$. Let $T : V \to W$ and $S : W \to X$ be linear transformations. Then*

$$\mathcal{M}_{S\circ T}(\mathcal{B}_V, \mathcal{B}_X) = \mathcal{M}_S(\mathcal{B}_W, \mathcal{B}_X)\mathcal{M}_T(\mathcal{B}_V, \mathcal{B}_W). \tag{2.7}$$

We complete this section with a final definition:

Definition 2.17 *Let A be an $m \times n$ matrix with entries in the field $\mathbb{F}$. The* **null space** *of A, denoted by null(A), consists of all vectors $\boldsymbol{v}$ in $\mathbb{F}^n$ such that $A\boldsymbol{v} = \boldsymbol{0}_m \in \mathbb{F}^m$.*

Exercises

In Exercises 1 and 2 assume the following: $T : V \to W$ is a linear transformation, $\mathcal{B}_V = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ is a basis for V, $\mathcal{B}_W = (\boldsymbol{w}_1, \dots, \boldsymbol{w}_m)$ is a basis for W, and $A = \mathcal{M}_T(\mathcal{B}_V, \mathcal{B}_W)$ is the matrix of T with respect to $\mathcal{B}_V$ and $\mathcal{B}_W$.

1. Prove that T is surjective if and only if the columns of A span $\mathbb{F}^m$.

2. Prove that T is injective if and only if the columns of A are linearly independent (as vectors in $\mathbb{F}^m$).

3. Give an example of a 2×2 real matrix A such that $A \neq 0_{2\times 2}$ but $A^2 = 0_{2\times 2}$. Use this to give an example of an operator $T : \mathbb{R}^2 \to \mathbb{R}^2$ such that $T \neq 0_{\mathbb{R}^2 \to \mathbb{R}^2}$ but $T^2 = 0_{\mathbb{R}^2 \to \mathbb{R}^2}$.

4. Give an example of 2×2 real matrices A, B such that $AB \neq 0_{2\times 2}$ but $BA = 0_{2\times 2}$.

5. Assume $T : \mathbb{R}^3 \to \mathbb{R}^3$ is a linear transformation and

$$T\left(\begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, T\left(\begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, T\left(\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Let

$$\mathcal{S} = \left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\right).$$

Determine $\mathcal{M}_T(\mathcal{S}, \mathcal{S})$.

6. Assume $T \in \mathcal{L}(\mathbb{F}^n, \mathbb{F}^m)$. Prove that there is a matrix A such that $T(\boldsymbol{v}) = A\boldsymbol{v}$.

7. Let A be an $m \times n$ matrix with entries in the field $\mathbb{F}$ and assume the sequence consisting of the columns of A spans $\mathbb{F}^m$. Prove that there is an $n \times m$ matrix B such that $AB = I_m$, the $m \times m$ identity matrix.

8. Let A be an $m \times n$ matrix with entries in the field $\mathbb{F}$ and assume the sequence consisting of the columns of A is linearly independent in $\mathbb{F}^m$. Prove that there exists an $n \times m$ matrix B such that $BA = I_n$, the $n \times n$ identity matrix.

9. Show that the columns of the matrix $A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & -1 & 3 \\ 1 & 0 & 3 & -2 \end{pmatrix} \in M_{34}(\mathbb{Q})$ span $\mathbb{Q}^3$. Then find a rational 4×3 matrix B such that $AB = I_3$.

10. Show that the columns of the matrix $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 0 \\ 1 & 2 & 1 \\ 1 & 3 & -1 \end{pmatrix} \in M_{43}(\mathbb{Q})$ are linearly independent in $\mathbb{Q}^4$. Then find a rational 3×4 matrix B such that $BA = I_3$.

11. Let V and W be vector spaces over the field $\mathbb{F}$ with $dim(V) = n, dim(W) = m$ with bases $\mathcal{B}_V$ and $\mathcal{B}_W$, respectively. Assume $T : V \to W$ is a linear transformation and $A = \mathcal{M}_T(\mathcal{B}_V, \mathcal{B}_W)$. Prove that a vector $\boldsymbol{v} \in Ker(T)$ if and only if $[\boldsymbol{v}]_{\mathcal{B}_V} \in null(A)$.

2.5 The Algebra of $\mathcal{L}(V, W)$ and $M_{mn}(\mathbb{F})$

In this section, we will introduce the notion of an algebra over a field $\mathbb{F}$ as well as the concept of an isomorphism of algebras. We will show that for an n-dimensional vector space V over a field $\mathbb{F}$ the space $\mathcal{L}(V, V)$ of operators on V is an algebra over $\mathbb{F}$. We will show that the space $M_{nn}(\mathbb{F})$ of $n \times n$ matrices with entries in the field $\mathbb{F}$ is an algebra isomorphic to $\mathcal{L}(V, V)$.

What You Need to Know

The following concepts are fundamental to understanding the new material in this section: vector space over a field $\mathbb{F}$, basis of a vector space, dimension of a vector space, linear transformation T from a vector space V to a vector space W, the composition of functions, linear operator on a vector space V, an isomorphism from a vector space V to a vector space W, and the matrix of a linear transformation $T : V \to W$ with respect to bases $\mathcal{B}_V$ for V and $\mathcal{B}_W$ for W.

Since we will often refer to the collection of $m \times n$ matrices with entries in a field $\mathbb{F}$, for convenience we give it a symbol and a name:

Definition 2.18 *Let $\mathbb{F}$ be a field and m, n natural numbers. By $M_{mn}(\mathbb{F})$, we shall mean the set of all $m \times n$ matrices with entries in $\mathbb{F}$. This is the* **space of all $m \times n$ matrices***.*

Recall that $\mathcal{L}(V, W)$ consists of all linear transformations $T : V \to W$ and that we have defined scalar multiplication and addition on $\mathcal{L}(V, W)$ as follows:

Scalar Multiplication: For $T \in \mathcal{L}(V, W)$ and $c \in \mathbb{F}$, the transformation $cT : V \to W$ is given by

$$(cT)(\boldsymbol{v}) = c \cdot T(\boldsymbol{v}).$$

Addition: For $T, S \in \mathcal{L}(V, W)$ and $\boldsymbol{v} \in V$

$$(T + S)(\boldsymbol{v}) = T(\boldsymbol{v}) + S(\boldsymbol{v}).$$

With these operations, $\mathcal{L}(V, W)$ has the structure of a vector space over $\mathbb{F}$.

Let V be an n-dimensional vector space with basis $\mathcal{B}_V = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ and W an m-dimensional vector space with basis $\mathcal{B}_W = (\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_m)$. Consider the map $\mu : \mathcal{L}(V, W) \to M_{mn}(\mathbb{F})$ given by $\mu(T) = \mathcal{M}_T(\mathcal{B}_V, \mathcal{B}_W)$. It follows from Remark (2.2) that the map μ is surjective. Moreover, since a linear transformation is uniquely determined by its images on a basis, it follows that the map μ is injective and therefore a bijection.

We defined scalar multiplication of a matrix $A \in M_{mn}(\mathbb{F})$ and $c \in \mathbb{F}$ in such a way that

$$\mu(cT) = c \cdot \mu(T).$$

Likewise, we defined the notion of the sum of matrices A, B in $M_{mn}(\mathbb{F})$ such that

$$\mu(T + S) = \mu(T) + \mu(S).$$

It now follows from this that $M_{mn}(\mathbb{F})$ has the structure of a vector space over $\mathbb{F}$ and as vector spaces $\mathcal{L}(V, W)$ and $M_{mn}(\mathbb{F})$ are isomorphic.

In our next result, we prove that when it is possible to compose linear transformations then associativity holds (in fact, we could prove this holds more generally whenever it is possible to compose functions between sets, however, we will not need this fact). We will then use this to show that matrix multiplication, when it can be performed, is associative.

Theorem 2.24 *Let $V, W, X,$ and Y be spaces with respective dimensions $n, m, l,$ and k and let $T : V \to W, S : W \to X$ and $R : X \to Y$ be linear transformations. Then $R \circ (S \circ T) = (R \circ S) \circ T$.*

Proof *Let $\boldsymbol{v} \in V$. Then $[R \circ (S \circ T)](\boldsymbol{v}) = R((S \circ T)(\boldsymbol{v}) = R(S(T(\boldsymbol{v}))$. On the other hand, $[(R \circ S) \circ T](\boldsymbol{v}) = (R \circ S)(T(\boldsymbol{v})) = R(S(T(\boldsymbol{v}))$, and so we have equality.*

As an immediate consequence of Theorem (2.24), we have:

Theorem 2.25 *Let $A \in M_{mn}(\mathbb{F}), B \in M_{lm}(\mathbb{F})$ and $C \in M_{kl}(\mathbb{F})$. Then $C(BA) = (CB)A$.*

Proof *Let $V, W, X,$ and Y be spaces with respective dimensions $n, m, l,$ and k, and with respective bases $\mathcal{B}_V, \mathcal{B}_W, \mathcal{B}_X,$ and $\mathcal{B}_Y$. Let T be the unique transformation in $\mathcal{L}(V, W)$ such that $\mathcal{M}_T(\mathcal{B}_V, \mathcal{B}_W) = A$; let S be the transformation in $\mathcal{L}(W, X)$ such that $\mathcal{M}_S(\mathcal{B}_W, \mathcal{B}_X) = B$; and R the transformation in $\mathcal{L}(X, Y)$ such that $\mathcal{M}_R(\mathcal{B}_X, \mathcal{B}_Y) = C$. By Theorem (2.24), $R \circ (S \circ T) = (R \circ S) \circ T$. It then follows that $\mathcal{M}_{R \circ (S \circ T)}(\mathcal{B}_V, \mathcal{B}_Y) = \mathcal{M}_{(R \circ S) \circ T}(\mathcal{B}_V, \mathcal{B}_Y)$. By repeated application of Theorem (2.23), we have*

$$\begin{aligned}
\mathcal{M}_{R\circ(S\circ T)}(\mathcal{B}_V,\mathcal{B}_Y) &= \mathcal{M}_R(\mathcal{B}_X,\mathcal{B}_Y)\mathcal{M}_{S\circ T}(\mathcal{B}_V,\mathcal{B}_X)\\
&= \mathcal{M}_R(\mathcal{B}_X,\mathcal{B}_Y)[\mathcal{M}_S(\mathcal{B}_W,\mathcal{B}_X)\mathcal{M}_T(\mathcal{B}_V,\mathcal{B}_W)]\\
&= C(BA).
\end{aligned}$$

On the other hand, again by repeated application of Theorem (2.23), we have

$$\begin{aligned}
\mathcal{M}_{(R\circ S)\circ T}(\mathcal{B}_V,\mathcal{B}_Y) &= \mathcal{M}_{R\circ S}(\mathcal{B}_W,\mathcal{B}_Y)\mathcal{M}_T(\mathcal{B}_V,\mathcal{B}_W)\\
&= [\mathcal{M}_R(\mathcal{B}_X,\mathcal{B}_Y)\mathcal{M}_S(\mathcal{B}_W,\mathcal{B}_X)]\mathcal{M}_T(\mathcal{B}_V,\mathcal{B}_W)\\
&= (CB)A.
\end{aligned}$$

Thus, $C(BA) = (CB)A$ as asserted.

We next show certain distributive properties hold for transformations and then use Theorems (2.21) and (2.23) to show that they hold for matrices.

Theorem 2.26 *Let V, W, and X be vector spaces over the field $\mathbb{F}$ with dimensions n, m, l, respectively.*

i) Let $T_1, T_2 \in \mathcal{L}(V,W)$ and $S \in \mathcal{L}(W,X)$. Then $S\circ(T_1+T_2) = S\circ T_1 + S\circ T_2$.

ii) Let $T \in \mathcal{L}(V,W)$ and $S_1, S_2 \in \mathcal{L}(W,X)$. Then $(S_1+S_2)\circ T = S_1\circ T + S_2\circ T$.

Proof *i) Let $\boldsymbol{v} \in V$. Then $[S\circ(T_1+T_2)](\boldsymbol{v}) = S((T_1+T_2)(\boldsymbol{v}))$ by the definition of composition. $S((T_1+T_2))(\boldsymbol{v})) = S(T_1(\boldsymbol{v})+T_2(\boldsymbol{v}))$ by the definition of T_1+T_2. Then $S(T_1(\boldsymbol{v})+T_2(\boldsymbol{v})) = S(T_1(\boldsymbol{v}_1)) + S(T_2(\boldsymbol{v}))$ by the additive property for linear transformations. However, $S(T_1(\boldsymbol{v})) = (S\circ T_1)(\boldsymbol{v})$ and $S(T_2(\boldsymbol{v})) = (S\circ T_2)(\boldsymbol{v})$. Thus, $[S\circ(T_1+T_2)](\boldsymbol{v}) = [S\circ T_1](\boldsymbol{v}) + [S\circ T_2](\boldsymbol{v})$, and, consequently, $S\circ T_1 + S\circ T_2 = S[T_1+T_2]$.*

ii) This is proved similarly.

We prove the corresponding result for matrix multiplication.

Theorem 2.27 (Distributive Properties of Matrices)

i) Let $A_1, A_2 \in M_{mn}(\mathbb{F})$ and $B \in M_{lm}(\mathbb{F})$. Then $B(A_1+A_2) = BA_1 + BA_2$.

ii) Let $A \in M_{mn}(\mathbb{F})$ and $B_1, B_2 \in M_{lm}(\mathbb{F})$. Then $(B_1+B_2)A = B_1A + B_2A$.

Proof *Because of their similarity, we only write down the proof of i). Let* V, W, X *be vector spaces over* $\mathbb{F}$ *of dimensions* n, m, l*, respectively, and let* $\mathcal{B}_V, \mathcal{B}_W$*, and* $\mathcal{B}_X$ *be bases of the respective spaces. Let* $T_i \in \mathcal{L}(V, W)$ *such that* $\mathcal{M}_{T_i}(\mathcal{B}_V, \mathcal{B}_W) = A_i, i = 1, 2$ *and* $S \in \mathcal{L}(W, X)$ *such that* $\mathcal{M}_S(\mathcal{B}_W, \mathcal{B}_X) = B$*. By Theorem (2.26),* $S \circ (T_1 + T_2) = S \circ T_1 + S \circ T_2$*. It then follows that* $\mathcal{M}_{S\circ(T_1+T_2)}(\mathcal{B}_V, \mathcal{B}_X) = \mathcal{M}_{S\circ T_1 + S\circ T_2}(\mathcal{B}_V, \mathcal{B}_X)$*. By Theorems (2.23) and (2.21), we have*

$$\begin{aligned} \mathcal{M}_{S\circ(T_1+T_2)}(\mathcal{B}_V, \mathcal{B}_X) &= \mathcal{M}_S(\mathcal{B}_W, \mathcal{B}_X)\mathcal{M}_{T_1+T_2}(\mathcal{B}_V, \mathcal{B}_W) \\ &= B(A_1 + A_2). \end{aligned}$$

On the other hand, by Theorem (2.21), we have the equality

$$\mathcal{M}_{S\circ T_1 + S\circ T_2}(\mathcal{B}_V, \mathcal{B}_X) = \mathcal{M}_{S\circ T_1}(\mathcal{B}_V, \mathcal{B}_X) + \mathcal{M}_{S\circ T_2}(\mathcal{B}_V, \mathcal{B}_X).$$

Then by Theorem (2.23), this sum is equal to

$$\mathcal{M}_S(\mathcal{B}_W, \mathcal{B}_X)\mathcal{M}_{T_1}(\mathcal{B}_V, \mathcal{B}_W) + \mathcal{M}_S(\mathcal{B}_W, \mathcal{B}_X)\mathcal{M}_{T_2}(\mathcal{B}_V, \mathcal{B}_W)$$
$$= BA_1 + BA_2.$$

Thus, $B(A_1 + A_2) = BA_1 + BA_2$*.*

For the remainder of this section, assume that V is an n-dimensional vector space over $\mathbb{F}$. We will denote by I_V the identity transformation from V to V. The following theorem enumerates many of the fundamental properties of $\mathcal{L}(V, V)$.

Theorem 2.28 *The following properties hold for* $\mathcal{L}(V, V)$*:*

i) $\mathcal{L}(V, V)$ *with the defined scalar multiplication and addition is a vector space over* $\mathbb{F}$*.*

ii) The product (composition) of any two elements of $\mathcal{L}(V, V)$ *is again an element of* $\mathcal{L}(V, V)$*. This defines a multiplication* $\mathcal{L}(V, V) \times \mathcal{L}(V, V) \to \mathcal{L}(V, V)$*. This multiplication satisfies:*

(a) It is associative: For any $R, S, T \in \mathcal{L}(V, V), (RS)T = R(ST)$*.*

(b) I_V *is a two-sided multiplicative identity element for* $\mathcal{L}(V, V)$*. That is, for any* $T \in \mathcal{L}(V, V), TI_V = I_V T = T$*.*

(c) The right and left distributive laws hold: If $R, S, T \in \mathcal{L}(V, V)$*, then*
$R(S + T) = RS + RT$ *and* $(S + T)R = SR + TR$*.*

(d) For any $R, S \in \mathcal{L}(V, V)$ *and scalar* $c, (cR)S = R(cS) = c(RS)$*.*

By what we have shown, the corresponding properties hold for $M_{nn}(\mathbb{F})$ as well. The next definition provides a context for these properties.

Definition 2.19 *A vector space A over a field $\mathbb{F}$ is said to be an* **associative algebra over** $\mathbb{F}$ *if, in addition to the vector space operations, there is a function $\mu : A \times A \to A$ denoted by $\mu(a, b) = ab$ and referred to as* **multiplication**, *which satisfies the following axioms:*

(M1) Multiplication is associative: For all $a, b, c \in A$, $(ab)c = a(bc)$.

(M2) The right and left distributive property holds: For all $a, b, c \in A$, $(a+b)c = ac + bc$ and $c(a + b) = ca + cb$.

(M3) For all $a, b \in A$ and scalar $\gamma \in \mathbb{F}$, $(\gamma a)b = a(\gamma b) = \gamma(ab)$.

If, in addition, there is an element 1_A such that for all $a \in A, 1_A a = a 1_A = a$, then we say that A is an **algebra with (multiplicative) identity**.

It is clear from the definition that if V is a vector space over a field $\mathbb{F}$, then $\mathcal{L}(V, V)$ is an algebra with identity over $\mathbb{F}$. Likewise, the space of all $n \times n$ matrices, $M_{nn}(\mathbb{F})$, is an algebra over $\mathbb{F}$. Perhaps you have a sense that they are virtually the same algebra, just described differently. This intuition is hopefully put into perspective by the following definition:

Definition 2.20 *Let A and B be algebras over the field $\mathbb{F}$. An* **algebra homomorphism** *from A to B is a linear transformation $\gamma : A \to B$ that additionally satisfies $\gamma(ab) = \gamma(a)\gamma(b)$ for all $a, b \in A$. An* **algebra isomorphism** *from A to B is a homomorphism γ from A to B, which is bijective. When $\gamma : A \to B$ is an isomorphism, we say that the algebras A and B are* **isomorphic**.

We can now state:

Theorem 2.29 *Let V be an n-dimensional vector space over the field $\mathbb{F}$. Then $\mathcal{L}(V, V)$ and $M_{nn}(\mathbb{F})$ are isomorphic $\mathbb{F}$-algebras.*

Algebras arise in many mathematical fields, from group theory and ring theory to functional analysis, differential geometry, and topology, and have applications in many branches of science.

We conclude this section with a couple of definitions that will be referred to in the exercises and in later chapters.

Definition 2.21 *Let a be a nonzero element in an algebra A.*

The element a is a **zero divisor** *if there is a nonzero element b such that either $ab = 0$ or $ba = 0$.*

On the other hand, if A has an identity, the element a is a **unit** *if there is an element b such that $ab = ba = 1$.*

Definition 2.22 *An* **ideal** *in an algebra A with identity is vector subspace I of A which further satisfies: If $r \in A$ and $b \in I$, then $rb \in I$ and $br \in I$. An algebra A is said to be* **simple** *if the only ideals in A are A and $\{\mathbf{0}_A\}$.*

Exercises

1. Assume V is a vector space over the field $\mathbb{F}$ with $dim(V) \geq 2$. Show by example that the multiplication of $\mathcal{L}(V, V)$ is not commutative.

2. Assume V is a vector space over the field $\mathbb{F}$ with $dim(V) \geq 2$. Show by example that there exist zero divisors in $\mathcal{L}(V, V)$.

3. Let A be an algebra with identity over a field $\mathbb{F}$ and $\boldsymbol{a} \in A$. Set $C_A(\boldsymbol{a}) = \{\boldsymbol{b} \in A | \boldsymbol{ab} = \boldsymbol{ba}\}$. This is the ***centralizer of $\boldsymbol{a}$ in** A*. Prove that $C_A(\boldsymbol{a})$ is an algebra with identity.

4. Prove that $M_{nn}(\mathbb{F})$ is a simple algebra, that is, prove that the only ideals in $M_{nn}(\mathbb{F})$ are $\{\mathbf{0}_{nn}\}$ and $M_{nn}(\mathbb{F})$.

5. Let $U_{nn}(\mathbb{F})$ denote the collection of upper triangular matrices with entries in $\mathbb{F}$, that is, all matrices of the form $\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & a_{nn} \end{pmatrix}$. Thus, the (i, j)-entry is zero if $i > j$. Prove that under the definition of addition and multiplication of matrices, $U_{nn}(\mathbb{F})$ is an algebra with identity.

6. Let $\overline{U}_{nn}(\mathbb{F})$ be the collection of strictly upper triangular matrices, that is, the upper triangular matrices with zeros on the diagonal. Prove that $\overline{U}_{nn}(\mathbb{F})$ is an ideal of the algebra $U_{nn}(\mathbb{F})$.

7. Let V be a finite-dimensional vector space over a field $\mathbb{F}$ with $dim(V) \geq 2$. Prove that every nonzero element of $\mathcal{L}(V, V)$ is either a unit or a zero divisor.

2.6 Invertible Transformations and Matrices

In this section, we investigate linear transformations that are bijective. We show that a linear transformation is bijective if and only if it has an inverse (which is also a linear transformation). We investigate the relationship between two matrices that arise as the matrix of the same transformation but with respect to different bases. This gives rise to the notion of a change of basis matrix, which is always invertible. Of particular importance is the situation where the transformation is an operator on a space V and motivates the definition of similar operators and matrices.

What You Need to Know

For the material of this section to be meaningful, you should understand the following concepts: vector space over a field, subspace of a vector space, span of a sequence or set of vectors, a sequence of vectors spans a subspace of a vector space, a sequence of vectors is linearly dependent/independent, a sequence of vectors is a basis of a vector space, dimension of a vector space, range of a function (map, transformation), surjective function, injective function, bijective function, linear transformation, isomorphism of vector spaces, and kernel of a linear transformation.

We begin with a definition:

Definition 2.23 *Let V and W be vector spaces and $T \in \mathcal{L}(V, W)$. By a* **left inverse** *to T we mean a linear transformation $S \in \mathcal{L}(W, V)$ such that $S \circ T = I_V$. By a* **right inverse** *to T we mean a linear transformation $S \in \mathcal{L}(W, V)$ such that $T \circ S = I_W$. By an* **inverse** *to T we mean a linear transformation $S \in \mathcal{L}(W, V)$ such that $S \circ T = I_V, T \circ S = I_W$. When T has an inverse, we say that T is* **invertible**.

In the next lemma, we prove that if a transformation $T \in \mathcal{L}(V, W)$ has a left and a right inverse then they are identical and hence an inverse for T.

Lemma 2.3 *Let $T \in \mathcal{L}(V, W)$. Assume R is a right inverse of T and S is a left inverse of T. Then $R = S$ and T is invertible.*

Proof *Consider $S \circ (T \circ R)$. Since $T \circ R = I_W$, we have $S \circ (T \circ R) = S \circ I_W = S$. On the other hand, by associativity of composition $S \circ (T \circ R) = (S \circ T) \circ R = I_V \circ R = R$. Thus, $R = S$ as claimed.*

The following is an immediate corollary:

Corollary 2.2 *Assume $T \in \mathcal{L}(V, W)$ is invertible. Then T has a unique inverse.*

The next result gives criteria for the existence of left and right inverses of a transformation $T \in \mathcal{L}(V, W)$.

Theorem 2.30 *Assume V and W are finite-dimensional and let $T \in \mathcal{L}(V, W)$. Then the following hold:*

i) T has a left inverse if and only if $Ker(T) = \{\mathbf{0}_V\}$ (if and only if T is injective).

ii) T has a right inverse if and only if $Range(T) = W$ (if and only if T is surjective).

iii) T is invertible if and only if T is bijective.

Proof *i) Assume T has a left inverse S and that $\boldsymbol{v} \in Ker(T)$. Then $T(\boldsymbol{v}) = \mathbf{0}_W$. Now $S \circ T = I_V$ and therefore $(S \circ T)(\boldsymbol{v}) = \boldsymbol{v}$. On the other hand, $(S \circ T)(\boldsymbol{v}) = S(T(\boldsymbol{v})) = S(\mathbf{0}_W) = \mathbf{0}_V$. Thus, $\boldsymbol{v} = \mathbf{0}_V$ and $Ker(T) = \{\mathbf{0}_V\}$, which implies that T is injective.*

Conversely, assume that $Ker(T) = \{\mathbf{0}_V\}$ and therefore that T is injective. Let $\mathcal{B}_V = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ be a basis for V and set $\boldsymbol{w}_i = T(\boldsymbol{v}_i)$ for $i = 1, 2, \ldots, n$. Since T is injective, $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n)$ is linearly independent by Theorem (2.11). Extend $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n)$ to a basis $\mathcal{B}_W = (\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m)$. By Theorem (2.6), there exists a unique linear transformation $S : W \to V$ such that $S(\boldsymbol{w}_i) = \boldsymbol{v}_i$ if $1 \leq i \leq n$ and $S(\boldsymbol{w}_i) = \mathbf{0}_V$ if $n < i \leq m$. Since $(S \circ T)(\boldsymbol{v}_i) = \boldsymbol{v}_i$ for $1 \leq i \leq n$ it follows that $S \circ T = I_V$.

ii) Suppose T has a right inverse S. Let $\boldsymbol{w} \in W$ be arbitrary and set $\boldsymbol{v} = S(\boldsymbol{w})$. Then $T(\boldsymbol{v}) = T(S(\boldsymbol{w})) = (T \circ S)(\boldsymbol{w}) = I_W(\boldsymbol{w}) = \boldsymbol{w}$. Thus, $\boldsymbol{w} \in Range(T)$ and T is surjective.

Conversely, assume that $Range(T) = W$ (so that T is surjective). Let $\mathcal{B}_W$ be a basis for W and for each $\boldsymbol{w} \in \mathcal{B}_W$ choose a vector $\boldsymbol{v} \in V$ such that $T(\boldsymbol{v}) = \boldsymbol{w}$ and denote this vector by $S(\boldsymbol{w})$. This defines a map from the basis $\mathcal{B}_W$ into the vector space V. S extends in a unique way to a linear transformation from W to V. Note that for $\boldsymbol{w} \in \mathcal{B}_W, T(S(\boldsymbol{w})) = \boldsymbol{w}$. This implies that $T \circ S = I_W$.

iii) This follows from i) and ii) and Lemma (2.3).

Theorem 2.31 *Let n be a natural number and assume $dim(V) = dim(W) = n$. Let T be a linear transformation from V to W. Then the following are equivalent:*
i) T is invertible.
ii) $Ker(T) = \{\mathbf{0}_V\}$.
iii) $Range(T) = W$.

Proof *i) implies ii). If T is invertible, then T has, in particular, a right inverse and so by Theorem (2.30) T is injective.*

ii) implies iii). By Theorem (2.10) T is injective. Now the implication follows from Theorem (2.12).

iii) implies i). By Theorem (2.12) T is also injective. Then T has a left inverse and then by Lemma (2.3) an inverse and T is invertible.

This next theorem indicates what happens when we compose two invertible linear transformations. The proof is left as an exercise.

Theorem 2.32 *Let V, W, X be vector spaces over the field $\mathbb{F}$. Assume $S : V \to W$ and $T : W \to X$ are invertible linear transformations. Then $T \circ S : V \to X$ is invertible and $(T \circ S)^{-1} = S^{-1} \circ T^{-1}$.*

Let V be a vector space over a field $\mathbb{F}$. The collection of invertible operators in $\mathcal{L}(V, V)$ will be denoted by $GL(V)$. For S, T invertible operators on V, that is, $S, T \in GL(V)$, define the product, ST, to be the composition $S \circ T$. Theorem (2.32) says that the product belongs to $GL(V)$. Since composition of maps is associative, the product is associative. There exists an identity element, namely, I_V, and each element has an inverse relative to I_V. In the mathematical literature, such an algebraic structure is called a ***group***. We refer to $GL(V)$ as the ***general linear group*** on V.

We now turn our attention to matrices. In what follows, we denote the $n \times n$ identity matrix by I_n.

Definition 2.24 *An $n \times n$ matrix A is is said to be* **invertible** *if there exists an $n \times n$ matrix B such that $AB = BA = I_n$.*

We next characterize invertible matrices:

Theorem 2.33 *Let V, W be n dimensional vector spaces, $\mathcal{B}_V$ and $\mathcal{B}_W$ be bases of V and W, respectively. Let $T \in \mathcal{L}(V, W)$ and set $A = \mathcal{M}_T(\mathcal{B}_V, \mathcal{B}_W)$. Then A is invertible if and only if T is invertible.*

Proof *Assume T is invertible. Let $S \in \mathcal{L}(W,V)$ be the inverse of T and set $B = \mathcal{M}_S(\mathcal{B}_W, \mathcal{B}_V)$. Then $AB = \mathcal{M}_{T\circ S}(\mathcal{B}_V, \mathcal{B}_V) = \mathcal{M}_{I_V}(\mathcal{B}_V, \mathcal{B}_V) = I_n$. In exactly the same way, $BA = I_n$ and therefore A is invertible.*

Conversely, assume that A is invertible and let B be the $n \times n$ matrix such that $AB = BA = I_n$. Let $S \in \mathcal{L}(W,V)$ be the linear transformation such that $\mathcal{M}_S(\mathcal{B}_W, \mathcal{B}_V) = B$. Then $I_n = AB$ is the matrix of $\mathcal{M}_{T\circ S}(\mathcal{B}_W, \mathcal{B}_W)$ and therefore $T \circ S = I_W$. In a similar fashion $S \circ T = I_V$.

Example 2.7 *Let $\mathcal{B} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n)$ and $\mathcal{B}' = (\boldsymbol{v}'_1, \boldsymbol{v}'_2, \dots, \boldsymbol{v}'_n)$ be two bases of the space V. Then the matrix $\mathcal{M}_{I_V}(\mathcal{B}, \mathcal{B}')$ is invertible by Theorem (2.33). Note the j^{th} column of this matrix consists of $[I_V(\boldsymbol{v}_j)]_{\mathcal{B}'} = [\boldsymbol{v}_j]_{\mathcal{B}'}$.*

Definition 2.25 *If $\mathcal{B}, \mathcal{B}'$ are bases of V then $\mathcal{M}_{I_V}(\mathcal{B}, \mathcal{B}')$ is called the* **change of basis matrix from $\mathcal{B}$ to $\mathcal{B}'$**.

Remark 2.3 *Assume that V is an n-dimensional vector space. Then for any basis $\mathcal{B}$ of V, the matrix $\mathcal{M}_{I_V}(\mathcal{B}, \mathcal{B}) = I_n$. Now let $\mathcal{B}, \mathcal{B}'$ be bases for V. Then $I_n = \mathcal{M}_{I_V}(\mathcal{B}, \mathcal{B}) = \mathcal{M}_{I_V}(\mathcal{B}, \mathcal{B}')\mathcal{M}_{I_V}(\mathcal{B}', \mathcal{B})$ and $I_n = \mathcal{M}_{I_V}(\mathcal{B}', \mathcal{B}') = \mathcal{M}_{I_V}(\mathcal{B}', \mathcal{B})\mathcal{M}_{I_V}(\mathcal{B}, \mathcal{B}')$. It follows that the change of basis matrices $\mathcal{M}_{I_V}(\mathcal{B}, \mathcal{B}')$ and $\mathcal{M}_{I_V}(\mathcal{B}', \mathcal{B})$ are inverses of each other.*

The next lemma indicates how the change of basis matrix relates coordinates with respect to different bases. It is an immediate consequence of the definitions.

Lemma 2.4 *Let $\mathcal{B}$ and $\mathcal{B}'$ be bases of the space V and $\boldsymbol{v} \in V$. Then $[\boldsymbol{v}]_{\mathcal{B}'} = \mathcal{M}_{I_V}(\mathcal{B}, \mathcal{B}')[\boldsymbol{v}]_{\mathcal{B}}$*

Proof *Recall, if $T : V \to W$ is a linear transformation with bases $\mathcal{B}_V$ and $\mathcal{B}_W$, respectively, and $\boldsymbol{v} \in V$ then $[T(\boldsymbol{v})]_{\mathcal{B}_W} = \mathcal{M}_T(\mathcal{B}_V, \mathcal{B}_W)[\boldsymbol{v}]_{\mathcal{B}_V}$. The result follows by taking $V = W, \mathcal{B}_V = \mathcal{B}, \mathcal{B}_W = \mathcal{B}'$ and $T = I_V$.*

In this next lemma, we indicate how the matrix of a linear transformation $T : V \to W$ is affected by a change in bases in the spaces V and W.

Lemma 2.5 *Let V be a finite-dimensional vector space with bases $\mathcal{B}_V$ and $\mathcal{B}'_V$, and W a finite-dimensional vector space with bases $\mathcal{B}_W$ and $\mathcal{B}'_W$. Let P be the change of basis matrix $\mathcal{M}_{I_V}(\mathcal{B}_V, \mathcal{B}'_V)$ and Q the change of basis matrix $\mathcal{M}_{I_W}(\mathcal{B}_W, \mathcal{B}'_W)$.*

Let $T : V \to W$ be a linear transformation and set $A = \mathcal{M}_T(\mathcal{B}_V, \mathcal{B}_W)$, the matrix of T with respect to $\mathcal{B}_V$ and $\mathcal{B}_W$ and $B = \mathcal{M}_T(\mathcal{B}'_V, \mathcal{B}'_W)$ the matrix of T with respect to $\mathcal{B}'_V$ and $\mathcal{B}'_W$. Then $B = QAP^{-1}$.

Proof *This follows from*

$$\begin{aligned} B &= \mathcal{M}_T(\mathcal{B}'_V, \mathcal{B}'_W) \\ &= \mathcal{M}_{I_W}(\mathcal{B}_W, \mathcal{B}'_W)\mathcal{M}_T(\mathcal{B}_V, \mathcal{B}_W)\mathcal{M}_{I_V}(\mathcal{B}'_V, \mathcal{B}_V) \\ &= QAP^{-1}. \end{aligned}$$

When T is a linear operator on V, it is customary to use the same basis for the domain and the codomain. In this case, we speak about the matrix of T with respect to a basis $\mathcal{B}$. The following lemma indicates the effect on the matrix of a linear operator when the basis is changed:

Lemma 2.6 *Let V be a finite-dimensional vector space with bases $\mathcal{B}$ and $\mathcal{B}'$. Let $T : V \to V$ be a linear operator. Let $A = \mathcal{M}_T(\mathcal{B}, \mathcal{B})$ be the matrix of T with respect to the basis $\mathcal{B}$ and $B = \mathcal{M}_T(\mathcal{B}', \mathcal{B}')$ the matrix of T with respect to $\mathcal{B}'$. Let $P = \mathcal{M}_{I_V}(\mathcal{B}, \mathcal{B}')$ be the change of basis matrix from $\mathcal{B}$ to $\mathcal{B}'$. Then $B = PAP^{-1}$.*

Proof *This follows from Lemma (2.5) by taking $V = W, \mathcal{B}_V = \mathcal{B}_W = \mathcal{B}$, and $\mathcal{B}'_V = \mathcal{B}'_W = \mathcal{B}'$.*

Definition 2.26 *Two operators $T_1, T_2 \in \mathcal{L}(V, V)$ are said to be* **similar** *if there exists an invertible operator S on V such that $T_2 = ST_1S^{-1}$.*

Definition 2.27 *Two square matrices A and B are said to be* **similar** *if there is an invertible matrix P such that $B = PAP^{-1}$.*

Remark 2.4 *Let $T \in \mathcal{L}(V, V)$ be an operator, $\mathcal{B}, \mathcal{B}'$ bases of V. Then $\mathcal{M}_T(\mathcal{B})$ and $\mathcal{M}_T(\mathcal{B}')$ are similar matrices.*

As we will learn in Chapter 4, similar operators are “structurally” the same. They play an important role in group theory, particularly representation theory. Exercises 11–14 below deal with similar operators and matrices.

Exercises

1. Show that the matrix $\begin{pmatrix} 2 & -3 & 1 \\ -1 & 2 & 0 \\ -1 & 1 & -2 \end{pmatrix}$ is invertible and determine its inverse.

2. Let S be the operator on $\mathbb{R}_{(2)}[x]$ given by

$$S(a + bx + cx^2) = (a + 2b + c) + (2a + 3b + 2c)x + (a + 3b + 2c)x^2.$$

Show that S is invertible by explicitly exhibiting S^{-1}.

3. Let V and W be vector spaces, $\mathcal{B}_V = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ a basis for V, and $T \in \mathcal{L}(V, W)$. Prove that T is invertible if and only if $(T(\boldsymbol{v}_1), T(\boldsymbol{v}_2), \ldots, T(\boldsymbol{v}_n))$ is a basis for W.

4. Let V be a finite-dimensional vector space over a field $\mathbb{F}$. Prove that there is a one-to-one correspondence between the units in $\mathcal{L}(V)$ and the collection of all bases of V.

5. Determine the number of units in $\mathcal{L}(\mathbb{F}_2^3, \mathbb{F}_2^3)$.

6. Determine the number of units in $\mathcal{L}(\mathbb{F}_3^3, \mathbb{F}_3^3)$.

7. Let V be a finite-dimensional vector space over a field $\mathbb{F}$. Assume $T \in \mathcal{L}(V, V), T \neq \mathbf{0}_V$. Prove that either T is invertible or there exists a nonzero operator S such that ST is the zero operator.

8. Prove Theorem (2.32).

9. Let V be a finite-dimensional vector space over the field $\mathbb{F}$ and let $S \in \mathcal{L}(V, V)$ be an invertible operator. Define $\widehat{S} : \mathcal{L}(V, V) \to \mathcal{L}(V, V)$ by $\widehat{S}(T) = S \circ T$. Prove that $\widehat{S}$ is an invertible operator on $\mathcal{L}(V, V)$.

10. An operator $S : V \to V$ is said to be ***nilpotent*** if S^k is the zero map for some natural number k. Prove if S is nilpotent then $I_V - S$ is invertible. (Hint: Consider the product of $I_V - S$ and $(I_V + S + S^2 + \cdots + S^{k-1}$.)

11. Prove that the relation on $\mathcal{L}(V, V)$ given by similarity is an equivalence relation.

12. Assume the operators $T_1, T_2 \in \mathcal{L}(V, V)$ are similar and that $\mathcal{B}$ is a basis of V. Prove that $\mathcal{M}_{T_1}(\mathcal{B}, \mathcal{B})$ and $\mathcal{M}_{T_2}(\mathcal{B}, \mathcal{B})$ are similar matrices.

13. Let $T_1, T_2 \in \mathcal{L}(V, V)$ and $\mathcal{B}$ a basis for V. Assume that $\mathcal{M}_{T_1}(\mathcal{B}, \mathcal{B})$ and $\mathcal{M}_{T_2}(\mathcal{B}, \mathcal{B})$ are similar. Prove that T_1 and T_2 are similar.

14. Let $T_1, T_2 \in \mathcal{L}(V, V)$ and $\mathcal{B}, \mathcal{B}'$ be bases for V. Assume that $\mathcal{M}_{T_1}(\mathcal{B}, \mathcal{B})$ and $\mathcal{M}_{T_2}(\mathcal{B}', \mathcal{B}')$ are similar matrices. Prove that operators T_1 and T_2 are similar.

3

Polynomials

CONTENTS

In this chapter, we build on high school algebra and develop the algebraic theory of polynomials. In section one we show that under the usual operations of addition and multiplication the collection of all polynomials with coefficients in a field $\mathbb{F}$ is a commutative algebra with identity. We define the concepts of greatest common divisor (gcd) and least common multiple (lcm) of two polynomials and make use of the division algorithm (division with remainders) to establish the existence and uniqueness of the gcd and lcm. In section two we prove some general results about roots of polynomials and then specialize to polynomials with coefficients in the fields $\mathbb{R}$ and $\mathbb{C}$.

3.1 The Algebra of Polynomials

What You Need to Know

Elementary properties of polynomials, such as how to add and multiply polynomials and how to compute the quotient and remainder when one polynomial is divided by another.

We begin by recalling the definition of a polynomial in a variable x and introduce some notation and terminology which will facilitate the discussion.

Definition 3.1 *Let $\mathbb{F}$ be a field. By a* **polynomial with coefficients in** $\mathbb{F}$, *we mean an expression of the form $a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$, where $a_i \in \mathbb{F}$ and x is an abstract symbol called an* **indeterminate or variable**. *The scalars a_i are the coefficients of the polynomial $f(x)$. The* **zero polynomial** *is the polynomial all of whose coefficients are zero. We denote this by 0.*

Suppose $f(x) \neq 0$. The largest natural number k such that the coefficient a_k is not zero is called the **degree** *of $f(x)$ and the term $a_k x^k$ is called the* **leading term**. *If the coefficient of the leading term is 1 we say the polynomial $f(x)$ is* **monic**.

We will denote by $\mathbb{F}[x]$ the collection of all polynomials with entries in $\mathbb{F}$ and by $\mathbb{F}_{(m)}[x]$ all polynomials of degree at most m.

We define the sum of two polynomials.

Definition 3.2 *Let $f(x)$ and $g(x)$ be two polynomials of degree k and l, respectively. Set $m = max\{k, l\}$ so that both $f(x)$ and $g(x)$ are in $\mathbb{F}_{(m)}[x]$. We can then write them as $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ and $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$. Then the* **sum of** *$f(x)$ and $g(x)$ is*

$$f(x)+g(x) = (a_m+b_m)x^m+(a_{m-1}+b_{m-1})x^{m-1}+\cdots+(a_1+b_1)x+(a_0+b_0).$$

We now define scalar multiplication:

Definition 3.3 *Let $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$ and $c \in \mathbb{F}$ be a scalar. Then $c \cdot f(x) = (ca_m)x^m + (ca_{m-1})x^{m-1} + \cdots + (ca_1)x + (ca_0)$.*

The following is tedious but straightforward.

Theorem 3.1 *The collection $\mathbb{F}[x]$ with the operations of addition and scalar multiplication is an infinite dimensional vector space over $\mathbb{F}$ with a basis $\{1\} \cup \{x^k | k \in \mathbb{N}\}$.*

There is more algebraic structure to $\mathbb{F}$ which we introduce in the following definition:

Definition 3.4 *Let $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ and $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$ be polynomials with entries in $\mathbb{F}$. Then the* **product** *$f(x)g(x)$ is defined by*

$$f(x)g(x) = \sum_{l=0}^{m+n} (\sum_{j+k=l} a_j b_k) x^l.$$

Hopefully, this is familiar since it coincides with the product of polynomials learned in high school algebra: To get the coefficient of x^l in the product, you multiply all terms $a_j x^j$ and $b_k x^k$, where $j + k = l$ and add up.

Remark 3.1 *Assume $f(x) \neq 0$ has leading term $a_m x^m$ and $g(x) \neq 0$ has leading term $b_n x^n$. Then $f(x)g(x)$ has leading term $a_m b_n x^{m+n}$. Therefore, $f(x)g(x)$ is non-zero and has degree $m + n$.*

The next theorem collects the basic properties of multiplication.

Theorem 3.2 *Let $f, g, h \in \mathbb{F}[x]$. Then the following hold:*

i) $(fg)h = f(gh)$. Multiplication of polynomials is associative.

ii) $fg = gf$. Multiplication of polynomials is commutative.

iii) The polynomial 1 is a multiplicative identity: $1 \cdot f = f \cdot 1 = f$.

iv) $(f + g)h = fh + gh$. Multiplication distributes over addition.

v) If $f(x)g(x) = 0$, then either $f(x) = 0$ or $g(x) = 0$.

As a consequence of Theorems (3.1) and (3.2), we can conclude:

Theorem 3.3 *$\mathbb{F}[x]$ is a commutative algebra with identity over $\mathbb{F}$.*

Lemma 3.1 *Assume $f(x) \neq 0$ and $f(x)g(x) = f(x)h(x)$. Then $g(x) = h(x)$.*

Proof *If $f(x)g(x) = f(x)h(x)$, then $f(x)g(x) - f(x)h(x) = f(x)[g(x) - h(x)] = 0$. Since $f(x) \neq 0$ by v) of Theorem (3.2) it follows that $g(x) - h(x) = 0$, whence $g(x) = h(x)$ as claimed.*

The next lemma is just a formal statement of how you divide one polynomial by another to obtain a quotient and a remainder.

Lemma 3.2 *Let $f(x)$ and $d(x) \neq 0$ be polynomials with coefficients in $\mathbb{F}$. Then there exists unique polynomials $q(x)$ and $r(x)$, which satisfy $f(x) = q(x)d(x) + r(x)$, where either $r(x) = 0$ or $deg(r(x)) < deg(d(x))$.*

Proof *We prove the existence of $q(x)$ and $r(x)$ by the second principle of mathematical induction on $deg(f(x))$. If $f(x) = 0$, there is nothing to prove. Suppose $deg(f(x)) = 0$ (so $f(x)$ is a constant polynomial, that is, an element of $\mathbb{F}$). If $d(x)$ has degree 0, then set $q(x) = \frac{f}{d}$ and $r(x) = 0$. If $d(x)$ is not constant, then set $q(x) = 0$ and $r(x) = f(x)$. This takes care of the base case.*

Now assume that $deg(f(x)) = n > 0$ and the result has been obtained for all polynomials $g(x)$ with $deg(g(x)) < n$. Suppose $deg(d(x)) > deg(f(x))$. Then set $q(x) = 0$ and $r(x) = f(x)$.

We may now assume that $deg(d(x)) \leq deg(f(x))$. Let the leading term of $d(x)$ be $b_m x^m$ and the leading term of $f(x)$ be $a_n x^m$. Set $g(x) = f(x) - \frac{a_n}{b_m} x^{n-m} d(x)$. By construction, $\frac{a_n}{b_m} x^{n-m} d(x)$ has the same leading term as $f(x)$ and, consequently, $deg(g(x)) < n$. Therefore, our inductive hypothesis can be invoked: there are polynomials $q_1(x)$ and $r(x)$ with $r(x) = 0$ or $deg(r(x)) < deg(d(x))$ such that $g(x) = q_1(x)d(x) + r(x)$. Now set $q(x) = \frac{b_n}{a_m} x^{n-m} + q_1(x)$. Then $g(x) = f(x) - \frac{b_n}{a_m} x^{n-m} d(x) = q_1(x)d(x) + r(x)$ and therefore $f(x) = [\frac{b_n}{a_m} x^{n-m} + q_1(x)]d(x) + r(x) = q(x)d(x) + r(x)$. This establishes the existence of $q(x)$ and $r(x)$.

We now prove uniqueness. Suppose $f(x) = q(x)d(x) + r(x) = q'(x)d(x) + r'(x)$. Then $[q(x) - q'(x)]d(x) = r'(x) - r(x)$. Suppose $q(x) - q'(x) \neq 0$. Then the degree of the left-hand side is at least $deg(d(x))$. On the other hand, the right-hand side has degree bounded above by $max\{deg(r(x)), deg(r'(x))\}$, which is less than $deg(d(x))$. Therefore, we must have $r(x) - r'(x) = 0$ so that $r(x) = r'(x)$ and then $q(x) - q'(x) = 0$.

When we invoke Lemma (3.2) we will say that we are **applying the division algorithm**.

Definition 3.5 *Let $f(x), g(x)$ be polynomials with entries in $\mathbb{F}$. We will say that $f(x)$* **divides** *$g(x)$ and write $f(x)|g(x)$ if there is a polynomial $q(x) \in \mathbb{F}[x]$ such that $g(x) = f(x)q(x)$.*

The following lemma makes explicit many of the properties of the relation "divides."

Lemma 3.3 *Let $f(x)$ be a non-zero polynomial. Then the following hold:*

i) If $f(x)$ divides $g(x)$ and $g(x)$ divides $h(x)$, then $f(x)$ divides $h(x)$.

ii) If $f(x)$ divides $g(x)$ and $h(x)$, then $d(x)$ divides $g(x)+h(x)$ and $g(x)-h(x)$.

iii) If $f(x)$ divides $g(x)$ and $h(x)$, then for all polynomials $a(x), b(x)$, $f(x)$ divides $a(x)g(x) + b(x)h(x)$.

iv) If $f(x)$ divides $g(x)$ and $g(x)$ divides $f(x)$, then there are non-scalars $a, b \neq 0$ such that $g(x) = af(x), f(x) = bg(x)$.

Proof *i) Suppose $g(x) = a(x)f(x)$ and $h(x) = b(x)g(x)$. Then $h(x) = b(x)[a(x)f(x)] = [b(x)a(x)]f(x)$ and so by the definition, $f(x)|h(x)$.*

ii) Suppose $g(x) = a(x)f(x)$ and $h(x) = b(x)f(x)$. Then $g(x) \pm h(x) = a(x)f(x) \pm b(x)f(x) = [a(x) \pm b(x)]f(x)$.

iii) Assume $f(x)$ divides $g(x)$ and $h(x)$. Then $f(x)$ divides $a(x)g(x)$ by i). Similarly, if $f(x)$ divides $h(x)$, then $f(x)$ divides $b(x)h(x)$ by i). Then by ii) $f(x)$ divides $a(x)g(x) + b(x)h(x)$.

iv) Let $g(x) = a(x)f(x), f(x) = b(x)g(x)$. Then $f(x) = b(x)[a(x)f(x)] = [b(x)a(x)]f(x)$. Since $f(x) \neq 0$ it follows that $b(x)a(x) = 1$. It follows from Remark (3.1) that both $a(x), b(x)$ have degree zero; that is, they are non-zero elements of $\mathbb{F}$.

If this relation reminds you of the relation of divides for integers, that is a good observation because the similarity is more than superficial. And, like that relation, there is a notion of greatest common divisor and least common multiple.

Definition 3.6 *Let $f(x)$ and $g(x)$ be polynomials, not both zero. A polynomial $d(x)$ is said to be a* **greatest common divisor** *(gcd) of $f(x)$ and $g(x)$ if the following hold:*

i) $d(x)$ is monic;

ii) $d(x)|f(x)$ and $d(x)|g(x)$; and

iii) if $d'(x)|f(x)$ and $d'(x)|g(x)$, then $d'(x)|d(x)$.

The definition refers to "a" greatest common divisor; however, in the next lemma we show that there is at most one gcd.

Lemma 3.4 *Assume $f(x)$ and $g(x)$ are polynomials, not both zero. If a gcd exists for $f(x)$ and $g(x)$, then it is unique.*

Proof *Suppose $d_1(x)$ and $d_2(x)$ are both gcd's for $f(x)$ and $g(x)$. By the definition, $d_1(x)|f(x)$ and $d_1(x)|g(x)$. Since $d_2(x)$ is a gcd, it follows that $d_1(x)|d_2(x)$. Similarly, since $d_2(x)|f(x)$ and $d_2(x)|g(x)$ and $d_1(x)$ is a gcd, we can conclude that $d_2(x)|d_1(x)$. Now by iv) of Lemma (3.3), it follows that there is an element $a \in \mathbb{F}$ such that $d_2(x) = ad_1(x)$. Since both $d_1(x)$ and $d_2(x)$ are monic, $a = 1$ and $d_2(x) = d_1(x)$.*

In our next theorem, we show the existence of the gcd of two polynomials.

Theorem 3.4 *Let $f(x), g(x)$ be polynomials, not both zero. Then the gcd of $f(x)$ and $g(x)$ exists.*

Proof *Let $J = \{a(x)f(x) + b(x)g(x)|a(x), b(x) \in \mathbb{F}[x]\}$. Then J satisfies the following:*

a) If $F(x), G(x) \in J$, then $F(x) + G(x) \in J$.

b) If $F(x) \in J$ and $c(x) \in \mathbb{F}[x]$, then $c(x)F(x) \in J$.

We leave the proof of these as exercises. Recall this means that J is an ideal of $\mathbb{F}[x]$; see Definition (2.22). Let $d(x)$ be a monic polynomial in J with $deg(d(x))$ minimal. Such a polynomial $d(x)$ exists by the well-ordering principle for the natural numbers. We claim that $d(x)$ is the gcd of $f(x)$ and $g(x)$. Clearly, $d(x)$ is monic so the first of the criteria holds. Also, suppose $d'(x)$ is a polynomial and $d'(x)|f(x)$ and $d'(x)|g(x)$. Then by iii) of Lemma (3.3), $d'(x)$ divides all $F(x) \in J$. In particular, $d'(x)$ divides $d(x)$. Therefore, the third criterion for a gcd is satisfied. It remains to show that $d(x)|f(x)$ and $d(x)|g(x)$.

Suppose the second criterion is not satisfied. Then $d(x)$ does not divide $f(x)$ or $d(x)$ does not divide $g(x)$. Without loss of generality, we may assume $d(x)$ does not divide $f(x)$. Applying the division algorithm to $f(x)$ and $d(x)$ we can conclude that there are unique polynomials $q(x)$ and $r(x)$ such that

$$f(x) = q(x)d(x) + r(x), deg(r(x)) < deg(d(x)),$$

the latter since we are assuming that $r(x) \neq 0$. However, $r(x) = f(x) + (-q(x))d(x)$. Since $f(x), d(x) \in J$, it follows by a) and b) above that $r(x) \in J$. Let $r'(x)$ be the unique scalar multiple of $r(x)$, which is monic. Then also $r'(x) \in J$. However, $deg(r'(x)) = deg(r(x)) < deg(d(x))$ and this contradicts the minimality of the degree of $d(x)$ among monic polynomials in J. Thus, $d(x)|f(x)$. In exactly the same way, we conclude that $d(x)|g(x)$ and $d(x)$ is the gcd of $f(x)$ and $g(x)$.

Our next result leads the way to an algorithm for finding the gcd of two polynomials.

Lemma 3.5 *Let $f(x), g(x)$ be two polynomials with $f(x) \neq 0$. Write $g(x) = q(x)f(x) + r(x)$ with $deg(r(x)) < deg(f(x))$. Then $gcd(f(x), g(x)) = gcd(f(x), r(x))$.*

Proof *Set $d(x) = gcd(f(x), g(x))$ and $d'(x) = gcd(f(x), r(x))$. It suffices to show that $d(x)|d'(x)$ and $d'(x)|d(x)$ by iv) of Theorem (3.3). By the definition of the gcd, $d(x)|f(x)$ and $d(x)|g(x)$. Then $d(x)|g(x) - q(x)f(x) = r(x)$. Since $d'(x)$ is the gcd of $f(x)$ and $r(x)$, it follows from the third part of the definition that $d(x)|d'(x)$.*

Now by the first part of the definition, since $d'(x)$ is the gcd of $f(x)$ and $r(x)$ we know that $d'(x)|f(x)$ and $d'(x)|r(x)$. Then $d'(x)|q(x)f(x) + r(x) = g(x)$. Since $d(x)$ is the gcd of $f(x)$ and $g(x)$, by the third part of the definition it follows that $d'(x)|d(x)$.

In the following, we describe an algorithm for finding the gcd of two polynomials.

The Euclidean Algorithm

Let $f(x)$ and $g(x)$ be polynomials with $f(x) \neq 0$. Define a sequence of polynomials as follows: Set $g_1(x) = g(x)$ and $d_1(x) = f(x)$.

Suppose $g_k(x)$ and $d_k(x)$ have been defined and $d_k(x) \neq 0$. Write $g_k(x) = q_k(x)d_k(x) + r_k(x)$, where either $r_k(x) = 0$ or $deg(r_k(x)) < deg(d_k(x))$. Then set $g_{k+1}(x) = d_k(x)$ and $d_{k+1}(x) = r_k(x)$. If $d_{k+1}(x) = r_k(x) = 0$, stop.

Since $deg(r_1(x)) < deg(f(x))$ and either $r_k(x) = 0$ or $deg(r_{k+1}(x)) < deg(r_k(x))$,c polynomial which is a scalar multiple of $r_m(x)$. We claim that $d(x)$ is the gcd of $f(x)$ and $g(x)$. From Lemma (3.5), we have

$$\begin{aligned}
gcd(f(x), g(x)) &= gcd(g_1(x), d_1(x)) \\
&= gcd(d_1(x), r_1(x)) \\
&= gcd(d_2(x), r_2(x) \\
&= \dots \\
&= gcd(d_m(x), r_m(x) \\
&= gcd(d_{m+1}(x), r_{m+1}(x)).
\end{aligned}$$

However, $d_{m+1}(x) = r_m(x)$ and $r_{m+1}(x) = 0$. It follows that the gcd is the monic polynomial of least degree, which is a multiple of $r_m(x)$ and this is the unique scalar multiple of $r_m(x)$ which is monic.

In our next definition we define the least common multiple (lcm) of two polynomials.

Definition 3.7 *Let $f(x)$ and $g(x)$ be polynomials, not both zero. A* **least common multiple** *of $f(x)$ and $g(x)$ is a polynomial $l(x)$ which satisfies the following:*

a) $l(x)$ is monic;
b) $f(x)|l(x)$ and $g(x)|l(x)$; and
c) if $f(x)|m(x)$ and $g(x)|m(x)$ then $l(x)|m(x)$.

We leave the proof that the least common multiple of two polynomials exists as an exercise. Our immediate goal is to prove something like the **Fundamental Theorem of Arithmetic**, which states that every natural number greater than one is either a prime or a product of primes. Toward that end, we introduce the concept of an irreducible polynomial, which is the analog for polynomials of a prime number among the integers. We also define the concept of relatively prime polynomials.

Definition 3.8 *A non-constant polynomial $f(x)$ is said to be* **irreducible** *if whenever $f(x) = g(x)h(x)$, either $g(x)$ is a constant (element of $\mathbb{F}$) or $h(x)$ is a constant. If $f(x)$ is not irreducible then it is* **reducible**.

Definition 3.9 *Let $f(x)$ and $g(x)$ be polynomials, not both zero. Then $f(x)$ and $g(x)$ are said to be* **relatively prime** *if the only polynomials that divide both $f(x)$ and $g(x)$ are constants. Note that this is equivalent to $gcd(f(x), g(x)) = 1$.*

Corollary 3.1 *Let $f(x), g(x) \in \mathbb{F}[x]$ and set $\langle f(x), g(x)\rangle_{\mathbb{F}[x]} = \{a(x)f(x) + b(x)g(x)|a(x), b(x) \in \mathbb{F}[x]\}$. Then $f(x)$ and $g(x)$ are relatively prime if and only if $\langle f(x), g(x)\rangle_{\mathbb{F}[x]} = \mathbb{F}[x]$.*

Proof *Assume $gcdf(x), g(x)) = 1$. Then by the proof of Theorem (3.4) there are polynomials $a(x), b(x)$ such that $a(x)f(x) + b(x)g(x) = 1$ and then for any polynomial $h(x)$ we have $[h(x)a(x)]g(x) + [h(x)b(x)]g(x) = h(x)$ so that $\langle f(x), g(x)\rangle_{\mathbb{F}[x]} = \mathbb{F}[x]$.*

Conversely, if $\langle f(x), g(x)\rangle_{\mathbb{F}[x]} = \mathbb{F}[x]$ then, in particular, $1 \in \langle f(x), g(x)\rangle_{\mathbb{F}[x]}$ so that there are polynomials $a(x), b(x)$ such that $a(x)f(x)+b(x)g(x) = 1$ from which we conclude by the proof of Theorem (3.4) that $gcd(f(x), g(x)\} = 1$ and $f(x), g(x)$ are relatively prime.

Lemma 3.6 *Assume $f(x)$ and $g(x)$ are relatively prime and $f(x)|g(x)h(x)$. Then $f(x)|h(x)$.*

Proof *Since $gcd(f(x), g(x)) = 1$, and there are polynomials $a(x), b(x)$ such that $a(x)f(x) + b(x)g(x) = 1$. Then $h(x) =$*

$$\begin{aligned}[a(x)f(x) + b(x)g(x)]h(x) &= [a(x)f(x)]h(x) + [b(x)g(x)]h(x) \\ &= [a(x)h(x)]f(x) + b(x)[g(x)h(x)].\end{aligned}$$

Clearly, $f(x)$ divides $[a(x)h(x)]f(x)$. Since by hypothesis $f(x)$ divides $g(x)h(x)$, it follows by i) of Lemma (3.3) that $f(x)$ divides $b(x)[g(x)h(x)]$. Then by ii) of Lemma (3.3) $f(x)$ divides $[a(x)h(x)]f(x) + b(x)[g(x)h(x)] = h(x)$.

A useful corollary is the following:

Corollary 3.2 *Assume $p(x)$ is irreducible and $p(x)|g_1(x)g_2(x)\dots g_s(x)$. Then for some $j, 1 \leq j \leq s$, $p(x)$ divides $g_j(x)$.*

Proof *The proof is by induction on s. Clearly, if $s = 1$ there is nothing to prove. We next prove the result for $s = 2$. Suppose $p(x)|g_1(x)g_2(x)$ and $p(x)$ does not divide $g_1(x)$. Since $p(x)$ is irreducible it follows that $p(x)$ and $g_1(x)$ are relatively prime. Then by Lemma (3.6) it follows that $p(x)|g_2(x)$ as required.*

Now assume the result is true for s and that $p(x)|g_1(x)g_2(x)\dots g_s(x)g_{s+1}(x)$. Set $h_1(x) = g_1(x)\dots g_s(x)$ and $h_2(x) = g_{s+1}(x)$. Then by the previous paragraph either $p(x)|h_1(x) = g_1(x)\dots g_s(x)$ or $p(x)|h_2(x) = g_{s+1}(x)$. In the latter case, we are done. In the former case, we can apply the inductive hypothesis and conclude that $p(x)$ divides $g_j(x)$ for some $j, 1 \leq j \leq s$.

Another useful corollary is:

Corollary 3.3 *Let $f(x), g(x)$ be relatively prime polynomials. Assume $h(x)$ is a polynomial with $f(x)|h(x)$ and $g(x)|h(x)$. Then $f(x)g(x)|h(x)$.*

Proof *Let $h_1(x) \in \mathbb{F}[x]$ such that $h(x) = f(x)h_1(x)$. Since $g(x)|h(x) = f(x)h_1(x)$ and $gcd(f(x), g(x)) = 1$ by Lemma (3.6) it follows that $g(x)|h_1(x)$. Let $h_2(x) \in \mathbb{F}[x]$ such that $h_1(x) = g(x)h_2(x)$. Then $h(x) = f(x)g(x)h_2(x)$ so that $f(x)g(x)|h(x)$.*

In our next theorem, we show that every non-zero polynomial can be written as a product of a scalar and monic irreducible polynomials. The main idea is the use of the second principle of mathematical induction.

Theorem 3.5 *Let $f(x)$ be a non-constant polynomial. Then there is a scalar a and monic irreducible polynomials $p_1(x), p_2(x), \dots, p_t(x)$ such that*

$$f(x) = ap_1(x)p_2(x)\dots p_t(x).$$

Proof *Let the leading coefficient of $f(x)$ be a and set $f'(x) = \frac{1}{a}f(x)$ so that $f(x)$ is monic. It suffices to prove that $f'(x)$ can be written as a product of monic irreducible polynomials, so without loss of generality we may assume that $f(x)$ is monic.*

The proof is by the second principle of mathematical induction on $deg(f(x))$. If $deg(f(x)) = 1$, then $f(x)$ is irreducible and there is nothing to prove. We now proceed to the inductive step. Assume that $deg(f(x)) = n$ and every monic polynomial of positive degree less than n can be expressed as a product of monic irreducible polynomials. If $f(x)$ is irreducible, there is nothing to prove so we may assume that $f(x)$ is reducible. It then follows that there are polynomials $g(x)$ and $h(x)$ with $deg(g(x)), deg(h(x)) > 0$ such that $f(x) = g(x)h(x)$. If the leading coefficient of $g(x)$ is b and the leading coefficient of $h(x)$ is c, then the leading coefficient of $f(x)$ is bc. Since $f(x)$ is monic, it follows that $bc = 1$. By replacing $(g(x), h(x))$ by $(cg(x), bh(x))$, we may assume that $g(x)$ and $h(x)$ are monic. Now $g(x)$ and $h(x)$ are non-constant and $deg(g(x)), deg(h(x)) < deg(f(x))$. Therefore, by the inductive hypothesis, we can express $g(x)$ as a product of monic irreducible polynomials, and we can express $h(x)$ as a product of monic irreducible polynomials. But then by multiplying $g(x)$ by $h(x)$, we obtain an expression for $f(x)$ as a product of monic irreducible polynomials.

When $f(x)$ is a non-constant polynomial, and we write $f(x) = ap_1(x)p_2(x)\dots p_t(x)$, where $p_i(x)$ are monic irreducible polynomials, we refer to this as a ***prime or complete factorization*** of $f(x)$.

Our next objective is to prove the essential uniqueness of a prime factorization of a polynomial.

Theorem 3.6 *Let $f(x)$ be a non-constant polynomial and assume that*

$$f(x) = ap_1(x)p_2(x)\dots p_t(x) = bq_1(x)q_2(x)\dots q_s(x),$$

where a, b are scalars and each $p_i(x)$ and $q_j(x)$ is a monic irreducible polynomial. Then $a = b, t = s$, and there is a permutation π of $\{1, 2, \dots, t\}$ such that $p_i(x) = q_{\pi(i)}(x)$.

Proof *The proof is by the second principle of induction on deg($f(x)$). If deg($f(x)$) $= 1$, then $f(x) = ax + c$ for some scalars a, c and $f(x) = a(x + \frac{c}{a})$ and this is the unique factorization of $f(x)$.*

Suppose now that deg($f(x)$) $= n > 1$ and the result has been established for all non-constant polynomials with degree less than n and assume that $f(x) = ap_1(x)p_2(x)\dots\ p_t(x) = bq_1(x)q_2(x)\dots q_s(x)$, where a, b are scalars and each $p_i(x)$ and $q_j(x)$ is a monic irreducible polynomial.

Since $p_i(x)$ are all monic, the product $p_1(x)\dots p_t(x)$ is monic and therefore a is the leading coefficient of $f(x)$. Similarly, b is the leading coefficient of $f(x)$. Consequently, $a = b$. We can therefore divide by $a = b$. After doing so we have the equality

$$p_1(x)p_2(x)\dots p_t(x) = q_1(x)q_2(x)\dots q_s(x).$$

We next prove that $t = s$. Now $p_t(x)|p_1(x)p_2(x)\dots p_t(x) = q_1(x)\dots q_s(x)$. We claim that there is some $j, 1 \leq j \leq s$ such that $p_t(x) = q_j(x)$. By Corollary(3.2), there exists some $j, 1 \leq j \leq s$ such that $p_t(x)|q_j(x)$.

By relabeling, if necessary we can assume that $p_t(x)|q_s(x)$. However, since $q_s(x)$ is an irreducible, if $p_t(x)|q_s(x)$, then there is a scalar c such that $q_s(x) = cp_t(x)$. Since both $p_t(x)$ and $q_s(x)$ are monic we conclude that $p_t(x) = q_s(x)$.

Since $p_1(x)\dots p_{t-1}(x)p_t(x) = q_1(x)\dots q_{s-1}(x)q_s(x) = q_1(x)\dots q_{s-1}(x)p_t(x)$ and $p_t(x) \neq 0$ by Lemma (3.1), it follows that $p_1(x)\dots p_{t-1}(x) = q_1(x)\dots q_{s-1}(x)$. Since deg($p_1(x)\dots p_{t-1}(x)$) is less than deg($p_1(x)\dots p_t(x)$) we can apply the inductive hypothesis and conclude that $t - 1 = s - 1$ and that there exists a permutation π of $\{1, 2, \dots, t-1\} = \{1, 2, \dots, s-1\}$ such that $p_i(x) = q_{\pi(i)}(x)$.

We conclude this section with the following:

Lemma 3.7 *Assume that $f(x)$ is relatively prime to $g(x)$ and $h(x)$. Then $f(x)$ is relatively prime to $g(x)h(x)$.*

Proof *Let $d(x)$ be the gcd of $f(x)$ and $g(x)h(x)$ and assume to the contrary that $d(x) \neq 1$. Let $p(x)$ be an irreducible polynomial, which divides $d(x)$. Then $p(x)$ divides $f(x)$ and $p(x)$ divides $g(x)h(x)$. Since $p(x)$ is irreducible and $p(x)$ divides $g(x)h(x)$, by Corollary (3.2), either $p(x)$ divides $g(x)$ or $p(x)$ divides $h(x)$. Suppose $p(x)$ divides $g(x)$. Then $p(x)$ divides gcd($f(x), g(x)$) $= 1$, a contradiction. We get a similar contradiction if $p(x)$ divides $h(x)$. Thus, $d(x) = 1$ and $f(x), g(x)h(x)$ are relatively prime as claimed.*

Exercises

1. Find the gcd of $x^3 + x^2 + x + 1$ and $x^5 + 2x^3 + x^2 + x + 1$.

In Exercises 2 and 3, let J be as defined in Theorem (3.4).

2. Prove that J is closed under addition. That is, prove if $F(x), G(x) \in J$, then $F(x) + G(x) \in J$.

3. Prove that J is closed under multiplication by elements of $\mathbb{F}[x]$. That is, prove if $F(x) \in J$ and $c(x) \in \mathbb{F}[x]$, then $c(x)F(x) \in J$.

4. Let $J \subset \mathbb{F}[x]$ be an ideal, $J \neq \{0\}$. Among all non-zero monic polynomials in J, let $d(x)$ have minimal degree. Prove that every element of J is a multiple of $d(x)$ and that $d(x)$ is unique. Such a polynomial is called a ***generator*** of J.

5. Let $f(x), g(x)$ be polynomials, not both zero, and let $d(x) = gcd(f(x), g(x))$. Suppose $f(x) = d(x)f^*(x), g(x) = d(x)g^*(x)$. Prove that $f^*(x), g^*(x)$ are relatively prime.

6. Assume $f(x), g(x) \in \mathbb{F}[x]$, are monic, with $gcd(f(x), g(x)) = d(x)$. Set $l(x) = \frac{f(x)g(x)}{d(x)}$. Prove that $l(x)$ is a least common multiple of $f(x)$ and $g(x)$.

7. Assume $f(x)$ and $g(x)$ are polynomials, not both zero. Prove that a least common multiple of $f(x)$ and $g(x)$ is unique.

8. Assume $f(x)$ is an irreducible polynomial, $g(x)$ is a polynomial, and $f(x)$ does not divide $g(x)$. Prove that $f(x)$ and $g(x)$ are relatively prime.

9. Assume $f(x)$ and $g(x)$ are relatively prime polynomials. Prove that the $lcm\{f(x), g(x)\}$ is the unique monic scalar multiple of $f(x)g(x)$.

10. Let $\mathbb{F} \subset \mathbb{K}$ be fields. Suppose $f(x)$ and $g(x)$ are polynomials with coefficients in $\mathbb{F}$, $h(x)$ a polynomial with coefficients in $\mathbb{K}$, and $f(x) = g(x)h(x)$. Prove that $h(x)$ has entries in $\mathbb{F}$.

11. Assume $f(x) = p_1(x)^{e_1} \dots p_t(x)^{e_t}$, where $p_1(x), \dots, p_t(x)$ are irreducible and distinct. Prove that $f(x)$ has exactly $(e_1 + 1) \dots (e_t + 1)$ monic factors.

3.2 Roots of Polynomials

What You Need to Know

The division algorithm for polynomials with coefficients in a field.

We begin with some definitions:

Definition 3.10 *Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a polynomial with coefficients in $\mathbb{F}$ and let $b \in \mathbb{F}$. Then by $f(b)$, which we refer to as $f(x)$* **evaluated at** *b, or the* **value of** *$f(x)$ at b, we mean the element of $\mathbb{F}$ obtained by substituting b for x in the expression $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$*

$$f(b) = a_nb^n + a_{n-1}b^{n-1} + \cdots + a_1b + a_0.$$

Definition 3.11 *By a* **root** *of $f(x)$, we mean an element λ of $\mathbb{F}$ such that $f(\lambda) = 0$.*

The following theorem is often included in second-year high school algebra courses and goes by the name of the **root-remainder theorem**:

Theorem 3.7 *Let $f(x)$ be a non-constant polynomial and $\lambda \in \mathbb{F}$. Set $r = f(\lambda)$. Then r is the remainder when $f(x)$ is divided by $x - \lambda$.*

Proof *Write $f(x) = q(x)(x - \lambda) + R(x)$, where either $R(x) = 0$ or $deg(R(x)) < deg(x - \lambda) = 1$. In either case, $R(x)$ is a scalar (element of $\mathbb{F}$). Now evaluate at λ:*

$$r = f(\lambda) = q(\lambda)(\lambda - \lambda) + R = q(\lambda) \cdot 0 + R = 0 + R = R.$$

An immediate corollary to the theorem is the following:

Corollary 3.4 *Let $f(x)$ be a polynomial. Then λ is a root of $f(x)$ if and only if $x - \lambda$ divides $f(x)$.*

The previous corollary allows us to define the multiplicity of the root of a polynomial:

Definition 3.12 *Let $f(x)$ be a polynomial and λ an element of $\mathbb{F}$. The scalar λ is said to be a* **root of multiplicity** *k of $f(x)$ if $(x-\lambda)^k$ divides $f(x)$ but $(x-\lambda)^{k+1}$ does not divide $f(x)$.*

As a further corollary, we can show that a polynomial of degree n has at most n roots (counting multiplicity).

Corollary 3.5 *Let $f(x)$ be a polynomial of degree n. Then $f(x)$ has at most n roots, counting multiplicity. In particular, $f(x)$ has at most n distinct roots.*

Proof *Let $\lambda_i, 1 \leq i \leq t$, be the distinct roots of $f(x)$ with λ_i occurring with multiplicity e_i. For $i \neq j$, $\frac{1}{\lambda_j - \lambda_i}[(x-\lambda_i)-(x-\lambda_j)] = 1$, and therefore $x-\lambda_i$ and $x-\lambda_j$ are relatively prime. It follows from Lemma (3.7) that $(x-\lambda_i)^{e_i}$ and $(x-\lambda_j)^{e_j}$ are relatively prime. It then follows from Exercise 9 of Section (3.1) that $(x-\lambda_1)^{e_1}(x-\lambda_2)^{e_2}\dots(x-\lambda_t)^{e_t}$ divides $f(x)$. Consequently, $deg(f(x)) \geq e_1+e_2+\cdots+e_t$.*

For the remainder of this section, we turn our attention to polynomials with real and complex coefficients. The importance of the field $\mathbb{C}$ is that it is algebraically closed, a concept we now define:

Definition 3.13 *A field $\mathbb{F}$ is said to be* **algebraically closed** *if every nonconstant polynomial $f(x)$ has a root in $\mathbb{F}$.*

Theorem 3.8 *Assume the field $\mathbb{F}$ is algebraically closed and $f(x)$ is a polynomial of degree $n \geq 0$. Then there exist elements a and $\lambda_i, 1 \leq i \leq n$ in $\mathbb{F}$ such that*

$$f(x) = a\prod_{i=1}^{n}(x-\lambda_i).$$

Proof *The proof is by induction on $deg(f(x))$. If $deg(f(x)) = 1$, say, $f(x) = ax+b$, then $\lambda = -\frac{b}{a}$ is a root and $f(x) = a(x-\lambda)$.*

Assume that all polynomials of degree n have n roots in $\mathbb{F}$ and that $deg(f(x)) = n+1$. Since $\mathbb{F}$ is algebraically closed there exists $\lambda \in \mathbb{F}$ such that $f(\lambda) = 0$. Then by Corollary (3.4), $x-\lambda$ divides $f(x)$. Let $g(x)$ be the polynomial such that $f(x) = g(x)(x-\lambda)$. Then $g(x)$ has degree n, and so by the inductive hypothesis, there are elements $a, \lambda_i, 1 \leq i \leq n$ in $\mathbb{F}$ such that

$$g(x) = a\prod_{i=1}^{n}(x - \lambda_i).$$

Set $\lambda_{n+1} = \lambda$. *Then*

$$f(x) = a\prod_{i=1}^{n+1}(x - \lambda_i).$$

Remark 3.2 *If follows immediately from Theorem (3.8) that if* $\mathbb{F}$ *is algebraically closed and* $f(x)$ *has degree* n*, then* $f(x)$ *has exactly* n *roots in* $\mathbb{F}$*, counting multiplicity.*

Theorem 3.9 Fundamental Theorem of Algebra

The complex field, $\mathbb{C}$*, is algebraically closed.*

Proof *The essential element of the proof is a result from complex analysis, known as Liouville's theorem, which states that a bounded entire function (holomorphic function) must be constant. In the present case, if* $f(x)$ *is a polynomial with complex coefficients and no root, then* $\frac{1}{f(x)}$ *will be a bounded entire function, whence constant, which is a contradiction. For more details consult a textbook on complex analysis such as ([7]).*

The Fundamental Theorem of Algebra has consequences for polynomials with real coefficients:

Lemma 3.8 *Let* $f(x)$ *be a polynomial with real coefficients. Suppose* $\lambda \in \mathbb{C}$ *is a root of* $f(x)$ *and* λ *is not real. Then* $\overline{\lambda}$ *is also a root of* $f(x)$.

Proof *Let* $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$. *Then*

$$0 = f(\lambda) = a_n\lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0.$$

Taking the complex conjugate we get

$$0 = \overline{0} = \overline{f(\lambda)} = \overline{a}_n\overline{\lambda}^n + \overline{a}_{n-1}\overline{\lambda}^{n-1} + \cdots + \overline{a}_1\overline{\lambda} + \overline{a}_0.$$

Since each a_i *is real,* $\overline{a}_i = a_i$. *Consequently,*

$$0 = a_n\overline{\lambda}^n + a_{n-1}\overline{\lambda}^{n-1} + \ldots a_1\overline{\lambda} + a_0 = f(\overline{\lambda}).$$

As a corollary, we have the following:

Corollary 3.6 *Let $f(x)$ be a real monic irreducible polynomial. Then either $deg(f(x)) = 1$ or 2.*

Proof *Since a real polynomial is a complex polynomial, there exists a complex root λ. Suppose λ is real. Then $x-\lambda$ divides $f(x)$ in $\mathbb{C}[x]$ and then by Exercise 10 of Section (3.1), $x-\lambda$ divides $f(x)$ in $\mathbb{R}[x]$. Since $f(x)$ is a monic irreducible polynomial it follows that $f(x) = x - \lambda$.*

So assume that $\lambda \in \mathbb{C} \setminus \mathbb{R}$. Then by Lemma (3.8) it follows that $\overline{\lambda}$ is also a root of $f(x)$. Write $\lambda = a + bi$ so that $\overline{\lambda} = a - bi$. Then $(x - \lambda)(x - \overline{\lambda}) = x^2 - 2ax + (a^2 + b^2)$ is a real quadratic polynomial. Moreover, $(x - \lambda)(x - \overline{\lambda})$ divides $f(x)$ in $\mathbb{C}[x]$ and therefore, again by Exercise 10 of Section (3.1), $x^2 - 2ax + (a^2 + b^2)$ divides $f(x)$ in $\mathbb{R}[x]$. Since $f(x)$ is a monic irreducible polynomial it follows that $f(x) = x^2 - 2ax + (a^2 + b^2)$.

We will need to know when a real monic polynomial $x^2 + bx + c$ is irreducible. The answer is supplied by the following:

Lemma 3.9 *The real monic quadratic polynomial $x^2 + bx + c$ is irreducible if and only if $b^2 - 4c < 0$.*

Proof *By adding and subtracting $(\frac{b}{2})^2$ from $x^2 + bx + c$ we obtain*

$$\begin{aligned} x^2 + bx + c &= x^2 + bx + \left(\frac{b}{2}\right)^2 + c - \left(\frac{b}{2}\right)^2 \\ &= (x + \frac{b}{2})^2 - \frac{b^2 - 4c}{4}. \end{aligned}$$

If $b^2 - 4c = 0$, then $f(x)$ has the root $-\frac{b}{2}$ with multiplicity 2. If $b^2 - 4c > 0$ then setting $\gamma = \sqrt{b^2 - 4c}$, we see that $-\frac{b}{2} \pm \frac{\gamma}{2} = \frac{-b\pm\gamma}{2}$ are real roots of $f(x)$. On the other hand, if $b^2 - 4c$ is negative, then for all real $x, f(x) > 0$, and there are no real roots.

Theorem 3.10 *Let $f(x)$ be a non-constant real polynomial. Then there are real numbers $c, r_1, r_2, \dots, r_s$ and real monic, irreducible, quadratic polynomials $p_1(x), p_2(x), \dots, p_t(x)$ such that*

$$f(x) = c(x - r_1)(x - r_2) \dots (x - r_s)p_1(x)p_2(x) \dots p_t(x).$$

Proof *This follows from Theorem (3.5) and Corollary (3.6).*

Exercises

1. Assume $f(x)$ is a real polynomial of degree $2m+1$, where m is a natural number. Prove that $f(x)$ has a real root.

2. Give an example of a real polynomial of degree four, which has no real roots and four distinct complex roots.

3. Assume $f(x) = x^n + a_{n-1}x^n + \cdots + a_1x + a_0$ is a complex polynomial and $\lambda \in \mathbb{C}$ is a root of $f(x)$. Prove that $\overline{\lambda}$ is a root of $\overline{f}(x) = x^n + \overline{a_{n-1}}x^{n-1} + \ldots \overline{a_1}x + \overline{a}_0$.

4. Determine a real polynomial of least degree which is divisible by $x^2 - 3x + (3 - i)$.

5. Assume that $f(x)$ and $g(x)$ are real polynomials and that $3 + 4i$ is a root of both polynomials. Prove that $f(x)$ and $g(x)$ have a common irreducible quadratic real polynomial as a factor.

In Exercises 6–9 for a polynomial $\sum_{i=0}^{n} a_i x^i \in \mathbb{F}[x]$ the formal derivative, $D(f(x))$, is given by $D(f(x)) := \sum_{i=1}^{n} i a_i x^{i-1}$.

6, Let $g(x), g(x) \in \mathbb{F}[x]$. Prove that $D(f(x) + g(x)) = D(f(x)) + D(g(x))$.

7. For $f(x) \in \mathbb{F}[x]$ and $c \in \mathbb{F}$, prove that $D(cf(x)) = cD(f(x))$.

8. Let $f(x), g(x) \in \mathbb{F}[x]$. Prove that $D(f(x)g(x)) = D(f(x))g(x) + f(x)D(g(x))$.

9. Let $f(x)$ be a polynomial of degree n with coefficients in a field $\mathbb{F}$. Assume that $f(x)$ is a product of linear polynomials in $\mathbb{F}[x]$. Prove that $f(x)$ has n distinct roots if and only if $f(x)$ and $D(f(x))$ are relatively prime.

10. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be distinct elements of the field $\mathbb{F}$. Set

$$F(x) = \prod_{i=1}^{n}(x - \alpha_i), F_j(x) = \frac{F(x)}{(x - \alpha_j)}, j = 1, 2, \ldots, n.$$

Further, set $f_j(x) = \frac{F_j(x)}{F_j(\alpha_j)}$. Prove that $\mathcal{B} = (f_1(x), f_2(x), \ldots, f_n(x))$ is linearly independent in $\mathbb{F}_{(n-1)}[x]$, and, consequently, a basis. (Hint: Note that $f_i(\alpha_j) = 0$ if $i \neq j$ and $f_i(\alpha_i) = 1$.)

11. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be distinct elements of the field $\mathbb{F}$ and let $\beta_i \in \mathbb{F}$ for $1 \leq i \leq n$. Prove that there exists a unique polynomial $f(x)$ such that $f(\alpha_i) = \beta_i$ for all $i = 1, 2, \ldots, n$.

In Exercises 12 and 13, $\mathcal{B}$ is the basis for $\mathbb{F}_{(n-1)}[x]$ of Exercise 10.

12. Let $g(x) \in \mathbb{F}_{n-1}[x]$. Prove that the coordinate vector of $g(x)$ with respect to $\mathcal{B}$ is $\begin{pmatrix} g(\alpha_1) \\ g(\alpha_2) \\ \vdots \\ g(\alpha_n) \end{pmatrix}$.

13. Determine the change of basis matrix from $\mathcal{S} = (1, x, x^2, \dots, x^{n-1})$ to $\mathcal{B}$. Conclude that this matrix is invertible.

4

Theory of a Single Linear Operator

CONTENTS

In this chapter we determine the structure of a single linear operator on a finite-dimensional vector space. The first section deals with the concept of an invariant subspace of an operator and the annihilator of a vector with respect to an operator. In section two we introduce the notion of a cyclic operator and uncover its properties. Section three concerns maximal vectors, in particular, we show that such vectors exist. Section four develops the theory of indecomposable operators. In section five we obtain our main structure theorem. This is applied in section six where we are able to obtain nice matrix representations for the similarity class of an operator. In the final section we specialize and apply these results to operators on finite-dimensional real and complex vector spaces.

For a different approach to the results of this chapter, based on the theory of finitely generated modules over principal ideal domains, see ([13]).

4.1 Invariant Subspaces of an Operator

In this section, we begin by defining what it means to evaluate a polynomial at an operator T on a vector space V. We further introduce the notion of a T-invariant subspace for an operator T on a finite-dimensional vector space V over a field $\mathbb{F}$. Finally, we define the concept of an eigenvector as well as what it means for an operator to be cyclic.

What You Need to Know

The following concepts are fundamental to understanding the new material in this section: vector space over a field $\mathbb{F}$, basis of a vector space, dimension of a vector space, linear operator on a vector space V, matrix of a linear operator $T : V \to V$ with respect to basis $\mathcal{B}$ for V, a polynomial of degree d with coefficients in a field $\mathbb{F}$, a monic polynomial, divisibility of polynomials, and an ideal in $\mathbb{F}[x]$.

Let V be a vector space of dimension n and $T : V \to V$ a linear operator on V. We begin by giving meaning to $f(T)$ for a polynomial $f(x)$:

Definition 4.1 *Let $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$. Then by $f(T)$ we mean the linear operator $a_m T^m + a_{m-1}T^{m-1} + \ldots a_1 T + a_0 I_V$.*

Definition 4.2 *Let $T \in \mathcal{L}(V, V)$ and $\boldsymbol{v} \in V$. The* **order ideal of $\boldsymbol{v}$ with respect to** *T, denoted by $Ann(T, \boldsymbol{v})$, we mean the set of all polynomials $f(x)$ such that $\boldsymbol{v} \in Ker(f(T))$, that is, $f(T)(\boldsymbol{v}) = \mathbf{0}$:*

$$Ann(T, \boldsymbol{v}) = \{f(x) \in \mathbb{F}[x] | f(T)(\boldsymbol{v}) = \mathbf{0}\}.$$

In the definition, we refer to $Ann(T, \boldsymbol{v})$ as an ideal; in Exercise 1 you verify this.

A priori there is no reason to believe that for an arbitrary vector $\boldsymbol{v} \in V$ that there are any non-zero polynomials $f(x)$ such that $f(T)(\boldsymbol{v}) = \mathbf{0}$. However, in our next theorem, we prove for any vector $\boldsymbol{v}, Ann(T, \boldsymbol{v}) \neq \{0\}$.

Theorem 4.1 *Let V be an n-dimensional vector space, T a linear operator on V, and $\boldsymbol{v}$ a non-zero vector in V. Then there exists a non-zero polynomial $f(x)$ of degree at most n such that $f(T)(\boldsymbol{v}) = \mathbf{0}$.*

Proof *Since the dimension of V is n, any sequence of $n+1$ vectors is linearly dependent by Theorem (1.16). In particular, the sequence $(\boldsymbol{v}, T(\boldsymbol{v}), T^2(\boldsymbol{v}), \ldots, T^n(\boldsymbol{v}))$ is linearly dependent.*

Consequently, there are scalars $a_i, 0 \le i \le n$, not all zero, such that

$$a_0\boldsymbol{v} + a_1T(\boldsymbol{v}) + a_2T^2(\boldsymbol{v}) + \cdots + a_{n-1}T^{n-1}(\boldsymbol{v}) + a_nT^n(\boldsymbol{v}) = \mathbf{0}.$$

Set $f(x) = a_0 + a_1x + \cdots + a_nx^n$. Then $f(x) \neq 0$ since some $a_i \neq 0$ and $deg(f(x)) \le n$. Moreover,

$$\begin{aligned} f(T)(\boldsymbol{v}) &= (a_0I_V + a_1T + \cdots + a_{n-1}T^{n-1} + a_nT^n)(\boldsymbol{v}) \\ &= a_0\boldsymbol{v} + a_1T(\boldsymbol{v}) + a_2T^2(\boldsymbol{v}) + \cdots + a_{n-1}T^{n-1}(\boldsymbol{v}) + a_nT^n(\boldsymbol{v}) \\ &= \mathbf{0}. \end{aligned}$$

Thus, $f(x) \in Ann(T, \boldsymbol{v})$.

As previously mentioned, in Exercise 1, you are asked to prove for any operator T and vector $\boldsymbol{v} \in V$, $Ann(T, \boldsymbol{v})$ is an ideal in the algebra $\mathbb{F}[x]$. By Exercise 4 of Section (3.1), $Ann(T, \boldsymbol{v})$ contains a monic polynomial $\mu(x)$ such that every polynomial in $Ann(T, \boldsymbol{v})$ is a multiple of $\mu(x)$. Recall such a polynomial is called a ***generator*** of $Ann(T, \boldsymbol{v})$. This motivates the following definition:

Definition 4.3 *Let V be a finite-dimensional vector space, T an operator on V, and $\boldsymbol{v}$ a vector in V. The unique monic generator of $Ann(T, \boldsymbol{v})$ is called the* **minimal polynomial of T with respect to $\boldsymbol{v}$**. *It is also sometimes referred to as the* **order of $\boldsymbol{v}$ with respect to T**. *It is denoted here by $\mu_{T,\boldsymbol{v}}(x)$.*

Remark 4.1 *Suppose $g(x) \in \mathbb{F}[x]$ and $g(T)(\boldsymbol{v}) = \mathbf{0}$. Then $\mu_{T,\boldsymbol{v}}(x)$ divides $g(x)$.*

Example 4.1 *Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ be defined by*

$$T(\boldsymbol{v}) = \begin{pmatrix} 2 & -1 & 1 \\ -3 & 4 & -5 \\ -3 & 3 & -4 \end{pmatrix} \boldsymbol{v}.$$

Let $\boldsymbol{v} = \begin{pmatrix} -1 \\ 2 \\ 2 \end{pmatrix}$. Determine $\mu_{T,\boldsymbol{v}}(x)$.

$$T(\boldsymbol{v}) = \begin{pmatrix} -2 \\ 1 \\ 1 \end{pmatrix}, T^2(\boldsymbol{v}) = \begin{pmatrix} -4 \\ 5 \\ 5 \end{pmatrix}, T^3(\boldsymbol{v}) = \begin{pmatrix} -8 \\ 7 \\ 7 \end{pmatrix}.$$

We find the null space of the matrix

$$A = (\boldsymbol{v} \;\; T(\boldsymbol{v}) \;\; T^2(\boldsymbol{v}) \;\; T^3(\boldsymbol{v})) = \begin{pmatrix} -1 & -2 & -4 & -8 \\ 2 & 1 & 5 & 7 \\ 2 & 1 & 5 & 7 \end{pmatrix}.$$

The reduced echelon form of A is $\begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$.

We conclude from this that $null(A) = Span \left\{ \begin{pmatrix} -2 \\ -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -2 \\ -3 \\ 0 \\ 1 \end{pmatrix} \right\}$.

Each of these basis vectors corresponds to a polynomial in $Ann(T, \boldsymbol{v})$*: From the vector* $\begin{pmatrix} -2 \\ -1 \\ 1 \\ 0 \end{pmatrix}$ *we obtain the polynomial* $f(x) = x^2 - x - 2 = (x+1)(x-2)$*. The vector* $\begin{pmatrix} -2 \\ -3 \\ 0 \\ 1 \end{pmatrix}$ *gives the polynomial* $g(x) = x^3 - x^2 - 3x - 2 = (x+1)(x^2 - x - 2) = (x+1)^2(x-2)$*. It now follows that* $Ann(T, \boldsymbol{v}) = \{a(x)f(x) | a(x) \in \mathbb{F}[x]\}$*. Thus,* $\mu_{T,\boldsymbol{v}}(x) = x^2 - x - 2$.

We now proceed to prove some results about the annihilator ideal and minimal polynomial of an operator with respect to a vector. These will be fundamental to our main goal of understanding the structure of a single linear operator. Before doing so, we introduce some additional definitions:

Definition 4.4 *Let V be a vector space and T an operator on V. A subspace W of V is said to be* T**-invariant** *if $T(\boldsymbol{w}) \in W$ for all $\boldsymbol{w} \in W$.*

Remark 4.2 *Assume V is a vector space, $T \in \mathcal{L}(V, V)$ and W is a T-invariant subspace. Then the restriction of T to W, denoted by $T_{|W}$, is an operator on W.*

Definition 4.5 *Let V be a finite-dimensional vector space, T an operator on V, and $\boldsymbol{v}$ a vector from V. Then the* **T-cyclic subspace generated by $\boldsymbol{v}$** *is $\{f(T)(\boldsymbol{v})|f(x) \in \mathbb{F}[x]\}$. We will denote this by $\langle T, \boldsymbol{v}\rangle$. By the* **order** *of the T-cyclic subspace $\langle T, \boldsymbol{v}\rangle$ generated by $\boldsymbol{v}$, we will mean the polynomial $\mu_{T,\boldsymbol{v}}(x)$.*

Example 4.2 *Let T be an operator on the finite-dimensional vector space V. For any subset of vectors $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k\}$ from $Ker(T), Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k)$ is a T-invariant subspace. In particular, if $\boldsymbol{v} \in Ker(T)$ then $\langle T, \boldsymbol{v}\rangle = Span(\boldsymbol{v}) = \{a\boldsymbol{v}|a \in \mathbb{F}\}$ is T-invariant.*

A more interesting example is when $\boldsymbol{v} \notin Ker(T)$ and $Span(\boldsymbol{v})$ is T-invariant. In this case, $T(\boldsymbol{v}) = \lambda\boldsymbol{v}$ for some non-zero scalar λ. This motivates the following definition.

Definition 4.6 *Let T be an operator on a vector space V. A vector $\boldsymbol{v}$ is said to be an* **eigenvector** *of T with* **eigenvalue** *λ if $T(\boldsymbol{v}) = \lambda\boldsymbol{v}$. The* **spectrum** *of the operator T is the set of all eigenvalues of T. This is denoted by $Spec(T)$.*

We have a corresponding definition for matrices:

Definition 4.7 *Let A be an $n \times n$ matrix with entries in the field $\mathbb{F}$. An* **eigenvector** *of A is an $n \times 1$ matrix X such that $AX = \lambda X$ for some scalar $\lambda \in \mathbb{F}$. The scalar λ is an* **eigenvalue** *of A. The* **spectrum** *of the matrix A is the set of all eigenvalues of A. This is denoted by $Spec(A)$.*

Remark 4.3 *When computing the spectrum of an operator or matrix it is important to specify what field one is over. As an example, the spectrum of the matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ when viewed as a real matrix is the empty set, whereas it is $\{i, -i\}$ when viewed as a complex matrix.*

The following definition will make an appearance later when we introduce the notion of a norm of an operator.

Definition 4.8 *Let V be a finite-dimensional vector space over $\mathbb{C}$ and $T : V \to V$ an operator. The* **spectral radius** *of T, denoted by $\rho(T)$, is the maximum of $\{|\lambda||\lambda \in Spec(T)\}$.*

The following theorem enumerates many of the properties of the T-cyclic subspace generated by a vector $\boldsymbol{v}$.

Theorem 4.2 *Let V be a finite-dimensional vector space, T an operator on V, and $\boldsymbol{v}$ a vector from V. Then the following hold:*

i) $\langle T, \boldsymbol{v}\rangle$ is a T-invariant subspace of V.

ii) If W is a T-invariant subspace of V, and $\boldsymbol{v} \in W$, then $\langle T, \boldsymbol{v}\rangle \subset W$.

iii) If $\mu_{T,\boldsymbol{v}}(x)$ has degree d, then $(\boldsymbol{v}, T(\boldsymbol{v}), \ldots, T^{d-1}(\boldsymbol{v}))$ is a basis for $\langle T, \boldsymbol{v}\rangle$.

Proof *i) We need to show that $\langle T, \boldsymbol{v}\rangle$ is closed under addition and scalar multiplication and for an arbitrary $\boldsymbol{x} \in \langle T, \boldsymbol{v}\rangle$ that $T(\boldsymbol{x}) \in \langle T, \boldsymbol{v}\rangle$.*

Suppose $\boldsymbol{x}, \boldsymbol{y} \in \langle T, \boldsymbol{v}\rangle$ and $c \in \mathbb{F}$. By the definition of $\langle T, \boldsymbol{v}\rangle$, there are polynomials $f(x)$ and $g(x)$ such that $\boldsymbol{x} = f(T)(\boldsymbol{v})$ and $\boldsymbol{y} = g(T)(\boldsymbol{v})$. Then $\boldsymbol{x} + \boldsymbol{y} = f(T)(\boldsymbol{v}) + g(T)(\boldsymbol{v}) = (f(T) + g(T))(\boldsymbol{v}) = [(f+g)(T)](\boldsymbol{v}) \in \langle T, \boldsymbol{v}\rangle$.

We also have $c\boldsymbol{x} = c(f(T)(\boldsymbol{v}) = [cf(T)](\boldsymbol{v}) = [(cf)(T)](\boldsymbol{v})$. Since $(cf)(x)$ is a polynomial it follows that $c\boldsymbol{x} \in \langle T, \boldsymbol{v}\rangle$.

Finally, assume $\boldsymbol{x} \in \langle T, \boldsymbol{v}\rangle$. Then there exists a polynomial $f(x)$ such that $\boldsymbol{x} = f(T)(\boldsymbol{v})$. Set $g(x) = xf(x)$. Now $T(\boldsymbol{x}) = T(f(T)(\boldsymbol{v})) = (Tf(T))(\boldsymbol{v}) = g(T)(\boldsymbol{v}) \in \langle T, \boldsymbol{v}\rangle$ as required.

ii) Assume W is a T-invariant subspace of V and $\boldsymbol{v} \in W$. Then by induction $T^k(\boldsymbol{v}) \in W$ for all natural numbers k. Since W is a subspace, it is closed under scalar multiplication and therefore for any scalar $a_k, a_kT^k(\boldsymbol{v}) \in W$. Finally, W is closed under addition from which we can conclude that an arbitrary sum $a_0\boldsymbol{v} + a_1T(\boldsymbol{v}) + \cdots + a_kT^k(\boldsymbol{v}) \in W$. But this implies for all polynomials $f(x)$ that $f(T)(\boldsymbol{v}) \in W$, hence $\langle T, \boldsymbol{v}\rangle \subset W$.

iii) We need to prove that $(\boldsymbol{v}, T(\boldsymbol{v}), \ldots, T^{d-1}(\boldsymbol{v}))$ is linearly independent and spans $\langle T, \boldsymbol{v}\rangle$.

Suppose $a_0\boldsymbol{v} + a_1T(\boldsymbol{v}) + \cdots + a_{d-1}T^{d-1}(\boldsymbol{v}) = \mathbf{0}$. Set $f(x) = a_0 + a_1x + \cdots + a_{d-1}x^{d-1}$. Then $f(x) \in Ann(T, \boldsymbol{v})$. By assumption, the least degree of a non-zero polynomial in $Ann(T, \boldsymbol{v})$ is d. If $f(x) \neq 0$, then $deg(f(x)) < d$, a contradiction. Thus, $f(x) = 0$ and $a_0 = a_1 = \cdots = a_{d-1} = 0$. Consequently, the sequence $(\boldsymbol{v}, T(\boldsymbol{v}), \ldots, T^{d-1}(\boldsymbol{v}))$ is linearly independent.

Next, let $f(x) \in \mathbb{F}[x]$ be arbitrary. Write $f(x) = q(x)\mu_{T,\boldsymbol{v}}(x) + r(x)$, where $r(x) = 0$ or $deg(r(x)) < \mu_{T,\boldsymbol{v}}(x) = d$. If $r(x) = 0$ the $f(T)(\boldsymbol{v}) = q(T)(\mu_{T,v}(T)(\boldsymbol{v})) = \mathbf{0}$ so $f(T)(\boldsymbol{v}) \in Span(\boldsymbol{v}, T(\boldsymbol{v}), \ldots, T^d(\boldsymbol{v}))$. We may therefore assume that $r(x) \neq 0$.

Let $r(x) = b_0 + b_1x + \cdots + b_{d-1}x^{d-1}$. Now

$$f(T)(\boldsymbol{v}) = [q(T)\mu_{T,\boldsymbol{v}}(T) + r(T)](\boldsymbol{v}) = q(T)(\mu_{T,\boldsymbol{v}}(T)(\boldsymbol{v})) + r(T)(\boldsymbol{v}).$$

However, $\mu_{T,\boldsymbol{v}}(T)(\boldsymbol{v}) = \mathbf{0}$ and therefore

$$f(T)(\boldsymbol{v}) = r(T)(\boldsymbol{v}) = b_0\boldsymbol{v} + b_1T(\boldsymbol{v}) + \cdots + b_{d-1}T^{d-1}(\boldsymbol{v}),$$

which proves that $(\boldsymbol{v}, T(\boldsymbol{v}), \ldots, T^{d-1}(\boldsymbol{v}))$ *spans* $\langle T, \boldsymbol{v}\rangle$.

Let V be a finite-dimensional vector space. We shall see below that there are polynomials that annihilate T independent of any particular vector. This motivates the following definition:

Definition 4.9 *Let V be a finite-dimensional vector space, T an operator on V. Then the* **annihilator ideal** *of T on V, denoted by $Ann(T, V)$ or just $Ann(T)$, consists of all polynomials $f(x)$ such that $f(T)$ is the zero operator:*

$$Ann(T) = \{f(x) \in \mathbb{F}[x] | f(T)(\boldsymbol{v}) = \mathbf{0}, \forall \boldsymbol{v} \in V\}.$$

Again we are confronted with the question of whether there are non-zero polynomials in $Ann(T)$. The next theorem answers this affirmatively:

Theorem 4.3 *Let V be an n-dimensional vector space and T an operator on V. Then there exists a non-zero polynomial $f(x)$ of degree at most n^2 such that $f(T) = \mathbf{0}_{V\to V}$.*

Proof *We have previously shown that $dim(\mathcal{L}(V, V))$ is n^2. As a consequence any sequence of $n^2 + 1$ operators is linearly dependent, in particular, the sequence*

$$(I_V, T, T^2, \ldots, T^{n^2}).$$

It therefore follows that there are scalars $a_i, 0 \leq i \leq n^2$, not all zero such that

$$a_0I_V + a_1T + a_2T^2 + \cdots + a_{n^2}T^{n^2} = \mathbf{0}_{V\to V}.$$

Set $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n^2}x^{n^2}$. Then $deg(f(x)) \leq n^2$ and $f(x) \neq 0$ since some coefficient is non-zero. Finally, $f(T) = \mathbf{0}_{V\to V}$.

Definition 4.10 *Let V be a finite-dimensional vector space and T a linear operator on V. The unique monic polynomial of least degree in $Ann(T, V)$ is called the* **minimal polynomial of** *T. This polynomial is denoted by $\mu_T(x)$.*

Remark 4.4 *Suppose $g(x) \in \mathbb{F}[x]$ and $g(T)(\boldsymbol{v}) = \mathbf{0}$ for all vectors $\boldsymbol{v} \in V$. Then it is consequence of the definition that $\mu_T(x)|g(x)$.*

Remark 4.5 *Let T be an operator on a finite-dimensional vector space V and $\boldsymbol{v} \in V$. Then $\mu_{T,\boldsymbol{v}}(x)|\mu_T(x)$.*

Remark 4.6 *If $dim(V) = n$, we presently have $deg(\mu_T(x)) \leq n^2$ but we will make a substantial improvement on this.*

Exercises

1. Give an explicit description of an operator $T \in \mathcal{L}(\mathbb{R}^3, \mathbb{R}^3)$ such that $T(U) \neq U$, where $U = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ 0 \end{pmatrix} \mid x_1, x_2 \in \mathbb{R} \right\}$.

2. Let V be a finite-dimensional vector space over the field $\mathbb{F}$ and assume U is a subspace, $U \neq V, \{\mathbf{0}\}$. Prove that there is an operator $T \in \mathcal{L}(V, V)$ such that $T(U) \neq U$.

3. Determine the minimal polynomial of the operator T from Example (4.1) with respect to the vector $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$.

4. Find $\mu_{T,\boldsymbol{y}}(x)$ for the operator T of Example (4.1) if $\boldsymbol{y} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$.

5. Let V be a finite-dimensional vector space over the field $\mathbb{F}$, $S, T \in \mathcal{L}(V, V)$, and assume $ST = TS$. If $\boldsymbol{v} \in V$ is an eigenvector of S with eigenvalue λ, prove that $T(\boldsymbol{v})$ is also an eigenvector of S with eigenvalue λ.

6. Let V be a finite-dimensional vector space and assume that $T \in \mathcal{L}(V, V)$ is invertible and U is a T-invariant subspace of V. Prove that U is a T^{-1}-invariant subspace of V.

7. Assume V is a finite-dimensional vector space over a field $\mathbb{F}$, where $2 \neq 0$ and $T \in \mathcal{L}(V, V)$ satisfies $T^2 = I_V$. Set $E_1 = \{\boldsymbol{v} \in V | T(\boldsymbol{v}) = \boldsymbol{v}\}$ and $E_{-1} = \{\boldsymbol{v} \in V | T(\boldsymbol{v}) = -\boldsymbol{v}\}$. Prove that $V = E_1 \oplus E_{-1}$.

8. Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ be the linear operator given by $T \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_3 \\ x_1 \\ x_2 \end{pmatrix}$. Determine all T-invariant subspaces of $\mathbb{R}^3$.

9. Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ be the linear operator given by $T \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_3 \\ 0 \end{pmatrix}$. Determine all T-invariant subspaces of $\mathbb{R}^3$.

10. Let V be a vector space over the field $\mathbb{F}$ and T an operator on V. Set $\mathcal{P}(T) = \{f(T)|f(x) \in \mathbb{F}[x]\}$. Prove that $\mathcal{P}(T)$ is an algebra over $\mathbb{F}$.

11. Let V be a finite-dimensional vector space over a field $\mathbb{F}$, $T \in \mathcal{L}(V,V)$, and $\boldsymbol{v} \in V$. Prove that $Ann(T, \boldsymbol{v})$ is an ideal of $\mathbb{F}[x]$.

12. Prove if U, W are T-invariant subspaces of the space V then $U + W$ and $U \cap W$ are a T-invariant subspaces of V.

13. Prove that $Ann(T)$ is an ideal in $\mathbb{F}[x]$.

14. Let T be an operator on the finite-dimensional vector space V. Prove that if T has an eigenvector, then $\mu_T(x)$ has a linear factor. The converse is true, but we leave it to section three.

15. Let T be an operator on the finite-dimensional vector space V and let $\mathcal{B}$ be a basis for V. Prove that a vector $\boldsymbol{v}$ is an eigenvector of T with eigenvalue λ if and only if the coordinate vector $[\boldsymbol{v}]_{\mathcal{B}}$ is an eigenvector of the matrix $\mathcal{M}_T(\mathcal{B}, \mathcal{B})$ with eigenvalue λ.

16. Let T be an operator on a finite-dimensional vector space V, $\mathcal{B} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ a basis for V, and $f(x) \in \mathbb{F}[x]$. Set $A = \mathcal{M}_T(\mathcal{B}, \mathcal{B})$. Prove that $f(T) = \mathbf{0}_{V \to V}$ if and only if $f(A) = 0_{nn}$.

17. Let S be an operator on the finite-dimensional vector space V and $\mathcal{B}$ be a basis for V. Let S' be the operator such that $\mathcal{M}_{S'}(\mathcal{B}, \mathcal{B}) = \mathcal{M}_S(\mathcal{B}, \mathcal{B})^{tr}$. Prove that S and S' have the same minimal polynomial. (Hint: For a square matrix A and a polynomial $f(x), f(A^{tr}) = f(A)^{tr}$).

18. Assume T is an invertible linear operator on the finite-dimensional vector space V and $\boldsymbol{v}$ is an eigenvector of T with eigenvalue λ. Prove that $\boldsymbol{v}$ is an eigenvector of T^{-1} with eigenvalue $\frac{1}{\lambda}$.

19. Assume T is a linear operator on the finite-dimensional vector space V over the field $\mathbb{F}$ and $\boldsymbol{v}$ is an eigenvector of T with eigenvalue λ. If $f(x) \in \mathbb{F}[x]$, prove that $\boldsymbol{v}$ is an eigenvector of $f(T)$ with eigenvalue $f(\lambda)$.

20. Let V be a finite-dimensional vector space over the field $\mathbb{F}; S, T$ linear operators on V; and assume that S is invertible. If $\boldsymbol{v}$ is an eigenvector of T with eigenvalue λ, prove that $S^{-1}(\boldsymbol{v})$ is an eigenvector of $S^{-1}TS$ with eigenvalue λ.

21. Let S, T be linear operators on the finite-dimensional vector space V over a field $\mathbb{F}$. Prove that $\mu_{ST}(x)$ divides $x\mu_{TS}(x)$ and $\mu_{TS}(x)$ divides $x\mu_{ST}(x)$. Use this to conclude that ST and TS have the same eigenvalues.

22. Let T be a linear operator on the finite-dimensional vector space V over the field $\mathbb{F}$, and $g(x) \in \mathbb{F}[x]$. Prove that $Ker(g(T))$ is a T-invariant subspace of V.

4.2 Cyclic Operators

In this short section, we assume that V is a finite-dimensional vector space, T is a linear operator on V, and $\boldsymbol{v}$ is a vector from V such that $V = \langle T, \boldsymbol{v}\rangle$. We investigate properties of such an operator.

What You Need to Know

The following concepts are fundamental to understanding the new material in this section: vector space over a field $\mathbb{F}$, basis of a vector space, dimension of a vector space, linear operator on a vector space V, matrix of a linear operator $T : V \to V$ with respect to a basis $\mathcal{B}$ for V, a polynomial of degree d with coefficients in a field $\mathbb{F}$, the evaluation $f(T)$ of a polynomial f at an operator T of a finite-dimensional vector space V, invariant subspace of an operator T on a vector space V, the T-cyclic subspace $\langle T, \boldsymbol{v}\rangle$ generated by a vector $\boldsymbol{v}$, the annihilator ideal of a vector with respect to an operator, the minimal polynomial of an operator with respect to a vector, the annihilator ideal of an operator T, the minimal polynomial of an operator T, eigenvalue and eigenvector of an operator T.

Definition 4.11 *Let V be a finite-dimensional vector space and T an operator on V. T is said to be a* **cyclic** *operator if there is a vector $\boldsymbol{v} \in V$ such that $V = \langle T, \boldsymbol{v}\rangle$.*

Lemma 4.1 *Assume T is a cyclic operator on the finite-dimensional vector space V and $\langle T, \boldsymbol{v}\rangle = V$. Then $\mu_{T,\boldsymbol{v}}(x) = \mu_T(x)$.*

Proof *By Remark (4.1), we know that $\mu_{T,\boldsymbol{v}}(x)$ divides $\mu_T(x)$ since $\mu_T(T)(\boldsymbol{v}) = \mathbf{0}_{V\to V}(\boldsymbol{v}) = \mathbf{0}$. On the other hand, for any vector $\boldsymbol{u} \in V$, there is a polynomial $g(x)$ such that $\boldsymbol{u} = g(T)(\boldsymbol{v})$. Then $\mu_{T,\boldsymbol{v}}(T)(\boldsymbol{u}) = \mu_{T,\boldsymbol{v}}(T)(g(T)(\boldsymbol{v})) = [\mu_{T,\boldsymbol{v}}(T)g(T)](\boldsymbol{v}) = [g(T)\mu_{T,\boldsymbol{v}}(T)](\boldsymbol{v}) = g(T)(\mu_{T,\boldsymbol{v}}(T)(\boldsymbol{v})) = g(T)(\mathbf{0}) = \mathbf{0}$. Thus, $\mu_{T,\boldsymbol{v}}(T)(\boldsymbol{u}) = \mathbf{0}$ for all vectors $\boldsymbol{u} \in V$. By Remark (4.4), we can conclude that $\mu_T(x)$ divides $\mu_{T,\boldsymbol{v}}(x)$. Consequently, by Lemma (3.3), there is a scalar a such that $\mu_T(x) = a\mu_{T,\boldsymbol{v}}(x)$. However, since both polynomials are monic, it follows that $a = 1$ and they are equal.*

For the remainder of this section, we assume that T is a cyclic operator on the finite-dimensional vector space V and that $V = \langle T, \boldsymbol{v}\rangle$. For convenience of notation, we set $f(x) = \mu_T(x) = \mu_{T,\boldsymbol{v}}(x)$. In our next result, we investigate $\mu_{T,g(T)(\boldsymbol{v})}(x)$.

Theorem 4.4 *Let $g(x) \in \mathbb{F}[x]$. Set $\boldsymbol{y} = g(T)(\boldsymbol{v}), d(x) = gcd(f(x), g(x))$ and $h(x) = \frac{f(x)}{d(x)}$. Then $h(x) = \mu_{T,\boldsymbol{y}}(x)$.*

Proof *Note that $d(x)$ is monic and divides $\mu_{T,\boldsymbol{v}}(x)$. Since $\mu_{T,\boldsymbol{v}}$ is monic the quotient, $h(x)$, is monic. We show that $h(x)$ divides $\mu_{T,\boldsymbol{y}}(x)$ and $\mu_{T,\boldsymbol{y}}(x)$ divides $h(x)$. Since both are monic, equality will follow.*

We claim that $h(T)(\boldsymbol{y}) = \mathbf{0}$. Let $g(x) = d(x)g'(x)$. We then have

$$h(T)(\boldsymbol{y}) = h(T)[g(T)(\boldsymbol{v})] = [h(T)g(T)](\boldsymbol{v}) =$$

$$[h(T)(d(T)g'(T))](\boldsymbol{v}) = [f(T)g'(T)](\boldsymbol{v}) = [g'(T)f(T)](\boldsymbol{v}) =$$

$$g'(T)(f(T)(\boldsymbol{v})) = g'(T)(\mathbf{0}) = \mathbf{0}.$$

Since $h(T)(\boldsymbol{y}) = \mathbf{0}$ it follows from Remark (4.1) that $\mu_{T,\boldsymbol{y}}(x)$ divides $h(x)$.

On the other hand,

$$\mathbf{0} = \mu_{T,\boldsymbol{y}}(T)(\boldsymbol{y}) = \mu_{T,\boldsymbol{y}}(T)(g(T)(\boldsymbol{v})) = [\mu_{T,\boldsymbol{y}}(T)g(T)](\boldsymbol{v}).$$

Therefore, by Remark (4.1), $f(x) = \mu_{T,\boldsymbol{v}}(x)$ divides $\mu_{T,\boldsymbol{y}}(x)g(x)$. Since $f(x) = d(x)h(x)$ and $g(x) = d(x)g'(x)$, it follows that $h(x)$ divides $\mu_{T,\boldsymbol{y}}(x)g'(x)$. However, by Exercise 7 of Section (3.1), $h(x)$ and $g'(x)$ are relatively prime. Consequently, $h(x)$ divides $\mu_{T,\boldsymbol{y}}(x)$.

In our final result, we prove that every T-invariant subspace of $V = \langle T, \boldsymbol{v}\rangle$ is cyclic.

Theorem 4.5 *Let W be a T-invariant subspace of $V = \langle T, \boldsymbol{v}\rangle$. Then there exists a vector $\boldsymbol{w} \in W$ such that $W = \langle T, \boldsymbol{w}\rangle$. If $g(x) = \mu_{T,\boldsymbol{w}}(x)$ then $g(x)$ divides $f(x)$. Moreover, for each monic divisor $g(x)$ of $f(x)$, there is a unique T-invariant subspace W of V such that $\mu_{T_{|W}}(x) = g(x)$.*

Proof *If $W = \{\mathbf{0}\}$, then $W = \langle T, \mathbf{0}\rangle$, and we are done. Therefore, we may assume that $W \neq \{\mathbf{0}\}$. Let $\boldsymbol{u} \neq \mathbf{0}$ be a vector in W. Let $k(x)$ be a polynomial such that $\boldsymbol{u} = k(T)(\boldsymbol{v})$.*

Now let $J = \{l(x) \in \mathbb{F}[x] | l(T)(\boldsymbol{v}) \in W\}$; this is an ideal of $\mathbb{F}[x]$. We have just demonstrated that there exists non-zero polynomials in J. Choose a monic polynomial $h(x)$ in J of minimal degree and set $\boldsymbol{w} = h(T)(\boldsymbol{v})$. We claim that $W = \langle T, \boldsymbol{w}\rangle$. Suppose to the contrary that $\boldsymbol{y} \in W \setminus \langle T, \boldsymbol{w}\rangle$. Let $\boldsymbol{y} = m(T)(\boldsymbol{v})$ for a polynomial $m(x)$. Suppose $h(x)$ divides $m(x)$, say, $m(x) = q(x)h(x)$. Then

$m(T)(\boldsymbol{v}) = [q(T)h(T)](\boldsymbol{v}) = q(T)(h(T)(\boldsymbol{v}) = q(T)(\boldsymbol{w}) \in \langle T, \boldsymbol{w}\rangle$, contradicting our assumption. Thus, $h(x)$ does not divide $m(x)$. Now apply the division algorithm to write $m(x) = q(x)h(x) + r(x)$ with $r(x) \neq 0$ and $deg(r(x)) < deg(h(x))$.

Now

$$r(T)(\boldsymbol{v}) = [m(T) - q(T)h(T)](\boldsymbol{v}) =$$
$$m(T)(\boldsymbol{v}) - q(T)(h(T)(\boldsymbol{v})) = \boldsymbol{y} - q(T)(\boldsymbol{w}) \in W.$$

However, since $deg(r(x)) < deg(h(x))$, this contradicts the minimality of the degree of $h(x)$. This proves that $W = \langle T, \boldsymbol{w}\rangle$ as claimed.

We next demonstrate that $h(x)$ divides $f(x)$. Set $d(x) = gcd(f(x), h(x))$. We need to show that $d(x) = h(x)$. Write $h(x) = h'(x)d(x), f(x) = f'(x)d(x)$. Also set $\boldsymbol{w}' = d(T)(\boldsymbol{v})$ and $W' = \langle T, \boldsymbol{w}'\rangle$. Since $\boldsymbol{w} = h'(T)(\boldsymbol{w}')$ it follows that $\boldsymbol{w} \in W'$ and therefore $W \subset W'$. On the other hand, $f'(x)$ and $h'(x)$ are relatively prime. Therefore, there are polynomials $a(x)$ and $b(x)$ such that

$$a(x)f'(x) + b(x)h'(x) = 1.$$

Multiplying by $d(x)$ we get

$$a(x)f'(x)d(x) + b(x)h'(x)d(x) = a(x)f(x) + b(x)h(x) = d(x).$$

It then follows that

$$\begin{aligned} \boldsymbol{w}' = d(T)(\boldsymbol{v}) &= [a(T)f(T) + b(T)h(T)](\boldsymbol{v}) \\ &= a(T)f(T)(\boldsymbol{v}) + b(T)h(T)(\boldsymbol{v}) \\ &= b(T)(\boldsymbol{w}), \end{aligned}$$

the latter equality since $f(T) = \boldsymbol{0}_{V\to V}$. We can therefore conclude that $\boldsymbol{w}' \in \langle T, \boldsymbol{w}\rangle = W$ and therefore $W' = W$. This implies that $d(x) \in J$. Since $d(x)$ divides $h(x)$ and $h(x)$ was chosen to have minimal degree among polynomials in J, we can conclude that $d(x)$ and $h(x)$ have the same degree. However, both are monic and this implies that $d(x) = h(x)$.

Now set $g(x) = \mu_{T,\boldsymbol{w}}(x)$. Since $\boldsymbol{w} = h(T)(\boldsymbol{v})$ by Theorem (4.4), it follows that $g(x) = \frac{\mu_T(x)}{h(x)}$, which divides $\mu_T(x) = f(x)$ as claimed.

Next we need to show for any monic divisor $g(x)$ there is a unique T-invariant subspace $W = \langle T, \boldsymbol{w}\rangle$ such that $\mu_{T,\boldsymbol{w}}(x) = g(x)$. Set $h(x) = \frac{f(x)}{g(x)}$ and $\boldsymbol{w} = h(T)(\boldsymbol{v})$. Then by Theorem (4.4), we know that

$$\mu_{T,\boldsymbol{w}}(x) = \frac{f(x)}{gcd(f(x), h(x))} = \frac{f(x)}{h(x)} = g(x).$$

This proves the existence of W.

On the other hand, suppose $\boldsymbol{w}' \in V$ *and* $\mu_{T,\boldsymbol{w}'}(x) = g(x)$. *Let* $\boldsymbol{w}' = k(T)(\boldsymbol{v})$ *and set* $d(x) = gcd(f(x), k(x))$. *Then* $g(x) = \frac{f(x)}{d(x)}$ *and therefore* $d(x) = h(x)$. *If we write* $k(x) = k'(x)h(x)$, *then* $\boldsymbol{w}' = k(T)(\boldsymbol{v}) = k'(T)h(T)(\boldsymbol{v}) = k'(T)(\boldsymbol{w})$ *and hence* $\boldsymbol{w}' \in \langle T, \boldsymbol{w}\rangle$. *Then* $W' \subset W$. *However,* $dim(W') = deg((g(x)) = dim(W)$, *and we can finally conclude that* $W' = W$.

Exercises

1. Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ be the transformation given by

$$T(\boldsymbol{v}) = \begin{pmatrix} 2 & -2 & 3 \\ 1 & 0 & 2 \\ -1 & 2 & 0 \end{pmatrix} \boldsymbol{v}.$$

a) Set $\boldsymbol{z} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$. Prove that $\mathbb{R}^3 = \langle T, \boldsymbol{z}\rangle$ and determine $\mu_{T,\boldsymbol{z}}(x)$.

b) Set $\boldsymbol{u} = (T^2 + I_V)(\boldsymbol{z})$. Determine $\mu_{T,\boldsymbol{u}}(x)$.

2. Let $T : \mathbb{R}^4 \to \mathbb{R}^4$ be given by

$$T(\boldsymbol{v}) = \begin{pmatrix} 0 & 0 & 0 & -4 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -5 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Set $\boldsymbol{z} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$. Prove that $\mathbb{R}^4 = \langle T, \boldsymbol{z}\rangle$ and determine $\mu_T(x)$.

3. Assume the operator T on the vector space V has no non-trivial invariant subspaces. Prove that T is cyclic.

4. Give an example of a cyclic operator T on $\mathbb{R}^4$ such that the subspaces $\left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ 0 \end{pmatrix} \mid x_1, x_2, x_3 \in \mathbb{R} \right\}$, $\left\{ \begin{pmatrix} x_1 \\ x_2 \\ 0 \\ 0 \end{pmatrix} \mid x_1, x_2 \in \mathbb{R} \right\}$ and $\left\{ \begin{pmatrix} x_1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \mid x_1 \in \mathbb{R} \right\}$ are T-invariant.

5. Assume T is a cyclic operator on $\mathbb{R}^3$. Let N be the number of T-invariant subspaces. Prove that $N \in \{4, 6, 8\}$.

6. Give an example of a cyclic operator T on $\mathbb{R}^3$, which has exactly four subspaces that are T-invariant.

7. Give an example of a cyclic operator T on $\mathbb{R}^3$, which has exactly six subspaces that are T-invariant. .

8. Assume T is a cyclic operator on $\mathbb{R}^4$. Let N be the number of T-invariant subspaces. Prove that $N \in \{3, 4, 5, 6, 8, 9, 12, 16\}$.

9. Give an example of a cyclic operator T on $\mathbb{R}^4$, which has exactly three subspaces that are T-invariant.

10. Give an example of a cyclic operator T on $\mathbb{R}^4$, which has exactly 12 subspaces that are T-invariant.

11. Give an example of a cyclic operator T on $\mathbb{R}^4$, which has exactly 16 subspaces that are T-invariant.

12. Let V be an n-dimensional vectors space. Assume $T : V \to V$ is cyclic, say $V = \langle T, \boldsymbol{v} \rangle$. Let $S \in \mathcal{L}(V, V)$ and assume that $ST = TS$. Prove there exists a polynomial $g(x) \in \mathbb{F}_{(n-1)}[x]$ such that $S = g(T)$.

4.3 Maximal Vectors

In this section, we consider a linear operator T on a finite-dimensional vector space V. We prove the existence of vectors $\boldsymbol{v}$ such that $\mu_{T,\boldsymbol{v}}(x) = \mu_T(x)$.

What You Need to Know

The following concepts are fundamental to understanding the new material in this section: vector space over a field $\mathbb{F}$, basis of a vector space, dimension of a vector space, linear operator on a vector space V, matrix of a linear operator $T : V \to V$ with respect to a base $\mathcal{B}$ for V, a polynomial of degree d with coefficients in a field $\mathbb{F}$, the evaluation $f(T)$ of a polynomial $f(x)$ at an operator T of a finite-dimensional vector space V, invariant subspace of an operator T on a vector space V, the T-cyclic subspace $\langle T, \boldsymbol{v}\rangle$ generated by a vector $\boldsymbol{v}$, the annihilator ideal of a vector with respect to an operator, the minimal polynomial of an operator with respect to a vector, the annihilator ideal of an operator T, the minimal polynomial of an operator T, eigenvalue and eigenvector of an operator T.

We begin with an important definition:

Definition 4.12 *A vector $\boldsymbol{z}$ such that $\mu_{T,\boldsymbol{z}}(x) = \mu_T(x)$ is called a* **maximal vector** *for T.*

The purpose of this section is to prove that maximal vectors always exist. In our first result we consider vectors $\boldsymbol{v}, \boldsymbol{w}$ such that $\mu_{T,\boldsymbol{v}}(x)$ and $\mu_{T,\boldsymbol{w}}(x)$ are relatively prime.

Lemma 4.2 *Let V be a finite-dimensional vector space, T an operator on V, and $\boldsymbol{v}, \boldsymbol{w}$ vectors in V. Assume gcd$(\mu_{T,\boldsymbol{v}}(x), \mu_{T,\boldsymbol{w}}(x)) = 1$. Then the following hold:*

i) $\langle T, \boldsymbol{v}\rangle \cap \langle T, \boldsymbol{w}\rangle = \{\boldsymbol{0}\}$;

ii) $\mu_{T,\boldsymbol{v}+\boldsymbol{w}}(x) = \mu_{T,\boldsymbol{v}}(x)\mu_{T,\boldsymbol{w}}(x)$.

iii) $\langle T, \boldsymbol{v}+\boldsymbol{w}\rangle = \langle T, \boldsymbol{v}\rangle \oplus \langle T, \boldsymbol{w}\rangle$.

Proof *i) For convenience, set $f(x) = \mu_{T,\boldsymbol{v}}(x)$ and $g(x) = \mu_{T,\boldsymbol{w}}(x)$. Since gcd$(f(x), g(x)) = 1$, there are polynomials $a(x)$ and $b(x)$ such that $a(x)f(x) + b(x)g(x) = 1$. Then $a(T)f(T) + b(T)g(T) = I_V$. Suppose now that $\boldsymbol{x} \in \langle T, \boldsymbol{v}\rangle \cap \langle T, \boldsymbol{w}\rangle$. Then $f(T)(\boldsymbol{x}) = g(T)(\boldsymbol{x}) = \boldsymbol{0}$. But we then have*

$$\begin{aligned} \boldsymbol{x} &= I_V(\boldsymbol{x}) \\ &= [a(T)f(T)+b(T)g(T)](\boldsymbol{x}) \\ &= a(T)(f(T)(\boldsymbol{x})+b(T)(g(T)(\boldsymbol{x}) \\ &= a(T)(\mathbf{0})+b(T)(\mathbf{0}) \\ &= \mathbf{0}. \end{aligned}$$

ii) Set $h(x)=\mu_{T,\boldsymbol{v}+\boldsymbol{w}}(x)$. We show that $h(x)|f(x)g(x)$ and $f(x)g(x)|h(x)$ and since both are monic we get equality.

First,

$$\begin{aligned} [f(T)g(T)](\boldsymbol{v}+\boldsymbol{w}) &= (f(T)g(T))(\boldsymbol{v})+(f(T)g(T))(\boldsymbol{w}) \\ &= g(T)(f(T)(\boldsymbol{v}))+f(T)(g(T)(\boldsymbol{w})) \\ &= g(T)(\mathbf{0})+f(T)(\mathbf{0})=\mathbf{0}. \end{aligned}$$

By Remark (4.1), it follows that $h(x)|f(x)g(x)$.

On the other hand, $\mathbf{0}=h(T)(\boldsymbol{v}+\boldsymbol{w})=h(T)(\boldsymbol{v})+h(T)(\boldsymbol{w})$ from which we conclude that $h(T)(\boldsymbol{v})=-h(T)(\boldsymbol{w})$. The former vector, $h(T)(\boldsymbol{v})$, is in $\langle T,\boldsymbol{v}\rangle$ and the latter, $-h(T)(\boldsymbol{w})$ is in $\langle T,\boldsymbol{w}\rangle$. By i) $\langle T,\boldsymbol{v}\rangle\cap\langle T,\boldsymbol{w}\rangle=\{\mathbf{0}\}$. Thus, $h(T)(\boldsymbol{v})=h(T)(\boldsymbol{w})=\mathbf{0}$. Again by Remark (4.1) it follows that $f(x)|h(x)$ and $g(x)|h(x)$. Then the lcm of $f(x)$ and $g(x)$ divides $h(x)$. However, since $f(x)$ and $g(x)$ are relatively prime and monic, the lcm of $f(x)$ and $g(x)$ is $f(x)g(x)$. Thus, $f(x)g(x)$ divides $h(x)$ as we claimed.

iii) Since $\langle T,\boldsymbol{v}\rangle$ and $\langle T,\boldsymbol{w}\rangle$ are T-invariant by Exercise 12 of Section (4.1), the sum $\langle T,\boldsymbol{v}\rangle+\langle T,\boldsymbol{w}\rangle$ is T-invariant and contains $\boldsymbol{v}+\boldsymbol{w}$. Therefore, by ii) of Theorem (4.2), $\langle T,\boldsymbol{v}+\boldsymbol{w}\rangle\subset\langle T,\boldsymbol{v}\rangle+\langle T,\boldsymbol{w}\rangle$.

By part i), $\langle T,\boldsymbol{v}\rangle\cap\langle T,\boldsymbol{w}\rangle=\{\mathbf{0}\}$. It follows from this that $dim(\langle T,\boldsymbol{v}\rangle+\langle T,\boldsymbol{w}\rangle)=dim(\langle T,\boldsymbol{v}\rangle)+dim(\langle T,\boldsymbol{w}\rangle)=deg(f(x))+deg(g(x))$, the latter equality by iii) of Theorem (4.2). On the other hand, by the same result, $dim(\langle T,\boldsymbol{v}+\boldsymbol{w}\rangle)=deg(\mu_{T,\boldsymbol{v}+\boldsymbol{w}}(x))=deg(f(x)g(x))$ by the second part above. It now follows that $\langle T,\boldsymbol{v}+\boldsymbol{w}\rangle=\langle T,\boldsymbol{v}\rangle+\langle T,\boldsymbol{w}\rangle=\langle T,\boldsymbol{v}\rangle\oplus\langle T,\boldsymbol{w}\rangle$.

Lemma 4.3 *Let V be an n-dimensional vector space with basis $\mathcal{B}=(\boldsymbol{v}_1,\boldsymbol{v}_2,\ldots,\ \boldsymbol{v}_n)$. Let T be an operator on V and set $f_i(x)=\mu_{T,\boldsymbol{v}_i}(x)$ and let $l(x)$ be the lcm of $f_1(x),f_2(x),\ldots,f_n(x)$. Then $l(x)$ is the minimal polynomial of T.*

Proof *Since $\mu_T(T)(\boldsymbol{v}) = \mathbf{0}$ for all vectors $\boldsymbol{v}$ it follows, in particular, that $\mu_T(T)(\boldsymbol{v}_i) = \mathbf{0}, i = 1, 2, \dots, n$. Then by Remark (4.1) we have that $f_i(x)|\mu_T(x)$ for all i and, consequently, $l(x)|\mu_T(x)$.*

On other hand, since $f_i(x)|l(x)$, $l(T)(\boldsymbol{v}_i) = \mathbf{0}$. Since $l(T)$ takes each vector of the basis to the zero vector, $l(T)$ is the zero operator. Then by Remark (4.4) we can say that $\mu_T(x)|l(x)$. Since $\mu_T(x)$ and $l(x)$ are both monic $\mu_T(x) = l(x)$.

We now come to our prime objective:

Theorem 4.6 *Let V be an n-dimensional vector space and T an operator on V. Then there exists a vector $\boldsymbol{z}$ such that $\mu_T(x) = \mu_{T,\boldsymbol{z}}(x)$.*

Proof *Let $\mathcal{B} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n)$ be a basis for V and set $f_i(x) = \mu_{T,\boldsymbol{v}_i}(x)$ and $l(x) = \mu_T(x)$. By Lemma (4.3), $l(x)$ is the lcm of $(f_1(x), f_2(x), \dots, f_n(x))$.*

Let the prime factorization of $l(x)$ be

$$p_1(x)^{e_1} p_2(x)^{e_2} \dots p_t(x)^{e_t},$$

where $p_i(x)$ is a monic irreducible polynomial and e_i is a natural number, $i = 1, 2, \dots, t$.

Since $l(x)$ is the lcm of $f_1(x), f_2(x), \dots, f_n(x)$, for each i, there exists an index j_i such that $p_i(x)^{e_i}$ divides $f_{j_i}(x)$. Write $f_{j_i}(x) = p_i(x)^{e_i} g_{j_i}(x)$ and set $\boldsymbol{w}_i = g_{j_i}(T)(\boldsymbol{v}_{j_i})$. Since $g_{j_i}(x)$ divides $f_{j_i}(x)$, the gcd of $g_{j_i}(x)$ and $f_{j_i}(x)$ is $g_{j_i}(x)$. By Theorem (4.4), the minimal polynomial of T with respect to $\boldsymbol{w}_i$ is the quotient of $f_{j_i}(x)$ by $g_{j_i}(x)$. However, $f_{j_i}(x) = p_i(x)^{e_i} g_{j_i}(x)$ and therefore $\mu_{T,\boldsymbol{w}_i}(x) = p_i(x)^{e_i}$.

Now set $\boldsymbol{z}_1 = \boldsymbol{w}_1$ and suppose that for $1 < k < t$ and that $\boldsymbol{z}_k$ has been defined. Set $\boldsymbol{z}_{k+1} = \boldsymbol{z}_k + \boldsymbol{w}_{k+1}$ and $\boldsymbol{z} = \boldsymbol{z}_t$. We claim that for each $k, 1 \leq k \leq t$ that $\mu_{T,\boldsymbol{z}_k}(x) = p_1(x)^{e_1} p_2(x)^{e_2} \dots p_k(x)^{e_k}$. If so, then the vector $\boldsymbol{z}$ will satisfy the conclusion of the theorem.

By part ii) Lemma (4.2), the minimal polynomial of T with respect to $\boldsymbol{z}_2 = \boldsymbol{w}_1 + \boldsymbol{w}_2$ is $p_1(x)^{e_1} p_2(x)^{e_2}$. Now assume that $1 < k < t$ and the minimal polynomial of T with respect to $\boldsymbol{z}_k$ is $p_1(x)^{e_1} p_2(x)^{e_2} \dots p_k(x)^{e_k}$. The minimal polynomial of T with respect to $\boldsymbol{w}_{k+1}$ is $p_{k+1}(x)^{e_{k+1}}$, which by Lemma (3.7) is relatively prime to $p_1(x)^{e_1}\ p_2(x)^{e_2}\ \dots p_k(x)^{e_k}$. By another application of part ii) of Lemma (4.2) the minimal polynomial of $\boldsymbol{z}_{k+1} = \boldsymbol{z}_k + \boldsymbol{w}_{k+1}$ is $p_1(x)^{e_1} p_2(x)^{e_2} \dots p_{k+1}(x)^{e_{k+1}}$. This completes the theorem.

As an immediate corollary we have:

Corollary 4.1 *Let V be an n-dimensional vector space and T an operator on V. Then the degree of $\mu_T(x)$ is at most n.*

Exercises.

1. Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ be the operator given by

$$T(\boldsymbol{v}) = \begin{pmatrix} -1 & 3 & -2 \\ -1 & 3 & -4 \\ -1 & 1 & -2 \end{pmatrix} \boldsymbol{v}.$$

a) For each of the standard basis vectors $\boldsymbol{e}_i$ find $\mu_{T,\boldsymbol{e}_i}(x)$.

b) Compute $\mu_T(x)$.

c) Find a maximal vector for T.

2. Let $T : \mathbb{F}_5^3 \to \mathbb{F}_5^3$ be the operator given by

$$T(\boldsymbol{v}) = \begin{pmatrix} 4 & 3 & 3 \\ 4 & 3 & 1 \\ 4 & 1 & 3 \end{pmatrix} \boldsymbol{v}.$$

Determine $\mu_T(x)$ and find a maximal vector for T.

3. Let $T : \mathbb{R}^4 \to \mathbb{R}^4$ be the operator given by

$$T(\boldsymbol{v}) = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 2 & 0 & 0 & -1 \\ -1 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \boldsymbol{v}.$$

Determine $\mu_T(x)$ and find a maximal vector for T.

4. Let V be a finite-dimensional vector space and T an operator on V. Assume $\boldsymbol{v}_1, \dots, \boldsymbol{v}_k$ are eigenvectors for V with distinct eigenvalues $\alpha_1, \dots, \alpha_k$. Prove the sequence $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_k)$ is linearly independent.

5. Assume $T \in \mathcal{L}(\mathbb{R}^4, \mathbb{R}^4)$ and $\mu_{T,\boldsymbol{v}_1}(x) = x^2 + 1, \mu_{T,\boldsymbol{v}_2}(x) = x + 1$ and $\mu_{T,\boldsymbol{v}_3}(x) = x - 2$. Prove that T is a cyclic operator and that $\boldsymbol{v}_1 + \boldsymbol{v}_2 + \boldsymbol{v}_3$ is a maximal vector.

6. Let $T \in \mathcal{L}(\mathbb{F}_3^4, \mathbb{F}_3^4)$ and $\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3, \boldsymbol{v}_4$ vectors from $\mathbb{F}_3^4$ such that $\mu_{T,\boldsymbol{v}_1}(x) = x^2 + 1, \boldsymbol{v}_2 = T(\boldsymbol{v}_1), \mu_{T,\boldsymbol{v}_3}(x) = x + 1$ and $\mu_{T,\boldsymbol{v}_4}(x) = x - 1$. Prove that a vector $c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + c_3\boldsymbol{v}_3 + c_4\boldsymbol{v}_4$ is maximal if and only if c_3 and c_4 are non-zero and at least one of c_1, c_2 is non-zero.

7. Let V be a finite-dimensional vector space and T an operator on V. Assume $\mu_T(x)$ is an irreducible polynomial. Prove that every non-zero vector in V is a maximal vector.

8. Assume $T \in \mathcal{L}(\mathbb{F}_5^5, \mathbb{F}_5^5)$ and $\mu_T(x) = x^5 - x$. Prove that T has exactly 4^5 maximal vectors.

4.4 Indecomposable Linear Operators

In this section we continue with our investigation into the structure of a linear operator T on a finite-dimensional vector space V. In particular, we determine when it is **not** possible to express V as the direct sum of two T-invariant subspaces. This leads to the definition of a T-indecomposable subspace of V.

What You Need to Know

The following concepts are fundamental to understanding the new material in this section: vector space over a field $\mathbb{F}$, basis of a vector space, dimension of a vector space, linear operator on a vector space V, matrix of a linear operator $T : V \to V$ with respect to a basis $\mathcal{B}$ for V, a polynomial of degree d with coefficients in a field $\mathbb{F}$, the evaluation $f(T)$ of a polynomial f at an operator T of a finite-dimensional vector space V, invariant subspace of an operator T on a vector space V, the T-cyclic subspace $\langle T, \boldsymbol{v}\rangle$ generated by a vector $\boldsymbol{v}$, the annihilator ideal of a vector with respect to an operator, the minimal polynomial of an operator with respect to a vector, the annihilator of an operator T, the minimal polynomial of an operator T, eigenvalue and eigenvector of an operator T, and the maximal vector for an operator on a finite-dimensional vector space.

We begin with some fundamental definitions:

Definition 4.13 *Let V be a finite-dimensional vector space, T an operator on V, and U a T-invariant subspace. By a* **T-complement** *to U in V we shall mean a T-invariant subspace W such that $V = U \oplus W$.*

Definition 4.14 *Let V be a finite-dimensional vector space and T an operator on V. T is said to be an* **indecomposable operator** *if no non-trivial T-invariant subspace has a T-invariant complement. In the contrary situation, where there exists non-trivial T-invariant subspaces U and W such that $V = U \oplus W$, we say T is* **decomposable***.*

Example 4.3 *Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ be given by*

$$T(\boldsymbol{v}) = \begin{pmatrix} 3 & 1 & 1 \\ 1 & 3 & 1 \\ 1 & 1 & 3 \end{pmatrix} \boldsymbol{v}.$$

The subspace $U = Span\left(\begin{pmatrix}1\\0\\-1\end{pmatrix}, \begin{pmatrix}0\\1\\-1\end{pmatrix}\right)$ *is* T*-invariant. The subspace* $W = Span\left(\begin{pmatrix}1\\1\\1\end{pmatrix}\right)$ *is a* T*-invariant complement to* U*.*

Example 4.4 *Let* $T : \mathbb{R}^2 \to \mathbb{R}^2$ *be the operator given by*

$$T(\boldsymbol{v}) = \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}\boldsymbol{v}.$$

The operator T *is an indecomposable operator.*

Definition 4.15 *Let* V *be a non-zero finite-dimensional vector space and* T *an operator on* V*.* T *is said to be an* **irreducible operator** *if the only* T*-invariant subspaces are* V *and* $\{\mathbf{0}\}$*.*

Example 4.5 *Let* $T : \mathbb{R}^2 \to \mathbb{R}^2$ *be the operator given by*

$$T(\boldsymbol{v}) = \begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix}\boldsymbol{v}.$$

The operator T *is an irreducible operator.*

Our main goal is to prove that an operator T is indecomposable if and only if T is cyclic and $\mu_T(x) = p(x)^m$, where $p(x)$ is an irreducible polynomial. We begin by characterizing irreducible operators.

Theorem 4.7 *Let* V *be an* n*-dimensional vector space and* T *an operator on* V*. Then* T *is irreducible if and only if* T *is cyclic and* $\mu_T(x)$ *is an irreducible polynomial.*

Proof *Assume* T *is irreducible. Let* $\boldsymbol{v} \in V, \boldsymbol{v} \neq \mathbf{0}$*. Then* $\langle T, \boldsymbol{v}\rangle$ *is a* T*-invariant subspace and since it contains* $\boldsymbol{v} \neq \mathbf{0}$ *we must have* $\langle T, \boldsymbol{v}\rangle = V$*. This proves that* T *is cyclic. Suppose* $\mu_T(x) = f(x)g(x)$*, where* $1 \leq deg(f(x)) < n$*. Set* $\boldsymbol{w} = f(T)(\boldsymbol{v})$*. Then by Theorem (4.4)* $\mu_{T,\boldsymbol{w}}(x) = g(x)$ *and* $\langle T, \boldsymbol{w}\rangle$ *is a non-trivial* T*-invariant subspace, contrary to assumption. Thus,* $\mu_T(x)$ *has no non-trivial factorizations and is irreducible.*

On the other hand, assume that $V = \langle T, \boldsymbol{v}\rangle$ *and* $\mu_T(x) = p(x)$ *is irreducible. Suppose* $\boldsymbol{w} \in V, \boldsymbol{w} \neq \mathbf{0}$*. Then there exists a polynomial* $h(x), deg(h(x)) < n$ *such that* $\boldsymbol{w} = h(T)(\boldsymbol{v})$*. By Theorem (4.4),* $\mu_{T,\boldsymbol{w}}(x) = \frac{p(x)}{gcd(h(x),p(x))}$*. Since* $deg(h(x)) < n = deg(p(x))$*, it follows that* $p(x)$ *does not divide* $h(x)$*. Since*

$p(x)$ is irreducible we can conclude that $h(x)$ and $p(x)$ are relatively prime. Therefore, $\mu_{T,\boldsymbol{w}}(x) = p(x)$. It then follows that $dim(\langle T, \boldsymbol{w}\rangle) = n = dim(V)$. Consequently, V contains no non-trivial T-invariant subspace and T is irreducible as claimed.

As an immediate corollary, we have:

Corollary 4.2 *Let V be a vector space, T an operator on V, and $\boldsymbol{v}$ a vector in V such that $\mu_{T,\boldsymbol{v}}(x) = p(x)$ is irreducible. Let W be a T-invariant subspace of V. Then either $\langle T, \boldsymbol{v}\rangle \subset W$ or $\langle T, \boldsymbol{v}\rangle \cap W = \{\mathbf{0}\}$.*

In our next result we prove the easy part of our main theorem:

Theorem 4.8 *Let V be a finite-dimensional vector space and T an operator on V. Assume T is cyclic and $\mu_T(x) = p(x)^m$, where $p(x)$ is an irreducible polynomial and m is a natural number. Then T is indecomposable.*

Proof *If $m = 1$, then T is irreducible, whence indecomposable. We may therefore assume that $m > 1$. Let $\boldsymbol{v}$ be a vector such that $V = \langle T, \boldsymbol{v}\rangle$. Set $\boldsymbol{u} = p(T)^{m-1}(\boldsymbol{v})$. Then by Theorem (4.4), $\mu_{T,\boldsymbol{u}}(x) = p(x)$ and $U = \langle T, \boldsymbol{u}\rangle$ is irreducible by Theorem (4.7). Now suppose W is a non-trivial T-invariant subspace of V. Then by Theorem (4.5) there is a vector $\boldsymbol{w} \in W$ such that $W = \langle T, \boldsymbol{w}\rangle$ and $\mu_{T,\boldsymbol{w}}(x)$ divides $\mu_{T,\boldsymbol{v}}(x) = p(x)^m$. Suppose $\mu_{T,\boldsymbol{w}}(x) = p(x)^k$. Set $\boldsymbol{y} = p(T)^{k-1}(\boldsymbol{w})$. Then $\mu_{T,\boldsymbol{y}}(x) = p(x)$. By Theorem (4.5), it follows that $\langle T, \boldsymbol{y}\rangle = \langle T, \boldsymbol{u}\rangle$ and therefore $U \subset W$. As a consequence of this, if W_1, W_2 are non-zero T-invariant subspaces of V then $U \subset W_1 \cap W_2$ and, in particular, $W_1 \cap W_2 \neq \{\mathbf{0}\}$. Therefore no non-trivial T-invariant subspace can have a T-invariant complement.*

The rest of this section will be devoted to proving the converse of Theorem (4.8): If T is an indecomposable operator on a finite-dimensional vector space V, then T is cyclic and $\mu_T(x) = p(x)^m$ where $p(x)$ is an irreducible polynomial. We first show if the minimal polynomial of T has two or more distinct irreducible factors then T is decomposable.

Lemma 4.4 *Assume $\mu_T(x) = f(x)g(x)$, where $f(x)$ and $g(x)$ are relatively prime. Then $Ker(f(T)) = Range(g(T))$ and $Ker(g(T)) = Range(f(T))$. Moreover, $V = Ker(f(T)) \oplus Ker(g(T))$.*

Proof *For convenience, we set* $K_f = Ker(f(T))$ *and* $K_g = Ker(g(T))$. *Also, set* $R_f = Range(f(T)), R_g = Range(g(T))$. *We claim that* $R_f \subset K_g$ *and* $R_g \subset K_f$. *To see this, suppose that* $\boldsymbol{u} \in R_f$ *so that there is a vector* $\boldsymbol{x}$ *with* $\boldsymbol{u} = f(T)(\boldsymbol{x})$. *Then* $g(T)(\boldsymbol{u}) = g(T)(f(T)(\boldsymbol{v})) = (g(T)f(T))(\boldsymbol{v}) = \mathbf{0}$. *Thus,* $\boldsymbol{u} \in K_g$. *Since* $\boldsymbol{u}$ *was arbitrary in* R_f, *it follows that* $R_f \subset K_g$. *In exactly the same way,* $R_g \subset K_f$.

We next show that $K_f \cap K_g = \{\mathbf{0}\}$. *Suppose* $\boldsymbol{u} \in K_f \cap K_g$. *Since* $f(x), g(x)$ *are relatively prime there are polynomials* $a(x), b(x)$ *such that* $a(x)f(x) + b(x)g(x) = 1$. *Then* $a(T)f(T) + b(T)g(T) = I_V$. *Then*

$$\boldsymbol{u} = I_V(\boldsymbol{u}) = [a(T)f(T) + b(T)g(T)](\boldsymbol{u}) = a(T)[f(T)(\boldsymbol{u})] + b(T)[g(T)(\boldsymbol{u})].$$

However, since $\boldsymbol{u} \in K_f \cap K_g, f(T)(\boldsymbol{u}) = g(T)(\boldsymbol{u}) = \mathbf{0}$. *We then have*

$$\boldsymbol{u} = a(T)[f(T)(\boldsymbol{u})] + b(T)[g(T)(\boldsymbol{u})] = \mathbf{0}$$

as claimed.

Since $R_f \subseteq K_g$ *it follows that* $K_f \cap R_f = \{\mathbf{0}\}$ *so that* $K_f + R_f = K_f \oplus R_f$. *By Theorem (2.9)* $dim(K_f) + dim(R_f) = dim(V)$ *and therefore* $K_f \oplus R_f = V$. *Since* $R_f \subseteq K_g$ *we also have* $K_f + K_g = K_f \oplus K_g = V$. *Thus,* $dim(R_f) = dim(V) - dim(K_f) = dim(K_g)$. *Since* $R_f \subset K_g$ *it then follows that* $R_f = K_g$. *Similarly,* $R_g = K_f$.

It now follows that if T is indecomposable on V then $\mu_T(x) = p(x)^m$ for some irreducible polynomial. It remains to show that T is cyclic.

Lemma 4.5 *Let* V *be a finite-dimensional vector space and* T *an operator on* V *with minimal polynomial* $p(x)^m$ *where* $p(x)$ *is irreducible of degree* d. *Then* $dim(V)$ *is a multiple of* d.

Proof *The proof is by the second principle of mathematical induction on* $dim(V)$. *Let* $\boldsymbol{u}$ *be a vector with* $\mu_{T,\boldsymbol{u}}(x) = p(x)$. *If* $V = \langle T, \boldsymbol{u}\rangle$ *then* $dim(V) = d$. *Otherwise, set* $U = \langle T, \boldsymbol{u}\rangle$, $\overline{V} = V/U$, *and let* $\overline{T} : \overline{V} \to \overline{V}$ *be given by* $\overline{T}(U + \boldsymbol{w}) = U + T(\boldsymbol{w})$. *The minimal polynomial of* $\overline{T}$, $\mu_{\overline{T}}(x)$, *divides* $p(x)^m$ *and so the inductive hypothesis applies. Therefore* $dim(\overline{V})$ *is a multiple of* d. *Since* $dim(V) = dim(U) + dim(\overline{V})$ *and* $dim(U) = d$, *it follows that* $dim(V)$ *is a multiple of* d.

The following lemma is fundamental to our goal. Basically, it says that if the subspace of V consisting of all vectors of order $p(x)$ is cyclic, then V is cyclic.

Lemma 4.6 *Let V be a finite-dimensional vector space and T an operator on V. Assume the minimal polynomial of T is $p(x)^m$ where $p(x)$ is irreducible of degree d. Set $W = \{\boldsymbol{w} \in V | p(T)(\boldsymbol{w}) = \mathbf{0}\}$ and let $\boldsymbol{z}$ be a maximal vector for T. If $W \subset \langle T, \boldsymbol{z}\rangle$, then $V = \langle T, \boldsymbol{z}\rangle$.*

Proof *Set $Z = \langle T, \boldsymbol{z}\rangle$. We prove the contrapositive statement: If $V \neq Z$ then there exists $\boldsymbol{w} \in W \setminus Z$. First note that that for every vector $\boldsymbol{v} \in V, \mu_{T,\boldsymbol{v}}(x) = p(x)^k$ for some $k, 0 \leq k \leq m$. Let J consist of those natural numbers j such that there exists $\boldsymbol{v} \in V \setminus Z$ with $\mu_{T,\boldsymbol{v}}(x) = p(x)^j$. Let k be the least element in J and choose $\boldsymbol{v} \notin Z$ such that $\mu_{T,\boldsymbol{v}}(x) = p(x)^k$. Set $\boldsymbol{y} = p(T)(\boldsymbol{v})$. Then $\mu_{T,\boldsymbol{y}}(x) = p(x)^{k-1}$ and therefore by the minimality of k it must be the case that $\boldsymbol{y} \in Z$. We claim that $\langle T, \boldsymbol{y}\rangle \neq Z$. Assume to the contrary that $\langle T, \boldsymbol{y}\rangle = Z$. Then $\mu_{T,\boldsymbol{y}}(x) = \mu_T(x) = p(x)^m$ so that $\mu_{T,\boldsymbol{v}}(x) = p(x)^{m+1}$ which is not possible. Suppose now that $\boldsymbol{y} = f(T)(\boldsymbol{z})$. Then $\mu_{T,\boldsymbol{y}}(x) = \frac{\mu_{p(x)^m}}{gcd(f(x),\mu_{T,\boldsymbol{z}}(x))} = p(x)^{k-1}$. It follows that $p(x)$ divides $f(x)$. Let $g(x)$ be the polynomial such that $f(x) = p(x)g(x)$ and set $\boldsymbol{u} = g(T)(\boldsymbol{z})$. Then $p(T)(\boldsymbol{u}) = \boldsymbol{y}$. Now set $\boldsymbol{w} = \boldsymbol{v} - \boldsymbol{u}$. Then $\boldsymbol{w} \notin Z$ since $\boldsymbol{v} \notin Z$ and $\boldsymbol{u} \in Z$. Also, $p(T)(\boldsymbol{w}) = p(T)(\boldsymbol{v} - \boldsymbol{u}) = p(T)(\boldsymbol{v}) - p(T)(\boldsymbol{u}) = \boldsymbol{y} - \boldsymbol{y} = \mathbf{0}$.*

Theorem 4.9 *Let V be a finite-dimensional vector space and T be an operator on V such that the minimal polynomial of T is $p(x)^m$, where $p(x)$ is irreducible of degree d. Let $\boldsymbol{z}$ be a maximal vector in V for T. Then $\langle T, \boldsymbol{z}\rangle$ has a T-invariant complement X in V.*

Proof *By Lemma (4.5), $dim(V) = dk$ for some natural number k. The proof is by induction on k. If $k = 1$ then $V = \langle T, \boldsymbol{u}\rangle$ for any $\boldsymbol{u} \neq \mathbf{0}$ and we can take $X = \{\mathbf{0}\}$.*

Suppose the result has been established for spaces V with $dim(V) = dk$. We need to prove that it is true for a space of dimension $d(k+1)$. If $V = \langle T, \boldsymbol{z}\rangle$, then we can take $X = \{\mathbf{0}\}$ so we may assume that $V \neq \langle T, \boldsymbol{z}\rangle$, that is, T is not cyclic. Then by Lemma (4.6) there is a vector $\boldsymbol{w} \in V \setminus \langle T, \boldsymbol{z}\rangle$ such that $p(T)(\boldsymbol{w}) = \mathbf{0}$. Set $W = \langle T, \boldsymbol{w}\rangle$ and $\overline{V} = V/W$. The dimension of $\overline{V}$ is $d(k+1) - d = dk$. Let $\overline{T} : \overline{V} \to \overline{V}$ be the induced operator given by $\overline{T}(W + \boldsymbol{y}) = W + T(\boldsymbol{y})$. The minimal polynomial of the vector $W + \boldsymbol{z}$ in $\overline{V}$ with respect to $\overline{T}$ is $p(x)^m$. Consequently, our inductive hypothesis holds: there exists a $\overline{T}$-invariant subspace $\overline{X}$, which is a complement to $\langle \overline{T}, W + \boldsymbol{z}\rangle$ in $\overline{V}$. Let X be the unique subspace of V such that $W \subset X$ and $X/W = \overline{X}$. Then X is T-invariant, and we claim that X is a complement to $\langle T, \boldsymbol{z}\rangle$ in V.

Since $\{W\} = \{\mathbf{0}_{\overline{V}}\} = \langle \overline{T}, W + \boldsymbol{z}\rangle \cap \overline{X} = [(W + \langle T, \boldsymbol{z}\rangle)/W] \cap [X/W]$ it follows that $\langle T, \boldsymbol{z}\rangle \cap X$ is contained in W. However, $W \cap \langle T, \boldsymbol{z}\rangle = \{\mathbf{0}\}$ and therefore $\langle T, \boldsymbol{z}\rangle \cap X = \{\mathbf{0}\}$.

On the other hand, suppose $\boldsymbol{v} \in V$ is arbitrary. Then $W + \boldsymbol{v}$ is a vector in $\overline{V}$ and we can find $\boldsymbol{z}' \in \langle T, \boldsymbol{z}\rangle$ and $\boldsymbol{x} \in X$ such that $W + \boldsymbol{v} = (W + \boldsymbol{z}') + (W + \boldsymbol{x})$. This implies that $\boldsymbol{v} - (\boldsymbol{z}' + \boldsymbol{x}) \in W \subset X$. Consequently, $\boldsymbol{v} \in \langle T, \boldsymbol{z}\rangle + X$. This completes the proof.

The second part of our main theorem is now a corollary of this:

Theorem 4.10 *Let V be a finite-dimensional vector space and T an indecomposable operator on V. Then T is a cyclic operator and the minimal polynomial of T is $p(x)^m$, where $p(x)$ is an irreducible polynomial.*

Proof *We already observed, subsequent to Lemma (4.4), that if T is indecomposable then $\mu_T(x) = p(x)^m$, where $p(x)$ is irreducible. Suppose T is not cyclic. Let $\boldsymbol{z}$ be a maximal vector. Since $\langle T, \boldsymbol{z}\rangle \neq V$, by Theorem (4.9), $\langle T, \boldsymbol{z}\rangle$ has a T-invariant complement. It then follows that T is decomposable.*

Exercises

1. Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ be the operator given by

$$T(\boldsymbol{v}) = \begin{pmatrix} -3 & 1 & 2 \\ -4 & 1 & 4 \\ 0 & 0 & -1 \end{pmatrix} \boldsymbol{v}.$$

Determine whether T is decomposable or indecomposable.

2. Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ be the operator given by

$$T(\boldsymbol{v}) = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix} \boldsymbol{v}.$$

Determine whether T is decomposable or indecomposable.

3. Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ be the operator given by

$$T(\boldsymbol{v}) = \begin{pmatrix} 0 & 0 & 8 \\ 1 & 0 & -12 \\ 0 & 1 & 6 \end{pmatrix} \boldsymbol{v}.$$

Determine whether T is decomposable or indecomposable.

4. Assume S is a cyclic operator on the finite-dimensional vector space U and that $\mu_S(x) = p(x)$ is irreducible. Prove that every non-zero element of the algebra $\mathcal{P}(S)$ is invertible and its inverse lies in $\mathcal{P}(S)$. (See Exercise 10 of Section (4.1).)

5. Let V be a finite-dimensional vector space with basis $\mathcal{B} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$. Let T be an operator on V and assume that the minimal polynomial of T is $p(x)^m$, where $p(x)$ is an irreducible polynomial. Prove that some vector $\boldsymbol{v}_i$ is maximal.

6. Let V be a finite-dimensional vector space with basis $\mathcal{B} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$. Assume $T \in \mathcal{L}(V, V)$ is indecomposable. Prove that $V = \langle T, \boldsymbol{v}_i \rangle$ for some $i, 1 \leq i \leq n$.

7. Assume $T : \mathbb{R}^{2n+1} \to \mathbb{R}^{2n+1}$ is an indecomposable operator. Prove that there is a real number a such that $\mu_T(x) = (x - a)^{2n+1}$.

8. Let $T : \mathbb{R}^{2n} \to \mathbb{R}^{2n}$ be an indecomposable operator. Prove that the number of T-invariant subspaces of V is either $2n + 1$ or $n + 1$.

9. Let p be a prime and $T : \mathbb{F}_p^4 \to \mathbb{F}_p^4$ be an indecomposable but not irreducible operator. Prove that the number of maximal vectors is either $p^4 - p^3$ or $p^4 - p^2$.

10. Let T be an operator on a finite-dimensional vector space. Prove that T is indecomposable if and only if there is a unique maximal proper T-invariant subspace of V.

4.5 Invariant Factors and Elementary Divisors

In this section, we consider an operator T on a finite-dimensional vector space V and investigate how V can be decomposed as a direct sum of T-invariant subspaces. One such way is as indecomposable, hence, cyclic, subspaces. Such a decomposition leads to the concept of elementary divisors of T. An alternative method leads to the definition of the invariant factors of T.

What You Need to Know

The following concepts are fundamental to understanding the new material in this section: vector space over a field $\mathbb{F}$, basis of a vector space, dimension of a vector space, linear operator on a vector space V, matrix of a linear operator $T : V \to V$ with respect to a basis $\mathcal{B}$ for V, a polynomial of degree d with coefficients in a field $\mathbb{F}$, the evaluation $f(T)$ of a polynomial f at an operator T of a finite-dimensional vector space V, invariant subspace of an operator T on a vector space V, the T-cyclic subspace $\langle T, \boldsymbol{v} \rangle$ generated by a vector $\boldsymbol{v}$, the annihilator ideal of a vector with respect to an operator, the minimal polynomial of an operator with respect to a vector, the annihilator ideal of an operator T, the minimal polynomial of an operator T, eigenvalue and eigenvector of an operator T, maximal vector for an operator on a finite-dimensional vector space, T-invariant complement to a T-invariant subspace,and an indecomposable linear operator.

We begin with the following result which makes use of Theorem (4.9):

Theorem 4.11 *Let $T \in \mathcal{L}(V, V)$ have minimal polynomial a power of $p(x)$ where $p(x)$ is irreducible of degree d. Then there are vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_r \in V$ such that*

$$V = \langle T, \boldsymbol{v}_1 \rangle \oplus \cdots \oplus \langle T, \boldsymbol{v}_r \rangle$$

with $\mu_{T,\boldsymbol{v}_i}(x) = p(x)^{m_i}$ with $m_1 \geq m_2 \cdots \geq m_r$.

Proof *Let $dim(V) = dk$. The proof is by the second principle of mathematical induction on k. Assume $\mu_T(x) = p(x)^m$ and let $\boldsymbol{v} \in V$ with $\mu_{T,\boldsymbol{v}}(x) = p(x)^m$, that is, $\boldsymbol{v}$ is a maximal vector. If $V = \langle T, \boldsymbol{v} \rangle$, then we are done with $r = 1$. Suppose $V \neq \langle T, \boldsymbol{v} \rangle$. By Theorem (4.9), there is a T-invariant complement X to $\langle T, \boldsymbol{v} \rangle$ in V. The dimension of X is $dk - dm = d(k - m) < dk$. Set $\overline{T} = T_{|X}$. We can apply the inductive hypothesis to $(\overline{T}, X)$ and find vectors $\boldsymbol{v}_2, \ldots, \boldsymbol{v}_r$ such that $X = \langle \overline{T}, \boldsymbol{v}_2 \rangle \oplus \cdots \oplus \langle \overline{T}, \boldsymbol{v}_r \rangle$ with $\mu_{T,\boldsymbol{v}_i}(x) = p(x)^{m_i}$ with $m_2 \geq m_3 \geq \cdots \geq m_r$. Note that $\langle \overline{T}, \boldsymbol{v}_i \rangle = \langle T, \boldsymbol{v}_i \rangle$ for $2 \leq i \leq r$. Set $\boldsymbol{v}_1 = \boldsymbol{v}$. Then $\mu_{T,\boldsymbol{v}}(x) = p(x)^m$. Since $m \geq m_2$ we have satisfied the conclusions of the result.*

The next result shows that while there may be many choices for the sequence of vectors $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r)$ the natural numbers r and $m_1, \ldots, m_r$ are unique.

Theorem 4.12 *Let V be a finite-dimensional vector space and T an operator on V such that $\mu_T(x) = p(x)^l$ where $p(x)$ is an irreducible polynomial of degree d. Assume that $V = \langle T, \boldsymbol{v}_1\rangle \oplus \cdots \oplus \langle T, \boldsymbol{v}_r\rangle$ with $\mu_{T,\boldsymbol{v}_i}(x) = p(x)^{m_i}$ and $m_1 \geq m_2 \geq \cdots \geq m_r$ and also that $V = \langle T, \boldsymbol{u}_1\rangle \oplus \cdots \oplus \langle T, \boldsymbol{u}_s\rangle$ with $\mu_{T,\boldsymbol{u}_j}(x) = p(x)^{n_j}$ with $n_1 \geq n_2 \geq \cdots \geq n_s$. Then $r = s$ and for each $i, m_i = n_i$.*

Proof *We know that $dim(V)$ is a multiple of d by Lemma (4.5). Let $dim(V) = dM$. The proof is by the second principle of mathematical induction on M. If $M = 1$, then clearly $r = s = m_1 = n_1 = 1$ and there is nothing to prove. So assume the result is true for any operator S acting on a space U, where $\mu_S(x)$ is a power of an irreducible polynomial $p(x)$ of degree d, and the dimension of U is dM' with $M' < M$.*

Let $W = Ker(p(T))$ and set $\boldsymbol{v}_i' = p(T)^{m_i-1}(\boldsymbol{v}_i), \boldsymbol{u}_j' = p(T)^{n_j-1}(\boldsymbol{u}_j)$. Then

$$W = \langle T, \boldsymbol{v}_1'\rangle \oplus \cdots \oplus \langle T, \boldsymbol{v}_r'\rangle = \langle T, \boldsymbol{u}_1'\rangle \oplus \cdots \oplus \langle T, \boldsymbol{u}_s'\rangle.$$

It follows that $dr = dim(W) = ds$, and, therefore, $r = s$.

Set $\overline{V} = V/W$ and let $\overline{T} : \overline{V} \to \overline{V}$ be defined by

$$\overline{T}(W + \boldsymbol{y}) = W + T(\boldsymbol{y}).$$

Let r' be the largest natural number such that $m_{r'} > 1$, and similarly define s' to be the largest natural number such that $n_{s'} > 1$. Set $\boldsymbol{v}_i' = W + \boldsymbol{v}_i$ for $1 \leq i \leq r'$ and $\boldsymbol{u}_j' = W + \boldsymbol{u}_j$ for $1 \leq j \leq s'$. Then

$$\begin{aligned} \overline{V} &= \langle \overline{T}, \boldsymbol{v}_1'\rangle \oplus \cdots \oplus \langle \overline{T}, \boldsymbol{v}_{r'}'\rangle \\ &= \langle \overline{T}, \boldsymbol{u}_1'\rangle \oplus \cdots \oplus \langle \overline{T}, \boldsymbol{u}_{s'}'\rangle. \end{aligned}$$

Moreover, $\mu_{\overline{T},\boldsymbol{v}_i'}(x) = p(x)^{m_i-1}$ and $\mu_{\overline{T},\boldsymbol{u}_j'}(x) = p(x)^{n_j-1}$.

By the inductive hypothesis, $r' = s'$ and for all $i, 1 \leq i \leq r' = s', m_i - 1 = n_i - 1$, from which we conclude that $m_i = n_i$. On the other hand, the number of $m_i = 1$ is $r - r'$ and the number of $n_j = 1$ is $s - s' = r - r'$ and this completes the theorem.

We now turn to the more general case.

Theorem 4.13 *Let V be a finite-dimensional vector space, T an operator on V, and assume the minimal polynomial of T is $\mu_T(x) = p_1(x)^{e_1} \dots p_t(x)^{e_t}$, where the polynomials $p_i(x)$ are irreducible and distinct.*

For each i, let

$$V_i = V(p_i) = \{\boldsymbol{v} \in V | p_i(T)^{e_i}(\boldsymbol{v}) = \boldsymbol{0}\} = Ker(p_i(T)^{e_i}).$$

Then each of the spaces V_i is T-invariant and

$$V = V_1 \oplus V_2 \oplus \dots \oplus V_t.$$

Proof *That each V_i is T-invariant follows from Exercise 22 of Section (4.1). We first prove that $V_1 + \dots + V_t = V_1 \oplus \dots \oplus V_t$. Thus, let $I = \{i_1, i_2, \dots, i_k\}$ be a subset of $\{1, 2, \dots, t\}$. Then the minimal polynomial of T restricted to $V_I = V_{i_1} + \dots + V_{i_k}$ is $p_{i_1}(x)^{e_{i_1}} \dots p_{i_k}(x)^{e_{i_k}}$. It then follows that if I, J are disjoint subsets of $\{1, 2, \dots, t\}$ then $V_I \cap V_J = \{\boldsymbol{0}\}$. In particular, for $I = \{i\}$ and $J = \{1, 2, \dots, t\} \setminus \{i\}$ this holds. This implies that $V_1 + \dots + V_t = V_1 \oplus \dots \oplus V_t$.*

To complete the proof we need to prove that $V = V_1 + V_2 + \dots + V_t$. We prove this by induction on $t \geq 2$.

The initial case follows from Lemma (4.4) so we have to prove the inductive step. Suppose the result is true for some $t \geq 2$. We prove that it is true for $t+1$. Assume that the minimal polynomial of the linear operator T on the space V is $p_1(x)^{e_1} \dots p_t(x)^{e_t} p_{t+1}(x)^{e_{t+1}}$, where the polynomials $p_1(x), \dots, p_t(x), p_{t+1}(x)$ are distinct (monic) irreducible polynomials.

As previously seen, $f(x) = p_1(x)^{e_1}$ and $g(x) = p_2(x)^{e_2} \dots p_t(x)^{e_t} p_{t+1}^{e_{t+1}}$ are relatively prime. By Lemma (4.4), $Ker(f(T))$ and $Ker(g(T))$ are T-invariant and

$$V = Ker(f(T)) \oplus Ker(g(T)).$$

Set $W = Ker(g(T))$ and $T' = T_{|W}$. The minimal polynomial of T' is $g(x) = p_2(x)^{e_2} \dots p_t(x)^{e_t} p_{t+1}^{e_{t+1}}(x)$. By the inductive hypothesis

$$W = Ker(p_2(T')^{e_2}) \oplus \dots \oplus Ker(p_t(T')^{e_t}))Ker(p_{t+1}(T')).$$

Since $T' = T_{|W}$, it follows that $Ker(p_i(T')^{e_i}) = Ker(p_i(T)^{e_i})$. Since $V = Ker(p_1(T)^{e_1}) \oplus W$, it now follows that

$$V = Ker(p_1(T)^{e_1}) \oplus Ker(p_2(T)^{e_2}) \oplus \dots \oplus Ker(p_{t+1}(T)^{e_{t+1}}).$$

Definition 4.16 *Let V be a finite-dimensional vector space and T an operator on V with minimal polynomial $\mu_T(x) = p_1(x)^{e_1} \dots p_t(x)^{e_t,}$ where $p_i(x)$ are distinct irreducible polynomials. The T-invariant subspace $Ker(p_i(T)^{e_i})$ is called the* **Sylow-$p_i(x)$ subspace of the operator** T.

Definition 4.17 *Let V be a vector space, T a linear operator on V, and assume that the minimal polynomial of T is $p_1(x)^{e_1} \dots p_t(x)^{e_t}$, where $p_i(x)$ are distinct irreducible polynomials. Set $V_i = Ker(p_i(T)^{e_i})$. Suppose*

$$V_i = \langle T, \boldsymbol{v}_{i1}\rangle \oplus \dots \oplus \langle T, \boldsymbol{v}_{i,s_i}\rangle,$$

where $\mu_{T,\boldsymbol{v}_{ij}}(x) = p_i(x)^{f_{ij}}, f_{i1} \geq f_{i2} \geq \dots \geq f_{i,s_i}$. Then the polynomials $p_i(x)^{f_{ij}}$ are the **elementary divisors of** T.

We next show that under the hypotheses of Theorem (4.13), if W is a T-invariant subspace of V then the Sylow-$p_i(x)$ subspace of W is $W \cap V_i$ and, consequently, $W = (W \cap V_1) \oplus \dots \oplus (W \cap V_t)$.

Theorem 4.14 *Let V be a finite-dimensional vector space, T an operator on V, and assume $\mu_T(x) = p_1(x)^{e_1} \dots p_t(x)^{e_t}$ where the $p_i(x)$ are distinct, monic, irreducible polynomials. Set $V_i = Ker(p_i(T)^{e_i})$ and assume that W is a T-invariant subspace of V. Then*

$$W = (W \cap V_1) \oplus (W \cap V_2) \oplus \dots \oplus (W \cap V_t).$$

Proof *Since $(W \cap V_i) \cap (W \cap V_j) \subset V_i \cap V_j = \{\mathbf{0}\}$ for $i \neq j$ we need to show that $W = (W \cap V_1) + (W \cap V_2) + \dots + (W \cap V_t)$.*

Let $\boldsymbol{w} \in W$ and write $\boldsymbol{w} = \boldsymbol{w}_1 + \dots + \boldsymbol{w}_t$ with $\boldsymbol{w}_i \in V_i$. Suppose $\boldsymbol{w}_i \neq \mathbf{0}$. Then we need to show that $\boldsymbol{w}_i \in W$. Set $\mu_{T,\boldsymbol{w}}(x) = p_1(x)^{f_1} \dots p_t(x)^{f_t} = g(x)$. If $\boldsymbol{w}_i \neq \mathbf{0}$, then $f_i > 0$. Let $g(x) = p_i(x)^{f_i}h(x)$. Then $h(x)$ and $p_i(x)^{f_i}$ are relatively prime. Consequently, there are polynomials $a(x), b(x)$ such that $a(x)p_i(x)^{f_i} + b(x)h(x) = 1$. Then $a(T)p_i(T)^{f_i} + b(T)h(T) = I_V$. From this it follows that

$$\boldsymbol{w}_i = b(T)h(T)(\boldsymbol{w}) \in \langle T, \boldsymbol{w}\rangle.$$

On the other hand, since W is T-invariant and $\boldsymbol{w} \in W, \langle T, \boldsymbol{w}\rangle \subset W$ by Theorem (4.2).

Theorem 4.15 *Let V be a finite-dimensional vector space and T a linear operator on V with minimal polynomial $\mu_T(x)$. Let $\boldsymbol{v}$ be a vector such that $\mu_{T,\boldsymbol{v}}(x) = \mu_T(x)$. Then $\langle T, \boldsymbol{v}\rangle$ has a T-invariant complement in V.*

Proof *Let the prime factorization of $\mu_T(x)$ be $p_1(x)^{e_1} \dots p_t(x)^{e_t}$. Set $V_i = Ker(p_i(T)^{e_i})$ so that $V = V_1 \oplus \dots \oplus V_t$. Let $\boldsymbol{x}_i$ be the vector in V_i such that $\boldsymbol{v} = \boldsymbol{x}_1 + \dots + \boldsymbol{x}_t$. Then $\mu_{T,\boldsymbol{x}_i}(x) = p_i(x)^{e_i}$. Note that*

$$\langle T, \boldsymbol{v}\rangle = \langle T, \boldsymbol{x}_1\rangle \oplus \dots \oplus \langle T, \boldsymbol{x}_t\rangle.$$

By Lemma (4.9) each $\langle T, \boldsymbol{x}_i\rangle$ has a T-invariant complement W_i in V_i. Note that

$$\begin{aligned} &W_i \ \cap \ (W_1 + \dots + W_{i-1} + W_{i+1} + \dots + W_t) \\ \subset\, &V_i \ \cap \ (V_1 + \dots + V_{i-1} + V_{i+1} + \dots + V_t) = \{\mathbf{0}\}, \end{aligned}$$

and therefore $W_1 + W_2 + \dots + W_t = W_1 \oplus \dots \oplus W_t$. Set $W = W_1 + W_2 + \dots + W_t$. Then W is T-invariant and a complement to $\langle T, \boldsymbol{v}\rangle$ in V.

Our final structure theorem is the following:

Theorem 4.16 *Let V be a finite-dimensional vector space and T a linear operator on V. Then there are vectors $\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_r$ such that the following hold:*

i. $V = \langle T, \boldsymbol{w}_1\rangle \oplus \dots \oplus \langle T, \boldsymbol{w}_r\rangle$.

ii. If $d_i(x) = \mu_{T,\boldsymbol{w}_i}(x)$ then $d_r(x)|d_{r-1}(x)| \dots |d_1(x) = \mu_T(x)$.

Proof *The proof is by the second principle of induction on $dim(V)$. If $dim(V) = 1$, there is nothing to prove so assume $dim(V) > 1$. Let $\boldsymbol{v}$ be a vector in V such that $\mu_{T,\boldsymbol{v}}(x) = \mu_T(x)$. If $V = \langle T, \boldsymbol{v}\rangle$ then we are done, so we may assume that $V \neq \langle T, \boldsymbol{v}\rangle$. By Lemma (4.15), there is a T-invariant complement W to $\langle T, \boldsymbol{v}\rangle$ in V. The dimension of W is less than the dimension of V. Set $T' = T_{|W}$. By the inductive hypothesis, there are vectors $\boldsymbol{u}_1, \dots, \boldsymbol{u}_{r-1}$ in W such that*

i. $W = \langle T', \boldsymbol{u}_1\rangle \oplus \dots \oplus \langle T, \boldsymbol{u}_{r-1}\rangle$.

ii. If $f_i(x) = \mu_{T',\boldsymbol{u}_i}(x)$ then $f_{r-1}(x)|f_{r-2}(x)| \dots |f_1(x)$. However, for each $i, 1 \leq i \leq r-1, \mu_{T',\boldsymbol{u}_i}(x) = \mu_{T,\boldsymbol{u}_i}(x)$. Moreover, since $\mu_{T,\boldsymbol{v}}(x) = \mu_T(x)$ it follows that $\mu_{T,\boldsymbol{u}_1}(x)|\mu_{T,\boldsymbol{v}}(x)$. Set $\boldsymbol{v}_1 = \boldsymbol{v}, \boldsymbol{v}_i = \boldsymbol{u}_{i-1}$ for $2 \leq i \leq r$. It is then the case that

$$V = \langle T, \boldsymbol{v}_1\rangle \oplus \langle T, \boldsymbol{v}_2\rangle \oplus \dots \oplus \langle T, \boldsymbol{v}_r\rangle.$$

Moreover, for $i > 1, d_i(x) = \mu_{T,\boldsymbol{v}_i}(x) = f_{i-1}(x)$ and therefore
$d_r(x)|d_{r-1}(x)| \dots d_2(x)$ and $d_2(x)|\mu_T(x) = \mu_{T,\boldsymbol{v}} = d_1(x)$.

Definition 4.18 *The polynomials $d_1(x), d_2(x), \dots, \dots, d_r(x)$ are called the* **invariant factors of** T.

Definition 4.19 *Let V be an n-dimensional vector space and T be a linear operator on V. The polynomial (of degree n) obtained by multiplying the invariant factors of T is called the* **characteristic polynomial of** T. *It is denoted by $\chi_T(x)$.*

Note that one of the invariant factors is $\mu_T(x)$ and therefore $\mu_T(x)$ divides the characteristic polynomial, $\chi_T(x)$. Since $\mu_T(T) = \mathbf{0}_{V \to V}$, we have proved the following:

Theorem 4.17 $\chi_T(T) = 0_{V \to V}$.

The fact that the operator obtained when the characteristic polynomial of T is evaluated at T is the zero operator goes by the name of the **Cayley–Hamilton theorem**. In this guise it is immediate as a consequence of how we have defined the characteristic polynomial. The form in which the Cayley–Hamilton theorem is meaningful will be taken up in a later chapter.

As a consequence of the result that every independent sequence from a vector space can be extended to a basis, we proved that every subspace has a complement. This can be interpreted to mean that every subspace invariant under the identity map, I_V, has an invariant complement. Are there other operators that have the same property? There are, but before we get to a characterization, we first give a name to such operators:

Definition 4.20 *Let T be a linear operator on a finite-dimensional vector space V. The operator T is said to be* **completely reducible** *if every T-invariant subspace U has a T-complement.*

Completely reducible operators are characterized by the following theorem whose proof we leave as an exercise.

Theorem 4.18 *Let T be a linear operator on a finite-dimensional vector space. Then T is completely reducible if and only if the minimum polynomial of T has distinct irreducible factors.*

Suppose T is an operator and we want to compute $T^n(\boldsymbol{v})$ for some natural number n. Such a computation can be simplified significantly if there is a basis $\mathcal{B}$ such that $\mathcal{M}_T(\mathcal{B}, \mathcal{B})$ is diagonal. We illustrate with an example.

Example 4.6 *Let $T : \mathbb{R}^2 \to \mathbb{R}^2$ be given by*

$$T(\boldsymbol{v}) = \begin{pmatrix} 8 & -3 \\ 14 & -7 \end{pmatrix} = A\boldsymbol{v}.$$

Compute the matrix of T^4 with respect to the standard basis $\mathcal{S} = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right)$.

Set $\mathcal{B} = \left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \end{pmatrix} \right)$. Note that

$$T \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \end{pmatrix} = 2 \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

$$T \begin{pmatrix} 1 \\ 3 \end{pmatrix} = \begin{pmatrix} -1 \\ -3 \end{pmatrix} = - \begin{pmatrix} 1 \\ 3 \end{pmatrix}.$$

Therefore, the matrix of T with respect to $\mathcal{B}$ is $B = \begin{pmatrix} 2 & 0 \\ 0 & -1 \end{pmatrix}$. Now if we let Q be the change of basis matrix from the $\mathcal{B}$ to the standard basis $\mathcal{S}$, $Q = \mathcal{M}_{I_{\mathbb{R}^2}}(\mathcal{B}, \mathcal{S})$ then

$$Q^{-1}AQ = \begin{pmatrix} 2 & 0 \\ 0 & -1 \end{pmatrix} = B.$$

It then follows that $[Q^{-1}AQ]^4 = Q^{-1}A^4Q = \begin{pmatrix} 2 & 0 \\ 0 & -1 \end{pmatrix}^4 = \begin{pmatrix} 16 & 0 \\ 0 & 1 \end{pmatrix}$. Then

$$A^4 = Q \begin{pmatrix} 16 & 0 \\ 0 & 1 \end{pmatrix} Q^{-1} = \begin{pmatrix} 46 & 17 \\ 90 & 29 \end{pmatrix}.$$

Definition 4.21 *We call a linear operator T on a finite-dimensional vector space V* **diagonalizable** *if there exists a basis $\mathcal{B}$ for V such that $\mathcal{M}_T(\mathcal{B}, \mathcal{B})$ is a diagonal matrix.*

There is a very nice characterization of diagonalizable operators which we state but leave as an exercise.

Theorem 4.19 *Let V be a finite-dimensional vector space and T a linear operator on V. Then T is diagonalizable if and only if T is completely reducible and $\mu_T(x)$ factors into linear factors.*

Exercises

1. Let S be an operator on a finite-dimensional real vector space U and assume that

$$U = \langle S, \boldsymbol{u}_1\rangle \oplus \langle S, \boldsymbol{u}_2\rangle \cdots \oplus \langle S, \boldsymbol{u}_6\rangle$$

and

$$\mu_{S,\boldsymbol{u_1}}(x) = \mu_{S,\boldsymbol{u_2}}(x) = (x^2+1)^5, \mu_{S,\boldsymbol{u_3}}(x) = (x^2+1)^4$$

$$\mu_{S,\boldsymbol{u_4}}(x) = \mu_{S,\boldsymbol{u_5}}(x) = (x^2+1)^2, \mu_{S,\boldsymbol{u_6}}(x) = x^2+1.$$

Set $U_i = \{\boldsymbol{u} \in U | (S^2 + I_U)^i(\boldsymbol{u}) = \boldsymbol{0}\}$ for $i = 1, 2, 3, 4, 5, 6$. Determine the dimension of each U_i.

2. Let T be a linear operator on the finite-dimensional real vector space V and assume that the elementary divisors of T are as follows:

$$(x+2)^2, (x+2)^2, x+2;$$

$$(x^2+1)^3, (x^2+1)^2, (x^2+1)^2, x^2+1;$$

$$(x^2-x+1)^4, (x^2-x+1)^3, (x^2-x+1)^2, (x^2-x+1)^2.$$

Determine the invariant factors of T as well as the dimension of V.

3. Let $T \in \mathcal{L}(\mathbb{R}^4, \mathbb{R}^4)$ be the operator given by

$$T(\boldsymbol{v}) = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \boldsymbol{v}.$$

Determine the invariant factors of T.

4. Let $T \in \mathcal{L}(\mathbb{R}^4, \mathbb{R}^4)$ be the operator given by

$$T(\boldsymbol{v}) = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \boldsymbol{v}.$$

Determine the invariant factors of T.

5. Let $T \in \mathcal{L}(\mathbb{R}^4, \mathbb{R}^4)$ be the operator given by

$$T(\boldsymbol{v}) = \begin{pmatrix} -3 & 2 & 2 & -4 \\ -3 & 1 & 4 & -4 \\ -2 & 0 & 3 & -2 \\ -1 & 0 & 2 & -1 \end{pmatrix} \boldsymbol{v}.$$

Determine the elementary divisors and the invariant factors of T.

6. Let $T \in \mathcal{L}(\mathbb{F}_2^4, \mathbb{F}_2^4)$ be the operator given by

$$T(\boldsymbol{v}) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Determine the elementary divisors and the invariant factors of T.

7. Prove Theorem (4.18).

8. Prove Theorem (4.19).

9. Let T be a linear operator on a finite-dimensional vector space V over an infinite field $\mathbb{F}$ (for example, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$) and let $p_1(x), \dots, p_t(x)$ be the distinct irreducible polynomials that divide $\mu_T(x)$. Prove that there exists infinitely many T-invariant subspaces if and only if there are infinitely many T-invariant subspaces in the p_i-Sylow subspace $V(p_i)$ for some i.

10. Let T be a linear operator on a finite-dimensional vector space V over an infinite field $\mathbb{F}$. Prove that T is a cyclic operator if and only if there are finitely many T-invariant subspaces.

11. Let T be an operator on the finite-dimensional vector space V over the field $\mathbb{F}$ and assume that $\mu_T(x) = p(x)^m q(x)^n$, where $p(x), q(x)$ are distinct irreducible polynomials in $\mathbb{F}[x]$, with at least one of m, n greater than 1. Let $a(x), b(x)$ be polynomials such that $a(x)p(x)^m + b(x)q(x)^n = 1$. Set $f(x) = a(x)p(x)^m q(x) + b(x)q(x)^n p(x)$. Prove that $f(T)$ is a nilpotent operator.

12. Let T be an operator on a vector space V of dimension n and assume that $\mu_T(x) = p(x)^m$, where $p(x)$ is an irreducible polynomial of degree d. For each $j < m$, set $U_i = \{\boldsymbol{v} \in v | p(T)^i(\boldsymbol{v}) = \boldsymbol{0}\}$ and $m_i = dim(U_i)$. Note that d divides m_i for each i.

a) Prove that the number of elementary divisors (invariant factors) of T is equal to $\frac{m_1}{d}$.

b) For $j > 1$, prove that the number of elementary divisors divisible by $p(x)^j$ is equal to $\frac{m_j - m_{j-1}}{d}$.

13. Let V be an n-dimensional vector space over a field $\mathbb{F}$, $T \in \mathcal{L}(V, V)$ with $\mu_T(x) = p_1(x)^{e_1} \dots p_t(x)^{e_t}$ where $p_1(x), \dots, p_t(x)$ are distinct irreducible polynomials with $deg(p_i(x)) = d_i$. Set $V_i = Ker(p_i(T)^n)$ so that $V = V_1 \oplus \cdots \oplus V_t$. Set $m_i = \frac{dim(V_i)}{d_i}$. Prove that $\chi_T(x) = p_1(x)^{m_1} \dots p_t(x)^{m_t}$.

4.6 Canonical Forms

In this section, we continue to study the structure of a linear operator T on a finite-dimensional vector space V. We make use of the two ways we have of decomposing the space V into a direct sum of T-invariant subspaces to obtain bases of V for which the matrix of T takes a nice form.

What You Need to Know

In order to fully understand the new material in this section you should have mastered the following concepts: a vector space is a direct sum of subspaces, basis of a finite-dimensional vector space, operator on a finite-dimensional vector space, coordinate vector with respect to a basis, matrix of a linear transformation, minimal polynomial of an operator T on a finite-dimensional vector space, for an operator T on a finite-dimensional vector space V a T-invariant subspace, for an operator T on a finite-dimensional vector space V a T-cyclic subspace, an invariant factor of a linear operator T, and an elementary divisor of T of a linear operator T.

Let V be a finite-dimensional vector space and T a linear operator on V. We have thus far exhibited two fundamental ways to decompose V as a direct sum of T-invariant subspaces:

i. By cyclic subspaces whose orders are the invariant factors of T.

ii. By cyclic subspaces whose orders are the elementary divisors of T.

The objective of this section is to use the results of Section (4.5) in order to choose a basis $\mathcal{B}$ for V such that the matrix $\mathcal{M}_T(\mathcal{B},\mathcal{B})$ has a particularly "nice form." We begin with a definition that makes precise the notion of a "nice form" of a matrix.

Definition 4.22 *A square matrix of the form*

$$\begin{pmatrix} A_1 & & & 0 \\ & \cdot & & \\ & & \cdot & \\ & & & \cdot & \\ 0 & & & A_s \end{pmatrix},$$

where the A_i are square matrices occurring along the diagonal and all entries outside these matrices are zero is called a **block diagonal matrix**.

Example 4.7 *The matrix*

$$A = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & -4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 1 & 0 \\ 0 & 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}$$

is a block diagonal matrix with three diagonal blocks:

$$A_1 = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}, A_2 = \begin{pmatrix} -4 \end{pmatrix}, A_3 = \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{pmatrix}.$$

The next lemma indicates the connection of block diagonal matrices to our objective.

Lemma 4.7 *Let V be a finite-dimensional vector space, T a linear operator on V, and assume that $V = V_1 \oplus \cdots \oplus V_s$, where each space V_i is T-invariant. Set $T_i = T_{|V_i}$ and let $\mathcal{B}_i$ be a basis for V_i and $\mathcal{B} = \mathcal{B}_1 \sharp \ldots \sharp \mathcal{B}_s$ the basis for V obtained by concatenating sequences $\mathcal{B}_i$. Let $A = \mathcal{M}_T(\mathcal{B}, \mathcal{B})$ and $A_i = \mathcal{M}_{T_i}(\mathcal{B}_i, \mathcal{B}_i)$. Then A is block diagonal with s diagonal blocks equal to the A_i.*

In light of this, we turn our attention to ways for choosing a basis for a space with a cyclic operator T.

Definition 4.23 *Let $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$. The* **companion matrix of** *$f(x)$ is the $m \times m$ matrix*

$$C(f) = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{m-1} \end{pmatrix}.$$

Lemma 4.8 *Let V be a finite-dimensional vector space and T a linear operator on V. Assume that T is cyclic, say, $V = \langle T, \boldsymbol{v} \rangle$ and $\mu_T(x) = \mu_{T,\boldsymbol{v}}(x) = f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$.*

Set $\boldsymbol{v}_1 = \boldsymbol{v}$. Assume that $\boldsymbol{v}_k$ has been defined and $k < m$. Then set $\boldsymbol{v}_{k+1} = T(\boldsymbol{v}_k) = T^k(\boldsymbol{v})$. Then $\mathcal{B} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m)$ is a basis for V and $\mathcal{M}_T(\mathcal{B}, \mathcal{B}) = C(f)$, the companion matrix of $f(x)$.

Proof *That $\mathcal{B}$ is a basis was proved in part iii) of Theorem (4.2).*

Now suppose $k < m$. Then $T(\boldsymbol{v}_k) = \boldsymbol{v}_{k+1}$ and consequently the coordinate vector of $T(\boldsymbol{v}_k)$ with respect to $\mathcal{B}$ is $\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, *where the single 1 occurs in the $k+1$ position.*

On the other hand,

$$T^m + \cdots + a_1T + a_0I_V(\boldsymbol{v}) = T^m(\boldsymbol{v}) + \cdots + a_1T(\boldsymbol{v}) + a_0\boldsymbol{v} = \mathbf{0}.$$

Therefore,

$$T(\boldsymbol{v}_m) = T^m(\boldsymbol{v}) = -a_{m-1}T^{m-1}(\boldsymbol{v}) - \cdots - a_1T(\boldsymbol{v}) - a_0\boldsymbol{v} =$$
$$-a_{m-1}\boldsymbol{v}_m - a_{m-2}\boldsymbol{v}_{m-1} - \cdots - a_1\boldsymbol{v}_2 - a_0\boldsymbol{v}_1.$$

Thus, the coordinate vector of $T(\boldsymbol{v}_m)$ with respect to $\mathcal{B}$ is $\begin{pmatrix} -a_0 \\ -a_1 \\ \vdots \\ -a_{m-2} \\ -a_{m-1} \end{pmatrix}$. *It now follows that $\mathcal{M}_T(\mathcal{B}, \mathcal{B}) = C(f)$ as asserted.*

Definition 4.24 *Let V be a finite-dimensional vector space and T be a linear operator on V. By applying Lemma (4.7) and Lemma (4.8) to the direct sum decomposition of V obtained from the invariant factors, we obtain the* **rational canonical form of** T.

We next turn our attention to a cyclic operator T on a space V with $\mu_T(x) = p(x)^m$, where $p(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$ is irreducible.

Theorem 4.20 *Let T be a linear operator on the space V and assume that $V = \langle T, \boldsymbol{v}\rangle$ and $\mu_{T,\boldsymbol{v}}(x) = \mu_T(x) = p(x)^m$, where $p(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$ is irreducible. Let $\mathcal{B}$ be the following sequence of vectors*

$$\boldsymbol{v}_1 = \boldsymbol{v}, \boldsymbol{v}_2 = T(\boldsymbol{v}), \dots, \boldsymbol{v}_d = T^{d-1}(\boldsymbol{v});$$

$$\boldsymbol{v}_{d+1} = p(T)(\boldsymbol{v}), \boldsymbol{v}_{d+2} = Tp(T)(\boldsymbol{v}); \dots \boldsymbol{v}_{2d} = T^{d-1}p(T)(\boldsymbol{v});$$

$$\vdots$$

$$\boldsymbol{v}_{(m-1)d+1} = p(T)^{m-1}(\boldsymbol{v}), \boldsymbol{v}_{(m-1)d+2} = Tp(T)^{m-1}(\boldsymbol{v}), \dots$$

$$\boldsymbol{v}_{md} = T^{d-1}p(T)^{m-1}(\boldsymbol{v}).$$

Then $\mathcal{B}$ is a basis for V. Moreover, the matrix of T with respect to $\mathcal{B}$ is

$$\begin{pmatrix} C(p) & 0_{d\times d} & 0_{d\times d} & \dots & 0_{d\times d} & 0_{d\times d} \\ L & C(p) & 0_{d\times d} & \dots & 0_{d\times d} & 0_{d\times d} \\ \vdots & \vdots & \vdots \dots & \vdots & \vdots & \\ 0_{d\times d} & 0_{d\times d} & 0_{d\times d} & \dots & C(p) & 0_{d\times d} \\ 0_{d\times d} & 0_{d\times d} & 0_{d\times d} & \dots & L & C(p) \end{pmatrix}, \tag{4.1}$$

where $C(p)$ is the companion matrix of $p(x)$ and L is a $d \times d$ matrix with a single non-zero entry, a 1 in the (1,d)-position.

Proof *Since V is cyclic, the dimension of V is equal to the degree of $\mu_T(x)$ and is therefore md. There are md vectors in the sequence so it suffices to prove that the sequence is independent. Note that the largest degree of a polynomial $x^k p(x)^l$ with $0 \le k \le d-1, 0 \le l \le m-1$ is $d-1+d(m-1) = md-1$. It follows from this that any non-trivial dependence relation on $\mathcal{B}$ will give rise to a polynomial $g(x)$ of degree less than md such that $g(T) = \mathbf{0}_{V\to V}$ contradicting the assumption that the minimal polynomial of T has degree md. Thus, $\mathcal{B}$ is a basis.*

We now compute the coordinate vector of $T(\boldsymbol{v}_j)$ with respect to $\mathcal{B}$. Suppose $j = kd+l$, where $0 \le k \le m-1$ and $1 \le l < d$. Then $\boldsymbol{v}_j = T^{l-1}p(T)^k(\boldsymbol{v})$ and $T(\boldsymbol{v}_j) = T^l p(T)^k(\boldsymbol{v}) = \boldsymbol{v}_{j+1}$. On the other hand, if $j = kd$ with $1 \le k < m$ then

$$\begin{aligned} T(\boldsymbol{v}_j) &= T(T^{d-1}p(T)^{k-1})(\boldsymbol{v}) \\ &= T^d p(T)^{k-1}(\boldsymbol{v}) = [p(T) - a_0 I_V - a_1 T - \dots - a_{d-1}T^{d-1}]p(T)^{k-1}(\boldsymbol{v}) \\ &= p(T)^k(\boldsymbol{v}) - a_0 p(T)^{k-1}(\boldsymbol{v}) - a_1 Tp(T^{k-1}(\boldsymbol{v}) - \dots - a_{d-1}p(T)^{k-1}(\boldsymbol{v}) \\ &= \boldsymbol{v}_{kd+1} - a_0 \boldsymbol{v}_{(k-1)d+1} - a_1 \boldsymbol{v}_{(k-1)d+2} - \dots - a_{d-1}\boldsymbol{v}_{kd}. \end{aligned}$$

Then the coordinate vector of $T(\boldsymbol{v}_{kd})$ *has zeros in entries 1 through* $(k-1)d$ *followed by the entries of the vector*

$$\begin{pmatrix} -a_0 \\ -a_1 \\ \vdots \\ -a_{d-1} \\ 1 \end{pmatrix}$$

and then zeros through the end. This is the kd^{th} *column of the matrix in Equation (4.1).*

Finally, suppose $j = md$. *Then*

$$\begin{aligned} T(\boldsymbol{v}_j) &= T(\boldsymbol{v}_{md}) \\ &= T(T^{d-1}p(T)^{m-1})(\boldsymbol{v}) = T^d p(T)^{m-1} \\ &= [p(T) - a_0 I_V - a_1 T - \cdots - a_{d-1}T^{d-1}]p(T)^{m-1}(\boldsymbol{v}) \\ &= p(T)^m(\boldsymbol{v}) - a_0 p(T)^{m-1}(\boldsymbol{v}) - a_1 T p(T^{m-1}(\boldsymbol{v}) - \cdots - a_{d-1}p(T)^{m-1}(\boldsymbol{v}) \\ &= -a_0\boldsymbol{v}_{(m-1)d+1} - a_1\boldsymbol{v}_{(m-1)d+2} - \cdots - a_{d-1}\boldsymbol{v}_{kd}. \end{aligned}$$

Then the coordinate vector of $T(\boldsymbol{v}_{md})$ *has* $d(m-1)$ *zeros followed by* $\begin{pmatrix} -a_0 \\ -a_1 \\ \vdots \\ -a_{d-1} \end{pmatrix}$, *which is the last column of the matrix in Equation (4.1). This completes the proof of the theorem.*

Definition 4.25 *The matrix in Equation (4.1) is called the* **generalized Jordan** m**-block centered at** $C(p(x))$. *It is denoted by* $J_m(p(x))$.

Definition 4.26 *Let* T *be a linear operator on a finite-dimensional vector space* V. *The block diagonal matrix whose diagonal blocks are the generalized Jordan blocks for the elementary divisors of* T *is called the* **generalized Jordan form** *of* T.

Example 4.8 *Let* T *be a linear operator on the space* $\mathbb{R}^{10}$ *and have minimum polynomial* $(x^2+2x+2)^3$ *and characteristic polynomial* $(x^2+2x+2)^5$. *Then* T *will have either two or three generalized Jordan blocks, depending on whether* *the elementary divisors (invariant factors) are* $(x^2+2x+2)^3, (x^2+2x+2)^2$ *or* $(x^2+2x+2)^3, x^2+2x+2, x^2+2x+2$.

In the former case, the generalized Jordan blocks are

$$\begin{pmatrix} 0 & -2 & 0 & 0 \\ 1 & -2 & 0 & 0 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & -2 \end{pmatrix}, \begin{pmatrix} 0 & -2 & 0 & 0 & 0 & 0 \\ 1 & -2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 & 0 & 0 \\ 0 & 0 & 1 & -2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 0 & 1 & -2 \end{pmatrix}.$$

In the latter case, there are two blocks $\begin{pmatrix} 0 & -2 \\ 1 & -2 \end{pmatrix}$ *and then one block*

$$\begin{pmatrix} 0 & -2 & 0 & 0 & 0 & 0 \\ 1 & -2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 & 0 & 0 \\ 0 & 0 & 1 & -2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 0 & 1 & -2 \end{pmatrix}.$$

Exercises

1. Find the rational canonical form of a linear transformation on a vector space over $\mathbb{Q}$ whose elementary divisors are $(x^2+x+1)^2, (x^2+x+1), (x^2+2)^2$.

2. Let $T \in \mathcal{L}(\mathbb{Q}^2, \mathbb{Q}^2)$ be given by $T(\boldsymbol{v}) = \begin{pmatrix} 1 & -1 \\ 1 & 3 \end{pmatrix} \boldsymbol{v}$. Find the rational canonical form of T.

3. Let $T \in \mathcal{L}(\mathbb{Q}^3, \mathbb{Q}^3)$ be given by $T(\boldsymbol{v}) = \begin{pmatrix} 1 & -1 & -4 \\ 1 & -1 & -3 \\ -1 & 2 & -2 \end{pmatrix} \boldsymbol{v}$. Find the rational canonical form of T.

4. Let $T \in \mathcal{L}(\mathbb{C}^4, \mathbb{C}^4)$ be given by $T(\boldsymbol{v}) = \begin{pmatrix} -5 & -1 & 9 & 8 \\ -1 & 7 & -2 & -2 \\ -2 & 7 & -1 & -3 \\ -1 & 4 & -2 & 1 \end{pmatrix} \boldsymbol{v}$. Find the Jordan canonical form of T.

5. Let T be the operator on $M_{22}(\mathbb{Q})$ defined by $T(\boldsymbol{m}) = \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix} \boldsymbol{m}$. Find the generalized Jordan canonical form.

6. Let T be an operator on a four-dimensional vector space V over the field $\mathbb{F}_2$ and assume that $T^2 = I_V$ but $T \neq I_V$. Determine all possible generalized Jordan canonical forms of T.

7. Let T be an operator on a six-dimensional vector space V over the field $\mathbb{F}_2$ and assume that $T^4 = I_V$ but $T^2 \neq I_V$. Determine all possible generalized Jordan canonical forms of T.

8. Assume T is a nilpotent operator on a four-dimensional vector space. Determine all the possible Jordan canonical forms of T. (An operator T on an n-dimensional space V is ***nilpotent*** if $T^n = \mathbf{0}_{V \to V}$).

9. Prove if a nilpotent operator T is completely reducible, then $T = \mathbf{0}_{V \to V}$.

10. Assume T is a linear operator on a finite-dimensional space V and that the minimal polynomial of T is $p(x)^e$ for an irreducible polynomial $p(x)$ with $e > 1$. Prove that $p(T)$ is a nilpotent operator.

11. Let S be an operator on the finite-dimensional vector space V and $\mathcal{B}$ be a basis for V. Let S' be the operator such that $\mathcal{M}_{S'}(\mathcal{B}, \mathcal{B}) = \mathcal{M}_S(\mathcal{B}, \mathcal{B})^{tr}$. Prove that S and S' have the same elementary divisors.

12. Let T be the operator on $\mathbb{Q}^4$ defined by $T(\boldsymbol{v}) = \begin{pmatrix} -2 & -2 & -2 & 4 \\ 5 & 4 & 3 & -3 \\ -5 & -3 & -1 & -4 \\ -4 & -3 & -2 & 1 \end{pmatrix} \boldsymbol{v}$.

Find the generalized Jordan form of T.

4.7 Operators on Real and Complex Vector Spaces

In this short section we turn our attention specifically to the structure of an operator on a finite-dimensional real or complex vector space. We make use of the general structure theorems and results on canonical forms to determine the (generalized) Jordan canonical form for a real or complex operator.

What You Need to Know

To successfully navigate the material of this new section you should by now have mastered the following concepts: finite-dimensional vector space, real vector space, complex vector space, operator on a vector space, eigenvalue of an operator on a vector space, eigenvector of an operator on a vector space, invariant factors and elementary divisors of an operator on a finite-dimensional vector space, generalized Jordan canonical form of an operator on a finite-dimensional vector space.

Operators on Complex Vector Spaces

Recall, the complex numbers are algebraically closed, which means that every polynomial of degree n factors into n linear polynomials, equivalently, a monic irreducible polynomial has the form $x - \lambda$ for some scalar $\lambda \in \mathbb{C}$.

Also recall, for a linear operator T on a vector space V, a vector $\boldsymbol{v}$ is an eigenvector with eigenvalue λ if $T(\boldsymbol{v}) = \lambda\boldsymbol{v}$.

Definition 4.27 *Assume V is a vector space and λ is an eigenvalue of the operator $T \in \mathcal{L}(V,V)$. The subspace $Ker(T - \lambda I_V)$ is the* **eigenspace** *of λ. Its dimension is called the* **geometric multiplicity** *of λ.*

Definition 4.28 *Let V be an n-dimensional vector space, T an operator on V, and λ an eigenvalue of T. Set $V_\lambda = \{\boldsymbol{v} \in V | (T - \lambda I_V)^n(\boldsymbol{v}) = \boldsymbol{0}\}$. Elements of V_λ are* **generalized eigenvectors**. *The* **algebraic multiplicity** *of λ is $dim(V_\lambda)$.*

Let V be a finite-dimensional complex vector space, T a linear operator on V with distinct eigenvalues $\lambda_1, \lambda_2, \dots, \lambda_t$. By Theorem (4.13)

$$V = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_t}.$$

Moreover,

$$n = dim(V) = dim(V_{\lambda_1}) + dim(V_{\lambda_2}) + \cdots + dim(V_{\lambda_t}).$$

As a consequence of Corollary (4.11), each $V_i = V_{\lambda_i}$ has a decomposition

$$V_{\lambda_i} = \langle T, \boldsymbol{u}_{i,1}\rangle \oplus \cdots \oplus \langle T, \boldsymbol{u}_{i,s_i}\rangle.$$

Suppose now that $\boldsymbol{v}$ is a generalized eigenvector for the eigenvalue λ and $\mu_{T,\boldsymbol{v}}(x) = (x-\lambda)^m$. It is a consequence of Theorem (4.20) that the following vectors are a basis for $\langle T, \boldsymbol{v}\rangle$.

$$\boldsymbol{v} = \boldsymbol{v}_1, (T-\lambda I)(\boldsymbol{v}) = \boldsymbol{v}_2, (T-\lambda I)^2(\boldsymbol{v}) = \boldsymbol{v}_3, \ldots, \boldsymbol{v}_m = (T-\lambda I)^{m-1}(\boldsymbol{v}) \quad (4.2)$$

It also follows from Theorem (4.20) that the matrix of $T_{|\langle T,\boldsymbol{v}\rangle}$ with respect to the basis (4.2) is

$$\begin{pmatrix} \lambda & 0 & 0 & 0 & \ldots & 0 \\ 1 & \lambda & 0 & 0 & \ldots & 0 \\ 0 & 1 & \lambda & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & \lambda \end{pmatrix}. \quad (4.3)$$

Definition 4.29 *The matrix of Equation (4.3) is called a* **Jordan block of size** m **centered at** λ. *It is denoted by* $J_m(\lambda)$.

Now suppose we decompose $V_i = V_{\lambda_i}$ as $\langle T, \boldsymbol{u}_{i1}\rangle \oplus \ldots \langle T, \boldsymbol{u}_{is_i}\rangle$, where $\mu_{T,\boldsymbol{u}_{ij}}(x) = (x-\lambda_i)^{m_{ij}}$, and $m_{i1} \geq m_{i2} \geq \cdots \geq m_{ir_i}$. Then we can choose bases for each $\langle T, \boldsymbol{u}_{ij}\rangle$ as above and their join is a basis for V_i. With respect to this basis, the matrix of $T|_{V_i}$ is the block diagonal matrix

$$\begin{pmatrix} J_{m_{i1}}(\lambda_i) & 0 & 0 & \ldots & 0 \\ 0 & J_{m_{i2}}(\lambda_i) & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & 0 & \ldots & J_{m_{ir_i}}(\lambda_i) \end{pmatrix}.$$

If we denote this matrix by $\mathcal{M}(V_i)$, then by taking the join of such bases for each V_i the matrix of T with respect to this basis will be

$$\begin{pmatrix} \mathcal{M}(V_1) & 0 & 0 & \ldots & 0 \\ 0 & \mathcal{M}(V_2) & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & 0 & \ldots & \mathcal{M}(V_t) \end{pmatrix}.$$

Definition 4.30 *Let T be a linear operator on a finite-dimensional complex vector space V. The block diagonal matrix whose diagonal blocks are the Jordan blocks for the elementary divisors of T is called the* **Jordan canonical form of** T.

Operators on Real Vector Spaces

Recall that a monic irreducible polynomial over $\mathbb{R}$ has either the form $x-a$ or x^2+bx+c, where $b^2-4c<0$. Consequently, if T is an operator on a finite-dimensional real vector space then the elementary divisors are either of the form $(x-a)^d$ or $(x^2+bx+c)^d$ with $b^2-4c<0$.

In the former case, a generalized Jordan block is a Jordan block and has the form

$$\begin{pmatrix} a & 0 & 0 & \dots & 0 & 0 \\ 1 & a & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a & 0 \\ 0 & 0 & 0 & \dots & 1 & a \end{pmatrix}.$$

In the latter case, a generalized Jordan block has the form

$$\begin{pmatrix} A & 0_{2\times 2} & 0_{2\times 2} & \dots & 0_{2\times 2} & 0_{2\times 2} \\ L & A & 0_{2\times 2} & \dots & 0_{2\times 2} & 0_{2\times 2} \\ \vdots & \vdots & \vdots & \dots & \vdots & \\ 0_{2\times 2} & 0_{2\times 2} & 0_{2\times 2} & \dots & A & 0_{2\times 2} \\ 0_{2\times 2} & 0_{2\times 2} & 0_{2\times 2} & \dots & L & A \end{pmatrix}.$$

where $A=\begin{pmatrix} 0 & -b \\ 1 & -c \end{pmatrix}$ and $L=\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

We can now state:

Theorem 4.21 *Let T be an operator on a real finite-dimensional vector space. Then there exists a basis $\mathcal{B}$ such that $\mathcal{M}_T(\mathcal{B},\mathcal{B})$ is block diagonal and each block is either of the form*

$$\begin{pmatrix} a & 0 & 0 & \dots & 0 & 0 \\ 1 & a & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a & 0 \\ 0 & 0 & 0 & \dots & 1 & a \end{pmatrix}$$

for a real scalar a or

$$\begin{pmatrix} A & 0_{2\times 2} & 0_{2\times 2} & \dots & 0_{2\times 2} & 0_{2\times 2} \\ L & A & 0_{2\times 2} & \dots & 0_{2\times 2} & 0_{2\times 2} \\ \vdots & \vdots & \vdots & \dots & \vdots & \\ 0_{2\times 2} & 0_{2\times 2} & 0_{2\times 2} & \dots & A & 0_{2\times 2} \\ 0_{2\times 2} & 0_{2\times 2} & 0_{2\times 2} & \dots & L & A \end{pmatrix},$$

where $A = \begin{pmatrix} 0 & -b \\ 1 & -c \end{pmatrix}$, $L = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ *and* $b^2 - 4c < 0$.

Exercises

1. For a linear operator T on a finite-dimensional complex vector space V, prove the following are equivalent:

i. T is completely reducible.

ii. The minimal polynomial of T has no repeated roots.

iii. V has a basis consisting of eigenvectors for T.

iv. The Jordan canonical form of T is a diagonal matrix.

2. For a linear operator T on an n-dimensional complex vector space V, prove the following are equivalent:

i. There does not exist a direct sum decomposition $V = U \oplus W$ with U, W non-trivial T-invariant subspaces;

ii. The Jordan canonical form of T consists of a single Jordan block of size n.

3. The following matrix is the rational canonical form of a **real** linear operator T. Determine the invariant factors, (real) elementary divisors, minimal polynomial, and the characteristic polynomial of T.

$$\begin{pmatrix} 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

4. Determine the generalized Jordan canonical form of the operator of Exercise 3.

5. Suppose the matrix of Exercise 3 is the matrix of a complex operator T on $\mathbb{C}^7$ with respect to the standard basis. Determine the Jordan canonical form of T.

6. Give an example of two linear operators S, T on a finite-dimensional complex space such that $\chi_S(x) = \chi_T(x), \mu_S(x) = \mu_T(x)$ but S and T are not similar.

7. Find all Jordan forms of a linear operator on $\mathbb{C}^8$ that have minimum polynomial $x^2(x+2i)^3$.

8. Assume S, T are linear operators on a finite-dimensional complex space V and $ST = TS$. Prove that there exists a basis $\mathcal{B}$ for V such that $\mathcal{M}_S(\mathcal{B}, \mathcal{B})$ and $\mathcal{M}_T(\mathcal{B}, \mathcal{B})$ are both in Jordan canonical form.

9. Compute the generalized canonical Jordan form of the linear operator on $\mathbb{R}^4$ that has matrix $\begin{pmatrix} 0 & 0 & 0 & -16 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 8 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ with respect to the standard basis.

10. Let T be an operator on a finite-dimensional complex vector space V. Prove that there are operators D and N such that $T = D + N$ and which satisfy the following:

i. D is diagonalizable.

ii. N is nilpotent.

iii. $DN = ND$.

Moreover, prove that there are polynomials $d(x), n(x)$ such that $D = d(T), N = n(T)$ and use this to prove the D and N are unique.

11. Assume V is a real finite-dimensional vector space. Prove that T does not have a real eigenvalue if and only if every T-invariant subspace of V has even dimension. In particular, $dim(V)$ is even.

12. Give an example of a linear operator T on $\mathbb{R}^2$ such that T does not have an eigenvalue but T^2 is diagonalizable.

13. Let S, T be operators on $\mathbb{C}^n$ with S invertible. Assume that ST is diagonalizable. Prove that TS is diagonalizable.

5

Normed and Inner Product Spaces

CONTENTS

This chapter is about real and complex vector spaces equipped with an inner product or, more generally, a norm. An inner product can be usefully thought of as a generalization of the dot product defined on $\mathbb{R}^n$ whereas a norm assigns to each vector a "length." In the first section we define the concept of an inner product, give several examples, and investigate basic properties. In section two we indicate how we can obtain a norm from an inner product, in particular, we prove that the Cauchy–Schwartz inequality holds for an inner product space as well as the triangle inequality. In section three we introduce several new concepts including that of an orthogonal sequence of vectors in an inner product space, an orthogonal basis, orthonormal sequence of vectors, and an orthonormal basis. We show how to obtain an orthogonal (orthonormal basis) of a finite-dimensional inner product space when given a basis of that space. In section four we prove that if U is a subspace of an finite-dimensional inner product space $(V, \langle\ ,\ \rangle)$ then V is the direct sum of U and its orthogonal complement. This is used to define the orthogonal projection onto U. In section five we define the dual space V' of a finite-dimensional vector space V. We also define, for a basis $\mathcal{B}_V$ in V, the basis, $\mathcal{B}_{V'}$, of V' dual to $\mathcal{B}_V$. For a linear transformation T from a finite-dimensional vector space V to a finite-dimensional space W, we define the transpose transformation T' from W' to V'. We investigate the relationship between that matrix of T with respect to bases $\mathcal{B}_V$ and $\mathcal{B}_W$ and the matrix of the transpose transformation T' with respect to the bases $\mathcal{B}_{W'}$ and $\mathcal{B}_{V'}$, which are dual to $\mathcal{B}_W$ and $\mathcal{B}_V$, respectively. In section six, we make use of the transpose of a linear transformation $T : V \to W$ to define the adjoint transformation, $T^* : W \to V$, of T. In section seven we introduce the general notion of a normed vector space, give several examples, and characterize the norm that arises from an inner product space.

5.1 Inner Products

What You Need to Know

In order for the new material in this section to make sense you should have a fundamental understanding of the following concepts: a real vector space, a complex vector space, the space $\mathbb{R}^n$, the space $\mathbb{C}^n$, the space $M_{nn}(\mathbb{R})$, and the space $M_{nn}(\mathbb{C})$, the dot product on $\mathbb{R}$.

We recall the definition of the dot product:

Definition 5.1 *Let* $\boldsymbol{u} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}, \boldsymbol{v} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$ *be two real n-vectors. Then the* **dot product** *of* $\boldsymbol{u}$ *and* $\boldsymbol{v}$ *is given by* $\boldsymbol{u} \cdot \boldsymbol{v} = u_1v_1 + u_2v_2 + \cdots + u_nv_n$.

It is the dot product that allows one to introduce notions like the length (norm, magnitude) of a vector as well as the angle between two vectors.

The basic properties of the dot product are enumerated in the following:

Theorem 5.1 *Let* $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}$ *be vectors from* $\mathbb{R}^n$ *and* γ *any scalar. Then the following hold:*

1. $\boldsymbol{u} \cdot \boldsymbol{u} \geq 0$ *and* $\boldsymbol{u} \cdot \boldsymbol{u} = 0$ *if and only if* $\boldsymbol{u} = \boldsymbol{0}$. *We say that the dot product is* **positive definite**.

2.$\boldsymbol{u} \cdot \boldsymbol{v} = \boldsymbol{v} \cdot \boldsymbol{u}$. *We say that the dot product is* **symmetric**.

3. $(\boldsymbol{u} + \boldsymbol{v}) \cdot \boldsymbol{w} = \boldsymbol{u} \cdot \boldsymbol{w} + \boldsymbol{v} \cdot \boldsymbol{w}$. *We say that the dot product is* **additive** *in the first argument.*

4. For all $(\gamma \boldsymbol{u}) \cdot \boldsymbol{v} = \boldsymbol{u} \cdot (\gamma \boldsymbol{v}) = \gamma(\boldsymbol{u} \cdot \boldsymbol{v})$. *We say the dot product is* **homogeneous** *with respect to scalars.*

We take the properties of the dot product as the basis for our definition of a real or complex inner product space. Because the definition encompasses both real and complex spaces, the conditions are slightly modified from Theorem (5.1).

Definition 5.2 *Let V be a vector space over the field $\mathbb{F}$, where $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. An* **inner product on** V *is a function*

$$\langle\ ,\ \rangle : V \times V \to \mathbb{F},$$

which satisfies:

1. For every vector $\boldsymbol{u}$, $\langle \boldsymbol{u}, \boldsymbol{u} \rangle$ is a non-negative real number and $\langle \boldsymbol{u}, \boldsymbol{u} \rangle = 0$ if and only if $\boldsymbol{u} = \mathbf{0}$. This means that $\langle\ ,\ \rangle$ is **positive definite***.*

2. For all vectors $\boldsymbol{u}, \boldsymbol{v}$, and $\boldsymbol{w}$, $\langle \boldsymbol{u} + \boldsymbol{v}, \boldsymbol{w} \rangle = \langle \boldsymbol{u}, \boldsymbol{w} \rangle + \langle \boldsymbol{v}, \boldsymbol{w} \rangle$. We say that $\langle\ ,\ \rangle$ is **additive** *in the first argument.*

3. For all vectors $\boldsymbol{u}, \boldsymbol{v}$ and scalars γ, $\langle \gamma\boldsymbol{u}, \boldsymbol{v} \rangle = \gamma\langle \boldsymbol{u}, \boldsymbol{v} \rangle$. We say that $\langle\ ,\ \rangle$ is **homogeneous** *in the first argument.*

4. For all vectors $\boldsymbol{u}$ and $\boldsymbol{v}$, $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = \overline{\langle \boldsymbol{v}, \boldsymbol{u} \rangle}$. We say that $\langle\ ,\ \rangle$ is **conjugate symmetric***.*

By an **inner product space***, we mean a pair $(V, \langle\ ,\ \rangle)$ consisting of a real or complex vector space V and an inner product $\langle\ ,\ \rangle$ on V.*

In 4) of the definition, $\overline{\langle \boldsymbol{v}, \boldsymbol{u} \rangle}$ refers to the complex conjugate of $\langle \boldsymbol{v}, \boldsymbol{u} \rangle$.

Definition 5.3 *By the* **usual inner product** *on the space $\mathbb{C}^n$ we mean the inner product defined by*

$$\begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} \cdot \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix} = w_1\overline{z_1} + w_2\overline{z_2} + \cdots + w_n\overline{z_n}.$$

The inner product spaces $(\mathbb{R}^n, \cdot)$ and $(\mathbb{C}^n, \cdot)$ with the usual inner product are often referred to as **Euclidean inner product spaces** *.*

Example 5.1 *Let $V = \mathbb{F}^n, \mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$ and let $a = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ where α_i are positive real numbers. Define*

$$\left\langle \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix}, \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix} \right\rangle = \alpha_1 w_1\overline{z_1} + \alpha_2 w_2\overline{z_2} + \cdots + \alpha_n w_n\overline{z_n}.$$

This is the **weighted Euclidean inner product** *with weights a.*

Example 5.2 *Let $V = \mathbb{F}^n$ where $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$, S be an invertible operator on V and let $\langle\ ,\ \rangle_{EIP}$ denote the Euclidean inner product on V. Define*

$$\langle \boldsymbol{u}, \boldsymbol{v}\rangle_S = \langle S(\boldsymbol{u}), S(\boldsymbol{v})\rangle_{EIP}.$$

Example 5.3 *Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. Recall that $\mathbb{F}_{(n)}[x]$ is the space of dimension $n+1$ consisting of all polynomials with coefficients in $\mathbb{F}$ of degree at most n. For $f(x), g(x) \in \mathbb{F}_{(n)}[x]$ set*

$$\langle f(x), g(x)\rangle = \int_0^1 f(x)\overline{g(x)}dx.$$

This defines an inner product on $\mathbb{F}_{(n)}[x]$.

Definition 5.4 *Let $A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$. The* **trace of** *$A$ is defined to be the sum of the diagonal entries:*

$$Trace(A) = a_{11} + a_{22} + \cdots + a_{nn}.$$

Example 5.4 *Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. For $A, B \in M_{nn}(\mathbb{F})$ set*

$$\langle A, B\rangle = Trace(A^{tr}\overline{B}).$$

Here A^{tr} is the transpose of the matrix A. This defines an inner product on $M_{nn}(\mathbb{F})$.

This is known as the Frobenius inner product.

Exercises

1. Prove Theorem (5.1).

2. Prove that if $\langle\ ,\ \rangle$ is an inner product on a real or complex space V, then for vectors $\boldsymbol{u}, \boldsymbol{v}$ and scalar γ

$$\langle \boldsymbol{u}, \gamma\boldsymbol{v}\rangle = \overline{\gamma}\langle \boldsymbol{u}, \boldsymbol{v}\rangle.$$

3. Prove that if $\langle\ ,\ \rangle$ is an inner product on a real or complex space V then for vectors $\boldsymbol{u}, \boldsymbol{v}$ and $\boldsymbol{w}$

$$\langle \boldsymbol{u}, \boldsymbol{v} + \boldsymbol{w} \rangle = \langle \boldsymbol{u}, \boldsymbol{v} \rangle + \langle \boldsymbol{u}, \boldsymbol{w} \rangle.$$

4. Prove that the function defined in Example (5.1) is an inner product.

5. Prove that the function defined in Example (5.2) is an inner product.

6. Prove that the function defined in Example (5.4) is an inner product.

7. Assume that $V_i, i = 1, 2$ are vector spaces over $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$ and $\langle\ ,\ \rangle_i$, $i = 1, 2$ is an inner product on V_i. Set $V = V_1 \oplus V_2$ and define $\langle\ ,\ \rangle : V \times V \to \mathbb{F}$ by

$$\langle (\boldsymbol{u}_1, \boldsymbol{u}_2), (\boldsymbol{v}_1, \boldsymbol{v}_2) \rangle = \langle \boldsymbol{u}_1, \boldsymbol{v}_1 \rangle_1 + \langle \boldsymbol{u}_2, \boldsymbol{v}_2 \rangle_2$$

for $\boldsymbol{u}_1, \boldsymbol{v}_1 \in V_1, \boldsymbol{u}_2, \boldsymbol{v}_2 \in V_2$. Determine whether $\langle\ ,\ \rangle$ is an inner product on V. Prove your conclusion.

8. Let $(V, \langle\ ,\ \rangle)$ be an inner product space and $\mathcal{L} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ a sequence of vectors. Prove that $\mathcal{L}$ is linearly independent if and only if the following matrix is invertible:

$$A = \begin{pmatrix} \langle \boldsymbol{v}_1, \boldsymbol{v}_1 \rangle & \langle \boldsymbol{v}_2, \boldsymbol{v}_1 \rangle & \ldots & \langle \boldsymbol{v}_n, \boldsymbol{v}_1 \rangle \\ \langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle & \langle \boldsymbol{v}_2, \boldsymbol{v}_2 \rangle & \ldots & \langle \boldsymbol{v}_n, \boldsymbol{v}_2 \rangle \\ \vdots & \vdots & \ldots & \vdots \\ \langle \boldsymbol{v}_1, \boldsymbol{v}_n \rangle & \langle \boldsymbol{v}_2, \boldsymbol{v}_n \rangle & \ldots & \langle \boldsymbol{v}_n, \boldsymbol{v}_n \rangle \end{pmatrix}.$$

9. Let $c_1, c_2, \ldots, c_n \in \mathbb{R}$. Define a function $\langle\ ,\ \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ by

$$\left\langle \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \right\rangle = c_1(x_1 y_1) + \cdots + c_n(x_n y_n).$$

Prove that if $\langle\ ,\ \rangle$ is an inner product then $c_i > 0$ for all i.

10. Let $V = \mathcal{M}_{fin}(\mathbb{N}, \mathbb{R})$, the real space of all maps f from $\mathbb{N}$ to $\mathbb{R}$ such that $spt(f) = \{i \in \mathbb{N} | f(i) \neq 0\}$ is finite. Define $\langle\ ,\ \rangle : V \times V \to \mathbb{R}$ by $\langle f, g \rangle = \sum_{i=1}^{\infty} f(i)g(i)$. Prove that $\langle\ ,\ \rangle$ is an inner product space on V.

11. Let $(V, \langle\ ,\ \rangle)$ be a complex inner product space. For vectors $\boldsymbol{v}, \boldsymbol{w}$, set $\langle \boldsymbol{v}, \boldsymbol{w} \rangle_{\mathbb{R}} = \frac{1}{2}[\langle \boldsymbol{v}, \boldsymbol{w} \rangle + \langle \boldsymbol{w}, \boldsymbol{v} \rangle]$. Consider V to be a real vector space. Is $(V, \langle\ ,\ \rangle_{\mathbb{R}})$ an inner product space? Support your answer with a proof.

5.2 Geometry in Inner Product Spaces

What You Need to Know

To succeed with the new material in this section, you will need to be familiar with the concept of a real inner product space, a complex inner product spaces, as well as subspaces of a vector space.

We begin with a definition.

Definition 5.5 *Let $(V, \langle , \rangle)$ be an inner product space. When $\langle \boldsymbol{u}, \boldsymbol{v}\rangle = 0$ we say that $\boldsymbol{u}, \boldsymbol{v}$ are* **perpendicular** *or* **orthogonal**. *When $\boldsymbol{u}$ and $\boldsymbol{v}$ are orthogonal we often represent this symbolically by writing $\boldsymbol{u} \perp \boldsymbol{v}$.*

Example 5.5 *Let $f(x) = x, g(x) = 2 - 3x$, which are polynomials in $\mathbb{R}_{(2)}[x]$. Then*

$$\int_0^1 f(x)\overline{g(x)} = \int_0^1 (2x - 3x^2)dx = (x^2 - x^3)|_0^1 = 0 - 0 = 0.$$

Thus, $x \perp (2 - 3x)$.

Definition 5.6 *Let $(V, \langle\ ,\ \rangle)$ be an inner product space and $\boldsymbol{u}$ be a vector in V. The* **orthogonal complement** *to $\boldsymbol{u}$, denoted by $\boldsymbol{u}^\perp$, is the set*

$$\{\boldsymbol{v} \in V | \langle \boldsymbol{v}, \boldsymbol{u}\rangle = 0\}.$$

More generally, if $U \subset V$ then $U^\perp$ is the set

$$\{\boldsymbol{v} \in V | \langle \boldsymbol{v}, \boldsymbol{u}\rangle = 0, \forall \boldsymbol{u} \in U\}.$$

We next define a notion of a norm of a vector. This can usefully be thought of as the length of a vector.

Definition 5.7 *Let $(V, \langle\ ,\ \rangle)$ be an inner product space. The* **norm, length, or magnitude** *of the vector $\boldsymbol{u}$, denoted by $\| \boldsymbol{u} \|$, is defined to be*

$$\sqrt{\langle \boldsymbol{u}, \boldsymbol{u}\rangle}.$$

The norm is always defined since $\langle \boldsymbol{u}, \boldsymbol{u}\rangle \geq 0$ and therefore we can always take a square root.

Example 5.6 *Find the norm of the vectors $f(x) = x$ and $g(x) = x^2$ in the inner product space of Example (5.3).*

$\langle x, x\rangle = \int_0^1 x^2 dx = \frac{1}{3}[x^3|_0^1 = \frac{1}{3}$. *So,* $\| x \|= \sqrt{\frac{1}{3}}$

$\langle x^2, x^2\rangle = \int_0^1 x^4 dx = \frac{1}{5}[x^5|_0^1 = \frac{1}{5}$. *Therefore,* $\| x^2 \|= \sqrt{\frac{1}{5}}$.

Definition 5.8 *For two n-vectors $\boldsymbol{u}, \boldsymbol{v}$ in an inner product space $(V, \langle\ ,\ \rangle)$ the* **distance** *between them, denoted by $d(\boldsymbol{u}, \boldsymbol{v})$, is given by $d(\boldsymbol{u}, \boldsymbol{v}) =\| \boldsymbol{u} - \boldsymbol{v} \|$.*

Example 5.7 *Find the distance between the vectors $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 4 \\ 5 & 13 \end{pmatrix}$ in the inner product space of Example (5.4) with $n = 2$.*

$A - B = \begin{pmatrix} 0 & -3 \\ -4 & -12 \end{pmatrix}$.

$$\begin{aligned} (A-B)^{tr}(A-B) &= \begin{pmatrix} 0 & -4 \\ -3 & -12 \end{pmatrix}\begin{pmatrix} 0 & -3 \\ -4 & -12 \end{pmatrix} \\ &= \begin{pmatrix} 16 & 48 \\ 48 & 153 \end{pmatrix}. \end{aligned}$$

The trace of this matrix is 16 + 153 = 169. Therefore, the distance from A to B is $\sqrt{169} = 13$.

Remark 5.1 *If $\boldsymbol{u}$ is a vector and c is a scalar, then $\| c\boldsymbol{v} \|= |c| \| \boldsymbol{u} \|$.*

A consequence of Remark (5.1) is the following:

Theorem 5.2 *Let $\boldsymbol{u}$ be a non-zero vector. Then the norm of $\frac{1}{\|\boldsymbol{u}\|}\boldsymbol{u}$ is 1.*

Proof $\| \frac{1}{\|\boldsymbol{u}\|}\boldsymbol{u} \| \;=\; |\frac{1}{\|\boldsymbol{u}\|}| \| \boldsymbol{u} \| \;=\; \frac{1}{\|\boldsymbol{u}\|} \| \boldsymbol{u} \|= 1.$

Definition 5.9 *A vector $\boldsymbol{u}$ of norm one is called a* **unit vector**. *When we divide a non-zero vector by its norm we say we are* **normalizing** *the vector and the vector so obtained is said to be* **a unit vector in the direction of** $\boldsymbol{u}$.

We next embark on proving several fundamental theorems about inner product spaces. The next theorem should be familiar in the case that $V = \mathbb{R}^2$ with the Euclidean inner product:

Theorem 5.3 Pythagorean theorem

Let $(V, \langle\ ,\ \rangle)$ be an inner product space and $\boldsymbol{u}, \boldsymbol{v} \in V$ be orthogonal. Then

$$\| \boldsymbol{u} + \boldsymbol{v} \|^2 = \| \boldsymbol{u} \|^2 + \| \boldsymbol{v} \|^2 .$$

Proof $\| \boldsymbol{u} + \boldsymbol{v} \|^2 = \langle \boldsymbol{u}+\boldsymbol{v}, \boldsymbol{u}+\boldsymbol{v} \rangle = \langle \boldsymbol{u}, \boldsymbol{u} \rangle + \langle \boldsymbol{u}, \boldsymbol{v} \rangle + \langle \boldsymbol{v}, \boldsymbol{u} \rangle + \langle \boldsymbol{v}, \boldsymbol{v} \rangle$

$$= \langle \boldsymbol{u}, \boldsymbol{u} \rangle + \langle \boldsymbol{v}, \boldsymbol{v} \rangle = \| \boldsymbol{u} \|^2 + \| \boldsymbol{v} \|^2 .$$

In our next result, we show how, given two vectors, $\boldsymbol{u}, \boldsymbol{v}$ with $\boldsymbol{v} \neq \boldsymbol{0}$ we can decompose $\boldsymbol{u}$ into a multiple of $\boldsymbol{v}$ and a vector orthogonal to $\boldsymbol{v}$.

Lemma 5.1 *Let $\boldsymbol{u}, \boldsymbol{v}$ be vectors with $\boldsymbol{v} \neq \boldsymbol{0}$. Then there is a unique scalar α such that $\boldsymbol{u} - \alpha\boldsymbol{v}$ is orthogonal to $\boldsymbol{v}$.*

Proof *We compute the inner product of $\boldsymbol{u} - \alpha\boldsymbol{v}$ and $\boldsymbol{v}$:*

$$\langle \boldsymbol{u} - \alpha\boldsymbol{v}, \boldsymbol{v} \rangle = \langle \boldsymbol{u}, \boldsymbol{v} \rangle - \alpha \langle \boldsymbol{v}, \boldsymbol{v} \rangle. \tag{5.1}$$

Setting the expression in (5.1) equal to zero and solving for α we obtain

$$\alpha = \frac{\langle \boldsymbol{u}, \boldsymbol{v} \rangle}{\langle \boldsymbol{v}, \boldsymbol{v} \rangle} = \frac{\langle \boldsymbol{u}, \boldsymbol{v} \rangle}{\| \boldsymbol{v} \|^2}.$$

Definition 5.10 *Let $\boldsymbol{u}, \boldsymbol{v}$ be vectors in an inner product space $(V, \langle\ ,\ \rangle)$ with $\boldsymbol{v} \neq \boldsymbol{0}$. The vector $\frac{\langle \boldsymbol{u}, \boldsymbol{v} \rangle}{\|\boldsymbol{v}\|^2}\boldsymbol{v}$ is the* **orthogonal projection** *of $\boldsymbol{u}$ onto $\boldsymbol{v}$. The vector $\boldsymbol{u} - \frac{\langle \boldsymbol{u}, \boldsymbol{v} \rangle}{\|\boldsymbol{v}\|^2}\boldsymbol{v}$ is the* **projection of $\boldsymbol{u}$ orthogonal to $\boldsymbol{v}$.** *The expression*

$$\boldsymbol{u} = \frac{\langle \boldsymbol{u}, \boldsymbol{v} \rangle}{\| \boldsymbol{v} \|^2}\boldsymbol{v} + \left(\boldsymbol{u} - \frac{\langle \boldsymbol{u}, \boldsymbol{v} \rangle}{\| \boldsymbol{v} \|^2}\boldsymbol{v} \right)$$

is referred to as an **orthogonal decomposition of $\boldsymbol{u}$** *with respect to $\boldsymbol{v}$.*

Theorem 5.4 *(***Cauchy–Schwartz Inequality***)*

Let $(V, \langle\ ,\ \rangle)$ be an inner product space and $\boldsymbol{u}, \boldsymbol{v}$ be vectors in V. Then

$$|\langle \boldsymbol{u}, \boldsymbol{v}\rangle| \leq \parallel \boldsymbol{u} \parallel\parallel \boldsymbol{v} \parallel \tag{5.2}$$

with equality if and only if the sequence $(\boldsymbol{u}, \boldsymbol{v})$ is linearly dependent.

Proof *If either $\boldsymbol{u} = \boldsymbol{0}$ or $\boldsymbol{v} = \boldsymbol{0}$, then both $|\langle \boldsymbol{u}, \boldsymbol{v}\rangle|$ and $\parallel \boldsymbol{u} \parallel\parallel \boldsymbol{v} \parallel$ are zero and we get equality. So assume $\boldsymbol{u}, \boldsymbol{v} \neq \boldsymbol{0}$. In this case, we can decompose $\boldsymbol{u}$ orthogonally with respect to $\boldsymbol{v}$:*

$$\boldsymbol{u} = \frac{\langle \boldsymbol{u}, \boldsymbol{v}\rangle}{\parallel \boldsymbol{v} \parallel^2}\boldsymbol{v} + \boldsymbol{w},$$

where $\boldsymbol{w} = \boldsymbol{u} - \frac{\langle \boldsymbol{u}, \boldsymbol{v}\rangle}{\|\boldsymbol{v}\|^2}\boldsymbol{v}$ is orthogonal to $\boldsymbol{v}$. We can apply the Pythagorean theorem (Theorem (5.3)) to get

$$\begin{aligned}
\parallel \boldsymbol{u} \parallel^2 &= \parallel \frac{\langle \boldsymbol{u}, \boldsymbol{v}\rangle}{\parallel \boldsymbol{v} \parallel^2}\boldsymbol{v} \parallel^2 + \parallel \boldsymbol{w} \parallel^2 \\
&= (\frac{|\langle \boldsymbol{u}, \boldsymbol{v}\rangle|}{\parallel \boldsymbol{v} \parallel^2})^2 \parallel \boldsymbol{v} \parallel^2 + \parallel \boldsymbol{w} \parallel^2 \\
&= \frac{|\langle \boldsymbol{u}, \boldsymbol{v}\rangle|^2}{\parallel \boldsymbol{v} \parallel^4} \parallel \boldsymbol{v} \parallel^2 + \parallel \boldsymbol{w} \parallel^2 \\
&= \frac{|\langle \boldsymbol{u}, \boldsymbol{v}\rangle|^2}{\parallel \boldsymbol{v} \parallel^2} + \parallel \boldsymbol{w} \parallel^2 \\
&\geq \frac{|\langle \boldsymbol{u}, \boldsymbol{v}\rangle|^2}{\parallel \boldsymbol{v} \parallel^2}.
\end{aligned}$$

Thus, $\parallel \boldsymbol{u} \parallel^2 \geq \frac{|\langle \boldsymbol{u}, \boldsymbol{v}\rangle|^2}{\|\boldsymbol{v}\|^2}$. Multiplying both sides of the inequality by $\parallel \boldsymbol{v} \parallel^2$ and taking square roots, we obtain

$$\parallel \boldsymbol{u} \parallel \cdot \parallel \boldsymbol{v} \parallel \quad \geq \quad |\langle \boldsymbol{u}, \boldsymbol{v}\rangle|.$$

Note that we get equality precisely when $\boldsymbol{w} = \boldsymbol{0}$, which is when $\boldsymbol{u}$ is a multiple of $\boldsymbol{v}$, that is, when $(\boldsymbol{u}, \boldsymbol{v})$ is linearly dependent.

Assume $\boldsymbol{u}, \boldsymbol{v}$ are non-zero vectors in a real inner product space $(V, \langle\ ,\ \rangle)$. Then, as an immediate consequence of the Cauchy–Schwartz inequality we have

$$-1 \leq \frac{\langle \boldsymbol{u}, \boldsymbol{v}\rangle}{\parallel \boldsymbol{u} \parallel\parallel \boldsymbol{v} \parallel} \leq 1.$$

Recall, for any real number r on the interval $[-1, 1]$ there is a unique $\theta \in [0, \pi]$ such that $cos\ \theta = r$. We use this to define the notion of an angle between $\boldsymbol{u}, \boldsymbol{v}$:

Definition 5.11 *Let $(V, \langle\ ,\ \rangle)$ be a real inner product space and $\boldsymbol{u}, \boldsymbol{v}$ vectors in V. If one, but not both $\boldsymbol{u}$ and $\boldsymbol{v}$, is the zero vector, define the angle between $\boldsymbol{u}, \boldsymbol{v}$, denoted by $\angle(\boldsymbol{u}, \boldsymbol{v})$, to be $\frac{\pi}{2}$. If both $\boldsymbol{u}, \boldsymbol{v}$ are non-zero vectors, then* **the angle** *between $\boldsymbol{u}, \boldsymbol{v}$, $\angle(\boldsymbol{u}, \boldsymbol{v})$, is the unique $\theta \in [0, \pi]$ such that cos $\theta = \frac{\langle \boldsymbol{u}, \boldsymbol{v}\rangle}{\|\boldsymbol{u}\|\|\boldsymbol{v}\|}$.*

We can use the Cauchy–Schwartz inequality to prove a familiar theorem from Euclidean geometry. Suppose that $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{u}+\boldsymbol{v}$ are the sides of a triangle. The lengths of the sides of this triangle are $\parallel \boldsymbol{u} \parallel, \parallel \boldsymbol{v} \parallel$ and $\parallel \boldsymbol{u}+\boldsymbol{v} \parallel$. One typically learns in Euclidean geometry that the sum of the lengths of any two sides of a triangle must exceed the length of the third side. This holds in any inner product space:

Theorem 5.5 (Triangle Inequality) *Let $(V, \langle\ ,\ \rangle)$ be an inner product space and $\boldsymbol{u}, \boldsymbol{v}$ be vectors in V. Then*

$$\parallel \boldsymbol{u}+\boldsymbol{v} \parallel \quad \leq \quad \parallel \boldsymbol{u} \parallel + \parallel \boldsymbol{v} \parallel . \tag{5.3}$$

Moreover, when $\boldsymbol{u}, \boldsymbol{v} \neq \boldsymbol{0}$ we have equality if and only if there is a positive λ such that $\boldsymbol{v} = \lambda \boldsymbol{u}$ (we say that $\boldsymbol{u}$ and $\boldsymbol{v}$ are parallel in the same direction).

Proof *Note that when either $\boldsymbol{u}$ or $\boldsymbol{v}$ is the zero vector there is nothing to prove and we have equality, so assume that $\boldsymbol{u}, \boldsymbol{v} \neq \boldsymbol{0}$. Applying properties of an inner product we get*

$$\parallel \boldsymbol{u}+\boldsymbol{v} \parallel^2 = \langle \boldsymbol{u}+\boldsymbol{v}, \boldsymbol{u}+\boldsymbol{v}\rangle$$

by the definition of the norm;

$$= \ \langle \boldsymbol{u}, \boldsymbol{u}\rangle + \langle \boldsymbol{v}, \boldsymbol{v}\rangle + \langle \boldsymbol{u}, \boldsymbol{v}\rangle + \langle \boldsymbol{v}, \boldsymbol{u}\rangle$$

by the additive property of the inner product;

$$= \ \parallel \boldsymbol{u} \parallel^2 + \parallel \boldsymbol{v} \parallel^2 + \langle \boldsymbol{u}, \boldsymbol{v}\rangle + \langle \boldsymbol{v}, \boldsymbol{u}\rangle$$

by the definition of the norm;

$$= \ \parallel \boldsymbol{u} \parallel^2 + \parallel \boldsymbol{v} \parallel^2 + \langle \boldsymbol{u}, \boldsymbol{v}\rangle + \overline{\langle \boldsymbol{u}, \boldsymbol{v}\rangle}$$

by conjugate symmetry;

$$= \ \parallel \boldsymbol{u} \parallel^2 + \parallel \boldsymbol{v} \parallel^2 + 2Re(\langle \boldsymbol{u}, \boldsymbol{v}\rangle);$$

$$\parallel \boldsymbol{u} \parallel^2 + \parallel \boldsymbol{v} \parallel^2 \ + \ 2Re(\langle \boldsymbol{u}, \boldsymbol{v}\rangle) \ \leq \ \parallel \boldsymbol{u} \parallel^2 + \parallel \boldsymbol{v} \parallel^2 + 2|\langle \boldsymbol{u}, \boldsymbol{v}\rangle| \tag{5.4}$$

$$\leq \quad \| \boldsymbol{u} \|^2 + \| \boldsymbol{v} \|^2 + 2 \| \boldsymbol{u} \| \cdot \| \boldsymbol{v} \| \tag{5.5}$$

by the Cauchy–Schwartz inequality;

$$= (\| \boldsymbol{u} \| + \| \boldsymbol{v} \|)^2.$$

By taking square roots, we obtain the required inequality.

In Equation (5.5), we have equality if and only $|\langle \boldsymbol{u}, \boldsymbol{v} \rangle| = \| \boldsymbol{u} \| \cdot \| \boldsymbol{v} \|$ *if and only if* $\boldsymbol{u}$ *is a multiple of* $\boldsymbol{v}$*. In Equation (5.4), we have equality if and only if* $2Re(\langle \boldsymbol{u}, \boldsymbol{v} \rangle) = |\langle \boldsymbol{u}, \boldsymbol{v} \rangle|$*. Together these imply that* $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = \| \boldsymbol{u} \| \cdot \| \boldsymbol{v} \|$*. If* $\boldsymbol{u} = c\boldsymbol{v}$ *for a positive real number, then this holds. On the other hand, suppose* $\boldsymbol{u} = \gamma \boldsymbol{v}$*, where either* γ *is real and negative or* γ *is not real. Then equality does not hold. This completes the theorem.*

The following theorem is often referred to as the **Parallelogram Equality**:

Theorem 5.6 *Assume* $\boldsymbol{u}, \boldsymbol{v} \in V$*. Then*

$$\| \boldsymbol{u} + \boldsymbol{v} \|^2 + \| \boldsymbol{u} - \boldsymbol{v} \|^2 = 2(\| \boldsymbol{u} \|^2 + \| \boldsymbol{v} \|^2).$$

Proof *Let* $\boldsymbol{u}, \boldsymbol{v}$ *be in* V*. We then have*

$$\begin{aligned} \| \boldsymbol{u} + \boldsymbol{v} \|^2 + \| \boldsymbol{u} - \boldsymbol{v} \|^2 &= \langle \boldsymbol{u} + \boldsymbol{v}, \boldsymbol{u} + \boldsymbol{v} \rangle + \langle \boldsymbol{u} - \boldsymbol{v}, \boldsymbol{u} - \boldsymbol{v} \rangle \\ &= \| \boldsymbol{u} \|^2 + \| \boldsymbol{v} \|^2 + \langle \boldsymbol{u}, \boldsymbol{v} \rangle + \langle \boldsymbol{v}, \boldsymbol{u} \rangle + \| \boldsymbol{u} \|^2 \\ &\quad + \| \boldsymbol{v} \|^2 - \langle \boldsymbol{u}, \boldsymbol{v} \rangle - \langle \boldsymbol{v}, \boldsymbol{u} \rangle \\ &= 2 \| \boldsymbol{u} \|^2 + 2 \| \boldsymbol{v} \|^2 \\ &= 2(\| \boldsymbol{u} \|^2 + \| \boldsymbol{v} \|^2). \end{aligned}$$

We state two results for later reference. We prove the first and leave the second as an exercise.

Lemma 5.2 *Let* $(V, \langle \ , \ \rangle)$ *be a real inner product space. Then*

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle = \frac{(\| \boldsymbol{u} + \boldsymbol{v} \|^2 - \| \boldsymbol{u} - \boldsymbol{v} \|^2)}{4}.$$

Proof $\| \boldsymbol{u} + \boldsymbol{v} \|^2 - \| \boldsymbol{u} - \boldsymbol{v} \|^2 = \langle \boldsymbol{u} + \boldsymbol{v}, \boldsymbol{u} + \boldsymbol{v} \rangle - \langle \boldsymbol{u} - \boldsymbol{v}, \boldsymbol{u} - \boldsymbol{v} \rangle$

$= \| \boldsymbol{u} \|^2 + \| \boldsymbol{v} \|^2 + \langle \boldsymbol{u}, \boldsymbol{v} \rangle + \langle \boldsymbol{v}, \boldsymbol{u} \rangle - (\| \boldsymbol{u} \|^2 + \| \boldsymbol{v} \|^2 - \langle \boldsymbol{u}, \boldsymbol{v} \rangle - \langle \boldsymbol{v}, \boldsymbol{u} \rangle)$

$= 2\langle \boldsymbol{u}, \boldsymbol{v} \rangle + 2\langle \boldsymbol{u}, \boldsymbol{v} \rangle = 4\langle \boldsymbol{u}, \boldsymbol{v} \rangle$. *Dividing by 4 yields the result.*

The identity asserted in the next lemma will prove useful in the Chapter 6. We leave its proof as an exercise.

Lemma 5.3 *Let $(V, \langle\ ,\ \rangle)$ be a complex inner product space. Then*

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle = \frac{\| \boldsymbol{u} + \boldsymbol{v} \|^2 - \| \boldsymbol{u} - \boldsymbol{v} \|^2 + \| \boldsymbol{u} + i\boldsymbol{v} \|^2 i - \| \boldsymbol{u} - i\boldsymbol{v} \|^2 i}{4}.$$

Exercises

1. Let $\boldsymbol{u} \in U$. Prove that $\boldsymbol{u}^\perp$ is a subspace of V.

2. If $dim(V) = n$ and $\boldsymbol{u} \neq \boldsymbol{0}$, prove that $dim(\boldsymbol{u}^\perp) = n - 1$.

3. Let $(V, \langle\ ,\ \rangle)$ be an n-dimensional inner product space and W a subspace of V. Prove that $W \cap W^\perp = \{\boldsymbol{0}\}$.

4. Let $V = \mathbb{R}_{(2)}[x]$ with the inner product of Example (5.3). Find a basis for the orthogonal complement to $x^2 + x + 1$.

5. Let $V = M_{22}(\mathbb{R})$ with the inner product of Example (5.4). Find the distance between the matrices $A = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ and $\begin{pmatrix} 5 & 4 \\ -4 & 5 \end{pmatrix}$.

6. Let $V = M_{22}(\mathbb{R})$ with the inner product of Example (5.4). Find the orthogonal complement to the identity matrix.

7. Let $V = M_{22}(\mathbb{R})$ with the inner product of Example (5.4). Find the orthogonal complement to the subspace of diagonal matrices.

8. Let $V = \mathbb{R}_{(2)}[x]$ with the inner product of Example (5.3). Find the distance between x and x^2.

9. Verify that $\boldsymbol{v}$ and $\boldsymbol{u} - \frac{\langle \boldsymbol{u}, \boldsymbol{v} \rangle}{\|\boldsymbol{v}\|^2}\boldsymbol{v}$ are orthogonal.

10. Prove Lemma (5.3).

11. Let $x_1, \ldots, x_n, y_1, \ldots, y_n$ be real numbers. Prove that

$$\left[\sum_{j=1}^{n} (x_j y_j)\right]^2 \leq \left(\sum_{j=1}^{n} \frac{x_j^2}{j}\right)\left(\sum_{j=1}^{n} j y_j^2\right).$$

12. Let $(V, \langle\ ,\ \rangle)$ be an inner product space and $d(\ ,\ )$ the corresponding distance function. Prove the following hold:

a) $d(\boldsymbol{u}, \boldsymbol{v}) \geq 0$ and $d(\boldsymbol{u}, \boldsymbol{v}) = 0$ if and only if $\boldsymbol{u} = \boldsymbol{v}$.

b) $d(\boldsymbol{u}, \boldsymbol{v}) = d(\boldsymbol{v}, \boldsymbol{u})$.

c) $d(\boldsymbol{u}, \boldsymbol{w}) \leq d(\boldsymbol{u}, \boldsymbol{v}) + d(\boldsymbol{v}, \boldsymbol{w})$.

13. Let $V = M_{22}(\mathbb{R})$ with the inner product of Example (5.4). Find the angle between the identity matrix $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and the all 1 matrix $J_2 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$.

14. Let $\boldsymbol{u}, \boldsymbol{v}$ be vectors in an inner product space $(V, \langle\ ,\ \rangle)$ and assume that $\| \boldsymbol{u} + \boldsymbol{v} \| = \| \boldsymbol{u} \| + \| \boldsymbol{v} \|$. Prove for all $c, d \in \mathbb{R}$ that

$$\| c\boldsymbol{u} + \ d\boldsymbol{v} \|^2 = c^2 \| \boldsymbol{u} \|^2 + d^2 \| \boldsymbol{v} \|^2 .$$

15. Let $(V, \langle\ ,\ \rangle_1)$ and $(V, \langle\ ,\ \rangle_2)$ be real inner product spaces with associated distance functions d_1 and d_2. If $d_1(\boldsymbol{u}, \boldsymbol{v}) = d_2(\boldsymbol{u}, \boldsymbol{v})$ for all vectors $\boldsymbol{u}, \boldsymbol{v} \in V$ prove that $\langle \boldsymbol{u}, \boldsymbol{v} \rangle_1 = \langle \boldsymbol{u}, \boldsymbol{v} \rangle_2$ for all vectors $\boldsymbol{u}, \boldsymbol{v}$.

16. Let $(V, \langle\ ,\ \rangle)$ be an inner product space, $\boldsymbol{x} \in V$ a unit vector, and $\boldsymbol{y} \in V$. Prove $\langle \boldsymbol{y}, \boldsymbol{x} \rangle \langle \boldsymbol{x}, \boldsymbol{y} \rangle \leq \langle \boldsymbol{y}, \boldsymbol{y} \rangle$.

5.3 Orthonormal Sets and the Gram–Schmidt Process

What You Need to Know

Understanding the new material in this section depends on mastery of the following concepts: basis of a finite-dimensional vector space, coordinate vector of a vector in a finite-dimensional vector space with respect to a given basis, inner product space, and orthogonal vectors in an inner product space.

We begin with an example:

Example 5.8 *a) Show that the vectors*

$$\boldsymbol{v}_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \boldsymbol{v}_2 = \begin{pmatrix} 2 \\ -1 \\ -1 \end{pmatrix}, \boldsymbol{v}_3 = \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}$$

are mutually orthogonal with respect to the dot product.

b) Prove that the sequence of vectors $(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3)$ is a basis for $\mathbb{R}^3$.

c) Find the coordinate vector of $\boldsymbol{u} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ with respect to $\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3$.

a) We compute the dot products directly

$$\boldsymbol{v}_1 \cdot \boldsymbol{v}_2 = (1)(2) + (1)(-1) + (1)(-1) = 0;$$

$$\boldsymbol{v}_1 \cdot \boldsymbol{v}_3 = (1)(0) + (1)(1) + (1)(-1) = 0;$$

$$\boldsymbol{v}_2 \cdot \boldsymbol{v}_3 = (2)(0) + (-1)(1) + (-1)(-1) = 0.$$

b) We could reduce the matrix $(\boldsymbol{v}_1 \ \boldsymbol{v}_2 \ \boldsymbol{v}_3)$ and show that it is invertible but we give a non-computational argument.

Quite clearly, $\boldsymbol{v}_2$ is not a multiple of $\boldsymbol{v}_1$ and therefore $(\boldsymbol{v}_1, \boldsymbol{v}_2)$ is linearly independent. If $(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3)$ is linearly dependent, then $\boldsymbol{v}_3$ must be a linear combination of $(\boldsymbol{v}_1, \boldsymbol{v}_2)$ by part ii) of Theorem (1.14). So assume that $\boldsymbol{v}_3$ is a linear combination of $(\boldsymbol{v}_1, \boldsymbol{v}_2)$, say, $\boldsymbol{v}_3 = c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2$.

Then $\boldsymbol{v}_3 \cdot \boldsymbol{v}_3 = \boldsymbol{v}_3 \cdot (c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2) = c_1(\boldsymbol{v}_3 \cdot \boldsymbol{v}_1) + c_2(\boldsymbol{v}_3 \cdot \boldsymbol{v}_2)$ by additivity and the scalar property of the dot product.

By a) $\boldsymbol{v}_3 \cdot \boldsymbol{v}_1 = \boldsymbol{v}_3 \cdot \boldsymbol{v}_2 = 0$ and therefore, $\boldsymbol{v}_3 \cdot \boldsymbol{v}_3 = 0$. But then by positive *definiteness,* $\boldsymbol{v}_3 = \mathbf{0}_3$*, a contradiction. Therefore* $\boldsymbol{v}_3$ *is not a linear combination of* $(\boldsymbol{v}_1, \boldsymbol{v}_2)$ *and* $(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3)$ *is linearly independent. Since the dimension of* $\mathbb{R}^3$ *is 3, it follows that* $(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3)$ *is a basis.*

c) We could find the coordinate vector of $\boldsymbol{u}$ *by finding the reduced echelon form of the matrix* $(\boldsymbol{v}_1\ \boldsymbol{v}_2\ \boldsymbol{v}_3 \mid \boldsymbol{u})$*, but we instead make use of the information we obtained from a).*

Write $\boldsymbol{u} = a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + a_3\boldsymbol{v}_3$ *and take the dot product of* $\boldsymbol{u}$ *with* $\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3$*, respectively:*

$$\boldsymbol{u} \cdot \boldsymbol{v}_1 = (a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + a_3\boldsymbol{v}_3) \cdot \boldsymbol{v}_1 = a_1(\boldsymbol{v}_1 \cdot \boldsymbol{v}_1) + a_2(\boldsymbol{v}_2 \cdot \boldsymbol{v}_1) + a_3(\boldsymbol{v}_3 \cdot \boldsymbol{v}_1) \quad (5.6)$$

by additivity and the scalar property of the dot product.

However, we showed in a) that $\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3$ *are mutually orthogonal. Making use of this in Equation (5.6) we get*

$$\boldsymbol{u} \cdot \boldsymbol{v}_1 = a_1(\boldsymbol{v}_1 \cdot \boldsymbol{v}_1). \quad (5.7)$$

A direct computation show shows that $\boldsymbol{u} \cdot \boldsymbol{v}_1 = 6$ *and* $\boldsymbol{v}_1 \cdot \boldsymbol{v}_1 = 3$ *and therefore* $6 = 3a_1$*. Thus,* $a_1 = 2$*. In exactly the same way, we obtain* $a_2 = -\frac{1}{2}, a_3 = -\frac{1}{2}$*.*

Remark 5.2 *If* $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$ *are non-zero vectors such that for* $i \neq j, \langle \boldsymbol{v}_i, \boldsymbol{v}_j \rangle = 0$ *then the vectors are distinct.*

Example (5.8) is the motivation for the next definition:

Definition 5.12 *A sequence* $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$ *of non-zero vectors in an inner product space* $(V, \langle\ ,\ \rangle)$ *is said to be an* **orthogonal sequence** *if for* $i \neq j, \langle \boldsymbol{v}_i, \boldsymbol{v}_j \rangle = 0$*. A set of vectors* $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}$ *is an* **orthogonal set** *if the sequence* $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)$ *is an orthogonal sequence. If* $dim(V) = n$*,* $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ *is a basis for* V *and an orthogonal sequence then it is said to be an* **orthogonal basis** *for V.*

Orthogonal sequences behave like the one in Example (5.8). In particular, they are linearly independent:

Theorem 5.7 *Let* $\mathcal{S} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)$ *be an orthogonal sequence in the inner product space* $(V, \langle\ ,\ \rangle)$*. Then* S *is linearly independent.*

Proof *The proof is by induction on k. Since the vectors in an orthogonal sequence are non-zero, if $k = 1$ (the initial case), then the result is true since a single non-zero vector is linearly independent. We now do the inductive case.*

So assume that every orthogonal sequence of k vectors is linearly independent and that $\mathcal{S} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k, \boldsymbol{v}_{k+1})$ is an orthogonal sequence. We need to show that S is linearly independent. Since $(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k)$ is an orthogonal sequence of length k, by the inductive hypothesis, it is linearly independent.

If $\mathcal{S}$ is linearly dependent, then it must be the case that $\boldsymbol{v}_{k+1}$ is a linear combination of $(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k)$. So assume that $\boldsymbol{v}_{k+1} = c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_k\boldsymbol{v}_k$. We then have

$$\begin{aligned}
\parallel \boldsymbol{v}_{k+1} \parallel^2 &= \langle \boldsymbol{v}_{k+1}, \boldsymbol{v}_{k+1} \rangle \\
&= \left\langle \sum_{i=1}^{k} c_i \boldsymbol{v}_i, \boldsymbol{v}_{k+1} \right\rangle \\
&= \sum_{i=1}^{k} c_i \langle \boldsymbol{v}_i, \boldsymbol{v}_{k+1} \rangle.
\end{aligned}$$

Since $\mathcal{S}$ is an orthogonal sequence, for each $i < k+1, \langle \boldsymbol{v}_i, \boldsymbol{v}_{k+1} \rangle = 0$ from which we can conclude that $\parallel \boldsymbol{v}_{k+1} \parallel^2 = \sum_{i=1}^{k} c_i \langle \boldsymbol{v}_i, \boldsymbol{v}_{k+1} \rangle = 0$. It then follows from positive definiteness that $\boldsymbol{v}_{k+1} = \mathbf{0}$. However, by the definition of an orthogonal sequence, $\boldsymbol{v}_{k+1} \neq \mathbf{0}$, and we have a contradiction. Thus, $\mathcal{S}$ is linearly independent.

It is also the case that for an orthogonal sequence $\mathcal{S} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k)$ in an inner product space $(V, \langle\ ,\ \rangle)$ it is easy to compute the coordinates of a vector in *Span*$(\mathcal{S})$ with respect to $\mathcal{S}$:

Theorem 5.8 *Let $\mathcal{S} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k)$ be an orthogonal sequence and $\boldsymbol{u}$ a vector in Span$(\mathcal{S})$. If $\boldsymbol{u} = c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_k\boldsymbol{v}_k$ is the unique expression of $\boldsymbol{u}$ as a linear combination of the vectors in $\mathcal{S}$ then $c_j = \frac{\langle \boldsymbol{u}, \boldsymbol{v}_j \rangle}{\langle \boldsymbol{v}_j, \boldsymbol{v}_j \rangle}$.*

Proof *Assume $\boldsymbol{u} = c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_k\boldsymbol{v}_k$, then $\langle \boldsymbol{u}, \boldsymbol{v}_j \rangle =$*

$$\langle (c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_k\boldsymbol{v}_k), \boldsymbol{v}_j \rangle = \sum_{i=1}^{k} c_i \langle \boldsymbol{v}_i, \boldsymbol{v}_j \rangle \tag{5.8}$$

by the additivity and scalar properties of the dot product.

Because $\langle \boldsymbol{v}_j, \boldsymbol{v}_i \rangle = 0$ for $j \neq i$, Equation (5.8) reduces to $\langle \boldsymbol{u}, \boldsymbol{v}_j \rangle = c_j \langle \boldsymbol{v}_j, \boldsymbol{v}_j \rangle$. Since $\boldsymbol{v}_j$ is non-zero, $\langle \boldsymbol{v}_j, \boldsymbol{v}_j \rangle \neq 0$, and we can deduce that $c_j = \frac{\langle \boldsymbol{u}, \boldsymbol{v}_i \rangle}{\langle \boldsymbol{v}_j, \boldsymbol{v}_j \rangle}$ as claimed.

The following is a consequence of Theorem (5.8): If W is a subspace of V, $\mathcal{S}$ is an orthogonal sequence and a basis for W, then the computation of the coordinates of a vector $\boldsymbol{u}$ in W with respect to $\mathcal{S}$ is quite easy. The computation of coordinates is even simpler when the vectors in an orthogonal sequence are unit vectors. We give a name to such sequences.

Definition 5.13 *Let $(V, \langle\ ,\ \rangle)$ be an inner product space. An orthogonal sequence $\mathcal{S}$ consisting of unit vectors is called an* **orthonormal sequence**. *If W is a subspace of $V, \mathcal{S}$ is a basis for W, and $\mathcal{S}$ is an orthonormal sequence, then $\mathcal{S}$ is said to be an* **orthonormal basis** *for W.*

The remainder of this section is taken up describing a method for obtaining an orthonormal basis for a subspace W of an inner product space $(V, \langle\ ,\ \rangle)$, given a basis of W. The method is known as the Gram–Schmidt process.

The Gram–Schmidt Process

Assume that W is a subspace of V and that $(\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_m)$ is a basis for W. We shall first define an orthogonal sequence of vectors $(\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_m)$ recursively. Moreover, this sequence will have the property that for each $k, 1 \leq k \leq m, Span(\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_k) = Span(\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_k)$. We then obtain an orthonormal basis by normalizing each vector. More specifically, we will set $\boldsymbol{v}_i = \frac{1}{\|\boldsymbol{x}_i\|}\boldsymbol{x}_i, i = 1, 2, \dots, m$.

To say that we define the sequence recursively means that we will initially define $\boldsymbol{x}_1$. Then, assuming that we have defined $\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_k$ with $k < m$ satisfying the required properties, we will define $\boldsymbol{x}_{k+1}$ such that i) $\boldsymbol{x}_{k+1}$ is orthogonal to $\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_k$ and ii) $Span(\boldsymbol{x}_1, \dots, \boldsymbol{x}_{k+1}) = Span(\boldsymbol{w}_1, \dots, \boldsymbol{w}_{k+1})$. Since the sequence $(\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_{k+1})$ is linearly independent it will then follow that the sequence $(\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_{k+1})$ is linearly independent. In particular, $\boldsymbol{x}_{k+1}$ will not be the zero vector.

The Definition of $\boldsymbol{x}_1$

We begin with the definition of $\boldsymbol{x}_1$ which we set equal to $\boldsymbol{w}_1$.

The Recursion

To get a sense of what we are doing, we first show how to define $\boldsymbol{x}_2$ in terms of $\boldsymbol{w}_2$ and $\boldsymbol{x}_1$ and then $\boldsymbol{x}_3$ in terms of $\boldsymbol{x}_1, \boldsymbol{x}_2$ and $\boldsymbol{w}_3$ before doing the general case.

Defining $\boldsymbol{x}_2$

The idea is to find a linear combination $\boldsymbol{x}_2$ of $\boldsymbol{w}_2$ and $\boldsymbol{x}_1$, which is orthogonal to $\boldsymbol{x}_1$. The vector $\boldsymbol{x}_2$ will be obtained by adding a suitable multiple of $\boldsymbol{x}_1$ to $\boldsymbol{w}_2$. Consequently, we will have that $Span(\boldsymbol{x}_1, \boldsymbol{x}_2) = Span(\boldsymbol{x}_1, \boldsymbol{w}_2) = Span(\boldsymbol{w}_1, \boldsymbol{w}_2)$.

Rather than just write down a formula, we compute the necessary scalar: Assume that $\boldsymbol{x}_2 = \boldsymbol{w}_2 + a\boldsymbol{x}_1$ and that $\langle \boldsymbol{x}_2, \boldsymbol{x}_1 \rangle = 0$. Then

$$0 = \langle \boldsymbol{x}_2, \boldsymbol{x}_1 \rangle = \langle (\boldsymbol{w}_2 + a\boldsymbol{x}_1), \boldsymbol{x}_1 \rangle = \langle \boldsymbol{w}_2, \boldsymbol{x}_1 \rangle + a\langle \boldsymbol{x}_1, \boldsymbol{x}_1 \rangle. \tag{5.9}$$

Solving for a we obtain

$$a = -\frac{\langle \boldsymbol{w}_2, \boldsymbol{x}_1 \rangle}{\langle \boldsymbol{x}_1, \boldsymbol{x}_1 \rangle}. \tag{5.10}$$

Using the value of a obtained in Equation (5.10), we set $\boldsymbol{x}_2 = \boldsymbol{w}_2 - \frac{\langle \boldsymbol{w}_2, \boldsymbol{x}_1 \rangle}{\langle \boldsymbol{x}_1, \boldsymbol{x}_1 \rangle}\boldsymbol{x}_1$.

Defining $\boldsymbol{x}_3$

Now that we have defined $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$ we find a vector $\boldsymbol{x}_3$ which is a linear combination of the form $\boldsymbol{x}_3 = \boldsymbol{w}_3 + a_1\boldsymbol{x}_1 + a_2\boldsymbol{x}_2$. We want to determine a_1, a_2 such that $\boldsymbol{x}_3$ is orthogonal to $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$. Since $\boldsymbol{x}_3$ and $\boldsymbol{x}_1$ are supposed to be orthogonal, we must have

$$\begin{aligned} 0 = \langle \boldsymbol{x}_3, \boldsymbol{x}_1 \rangle &= \langle \boldsymbol{w}_3 + a_1\boldsymbol{x}_1 + a_2\boldsymbol{x}_2, \boldsymbol{x}_1 \rangle \\ &= \langle \boldsymbol{w}_3, \boldsymbol{x}_1 \rangle + a_1\langle \boldsymbol{x}_1, \boldsymbol{x}_1 \rangle + a_2\langle \boldsymbol{x}_2, \boldsymbol{x}_1 \rangle. \end{aligned} \tag{5.11}$$

Because $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$ are orthogonal we get

$$0 = \langle \boldsymbol{w}_3, \boldsymbol{x}_1 \rangle + a_1\langle \boldsymbol{x}_1, \boldsymbol{x}_1 \rangle, a_1 = -\frac{\langle \boldsymbol{w}_3, \boldsymbol{x}_1 \rangle}{\langle \boldsymbol{x}_1, \boldsymbol{x}_1 \rangle}. \tag{5.12}$$

In an entirely analogous way, using the fact that $\boldsymbol{x}_3$ and $\boldsymbol{x}_2$ are supposed to be orthogonal we obtain

$$a_2 = -\frac{\langle \boldsymbol{w}_3, \boldsymbol{x}_2 \rangle}{\langle \boldsymbol{x}_2, \boldsymbol{x}_2 \rangle}. \tag{5.13}$$

Thus,

$$\boldsymbol{x}_3 = \boldsymbol{w}_3 - \frac{\langle \boldsymbol{w}_3, \boldsymbol{x}_1 \rangle}{\langle \boldsymbol{x}_1, \boldsymbol{x}_1 \rangle}\boldsymbol{x}_1 - \frac{\langle \boldsymbol{w}_3, \boldsymbol{x}_2 \rangle}{\langle \boldsymbol{x}_2, \boldsymbol{x}_2 \rangle}\boldsymbol{x}_2. \tag{5.14}$$

Since $\boldsymbol{x}_3$ is obtained by adding a linear combination of $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$ to $\boldsymbol{w}_3$ we have that $Span(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3) = Span(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{w}_3)$. Since $Span(\boldsymbol{x}_1, \boldsymbol{x}_2) = Span(\boldsymbol{w}_1, \boldsymbol{w}_2)$ it then follows that $Span(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3) = Span(\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}_3)$. Since $(\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}_3)$ is linearly independent, $dim(Span(\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}_3)) = 3$. It then must be the case that $\boldsymbol{x}_3 \neq \boldsymbol{0}$.

The General Recursive Case

We now do the general case. So assume that $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k$ have been defined with $k < m$ satisfying

i) $\langle \boldsymbol{x}_i, \boldsymbol{x}_j \rangle = 0$ for $i \neq j$; and

ii) $Span(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k) = Span(\boldsymbol{w}_1,\ \boldsymbol{w}_2, \ldots, \boldsymbol{w}_k)$.

Set

$$\boldsymbol{x}_{k+1} = \boldsymbol{w}_{k+1} - \sum_{j=1}^{k} \frac{\langle \boldsymbol{w}_{k+1}, \boldsymbol{x}_j \rangle}{\langle \boldsymbol{x}_j, \boldsymbol{x}_j \rangle} \boldsymbol{x}_j. \tag{5.15}$$

We show that $\langle \boldsymbol{x}_{k+1}, \boldsymbol{x}_i \rangle = 0$ for all $i = 1, 2, \ldots, k$.

$$\langle \boldsymbol{x}_{k+1}, \boldsymbol{x}_i \rangle = \langle \boldsymbol{w}_{k+1} - \textstyle\sum_{j=1}^{k} \frac{\langle \boldsymbol{w}_{k+1}, \boldsymbol{x}_j \rangle}{\langle \boldsymbol{x}_j, \boldsymbol{x}_j \rangle} \boldsymbol{x}_j, \boldsymbol{x}_i \rangle$$

$$= \langle \boldsymbol{w}_{k+1}, \boldsymbol{x}_i \rangle - \sum_{j=1}^{k} \frac{\langle \boldsymbol{w}_{k+1}, \boldsymbol{x}_j \rangle}{\langle \boldsymbol{x}_j, \boldsymbol{x}_j \rangle} \langle \boldsymbol{x}_j, \boldsymbol{x}_i \rangle. \tag{5.16}$$

Since $\langle \boldsymbol{x}_j, \boldsymbol{x}_i \rangle = 0$ for $i \neq j$, Equation (5.16) becomes

$$\langle \boldsymbol{w}_{k+1}, \boldsymbol{x}_i \rangle - \frac{\langle \boldsymbol{w}_{k+1}, \boldsymbol{x}_i \rangle}{\langle \boldsymbol{x}_i, \boldsymbol{x}_i \rangle} \langle \boldsymbol{x}_i, \boldsymbol{x}_i \rangle = \langle \boldsymbol{w}_{k+1}, \boldsymbol{x}_i \rangle - \langle \boldsymbol{w}_{k+1}, \boldsymbol{x}_i \rangle = 0. \tag{5.17}$$

So, indeed, $\boldsymbol{x}_{k+1}$ as defined is orthogonal to $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k$.

Since $\boldsymbol{x}_{k+1}$ is obtained from $\boldsymbol{w}_{k+1}$ by adding a linear combination of $(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k)$ to $\boldsymbol{w}_{k+1}$, it follows that $Span(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k, \boldsymbol{x}_{k+1}) = Span(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k, \boldsymbol{w}_{k+1})$. Since $Span(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k) = Span(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k)$ we can conclude that $Span(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k, \boldsymbol{x}_{k+1}) = Span(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k, \boldsymbol{w}_{k+1})$. In particular, this implies that $\boldsymbol{x}_{k+1} \neq \mathbf{0}$.

Now normalize each $\boldsymbol{x}_i$ to obtain $\boldsymbol{v}_i$:

$$\boldsymbol{v}_i = \frac{1}{\parallel \boldsymbol{x}_i \parallel} \boldsymbol{x}_i, i = 1, 2, \ldots, m.$$

Since each $\boldsymbol{v}_i$ is obtained from $\boldsymbol{x}_i$ by scaling, it follows that $Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k) = Span(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k) = Span(\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_k)$ for each $k = 1, 2, \ldots, m$.

We state what we have shown as a theorem:

Theorem 5.9 (Gram–Schmidt Process)

Let W be a subspace of the inner product space $(V, \langle\ ,\ \rangle)$ with basis $(\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_m)$. Define $\boldsymbol{x}_1 = \boldsymbol{w}_1$.

Assume that $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k$ have been defined with $k < m$. Set

$$\boldsymbol{x}_{k+1} = \boldsymbol{w}_{k+1} - \sum_{j=1}^{k} \frac{\langle \boldsymbol{w}_{k+1}, \boldsymbol{x}_j \rangle}{\langle \boldsymbol{x}_j, \boldsymbol{x}_j \rangle} \boldsymbol{x}_j,$$

$$\boldsymbol{v}_i = \frac{1}{\parallel \boldsymbol{x}_i \parallel} \boldsymbol{x}_i, i = 1, 2, \ldots, m.$$

Then the following hold:

i. The sequence of vectors $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m)$ is an orthonormal basis of W.

ii. $Span(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k) = Span(\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_k)$, for each $k = 1, 2, \ldots .m$.

When the inner product space $(V, \langle\ ,\ \rangle)$ is finite-dimensional, every subspace of V has a basis; as a consequence of the Gram–Schmidt process, we have the following theorem:

Theorem 5.10 *Let W be a subspace of a finite-dimensional inner product space $(V, \langle\ ,\ \rangle)$. Then W has an orthonormal basis.*

To complete our results, we state the following theorem, which we leave as an exercise.

Theorem 5.11 *Let W be a subspace of the n-dimensional inner product space $(V, \langle\ ,\ \rangle)$. Then $dim(W) + dim(W^{\perp}) = n$.*

Exercises

1. In the Gram–Schmidt process, check that $\langle \boldsymbol{x}_2, \boldsymbol{x}_1 \rangle = 0$.

2. Prove that $\boldsymbol{x}_3$ defined by Equation (5.14) is orthogonal to $\boldsymbol{x}_1, \boldsymbol{x}_2$.

3. Assume $U \subset W$ are subspaces of an inner product space $(V, \langle\ ,\ \rangle)$. Prove that $W^{\perp} \subset U^{\perp}$.

4. Prove Theorem (5.11).

5. Let $(V, \langle\ ,\ \rangle)$ be a finite dimension inner product space and W a subspace of V. Prove that $V = W \oplus W^{\perp}$.

6. Let W be a subspace of a finite-dimensional inner product space $(V, \langle\ ,\ \rangle)$. Prove $W = (W^{\perp})^{\perp}$.

7. Assume U, W are subspaces of the finite-dimensional inner product space $(V, \langle\ ,\ \rangle)$. Prove that $(U+W)^\perp = U^\perp \cap W^\perp$ and $(U \cap W)^\perp = U^\perp + W^\perp$.

An $n \times n$ matrix A with entries $a_{ij}, 1 \leq i, j \leq n$ is ***upper triangular*** if $a_{ij} = 0$ for $i > j$.

8. Let V be an inner product space with basis $\mathcal{B} = (\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_m)$. Let $\mathcal{B}'$ be the basis obtained by the Gram–Schmidt process. Prove that the change of basis matrix from $\mathcal{B}'$ to $\mathcal{B}, \mathcal{M}_{I_V}(\mathcal{B}', \mathcal{B})$, and the change of basis matrix of $\mathcal{B}$ to $\mathcal{B}', \mathcal{M}_{I_V}(\mathcal{B}, \mathcal{B}')$, are upper triangular.

9. Starting with the basis $(1, x, x^2)$ for $\mathbb{R}_{(2)}[x]$, use the Gram–Schmidt process to obtain an orthonormal basis.

10. Assume $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_k)$ is an orthonormal sequence in an inner product space $(V, \langle\ ,\ \rangle)$ and $\boldsymbol{u} \in V$. Prove the following inequality (known as the Bessel inequality)

$$\sum_{i=1}^{k} |\langle \boldsymbol{u}, \boldsymbol{v}_i \rangle|^2 \ \leq\ \parallel \boldsymbol{u} \parallel^2$$

with equality if and only if $\boldsymbol{u} \in Span(\boldsymbol{v}_1, \dots, \boldsymbol{v}_k)$.

11. Let $V = M_{22}(\mathbb{R})$ with the inner product of Example (5.4). Let $W = Span(J_2)$. Find an orthonormal basis for $W^\perp$. Here J_2 is the 2×2 matrix with all entries equal to 1.

12. Let $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ be an orthonormal basis for the inner product space $(V, \langle\ ,\ \rangle)$ and $\boldsymbol{x}, \boldsymbol{y} \in V$. Prove Parseval's identity

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \sum_{i=1}^{n} \langle \boldsymbol{x}, \boldsymbol{v}_i \rangle \overline{\langle \boldsymbol{v}_i, \boldsymbol{y} \rangle}.$$

5.4 Orthogonal Complements and Projections

What You Need to Know

Understanding the new material in this section depends on mastery of the following concepts: basis of a finite-dimensional vector space, coordinate vector of a vector in a finite-dimensional vector space with respect to a given basis, inner product space, orthogonal vectors in an inner product space, orthogonal sequence in an inner product space, orthonormal sequence in an inner product space, and orthogonal basis in an inner product space, orthonormal basis in an inner product space.

Let $(V, \langle\ ,\ \rangle)$ be in inner product space and W a subspace of V. Recall in Section (5.2) we defined the ***orthogonal complement*** $W^\perp$ to W:

$$W^\perp = \{\boldsymbol{v} \in V | \langle \boldsymbol{v}, \boldsymbol{w}\rangle = 0 \text{ for all } \boldsymbol{w} \in W\}.$$

In various places in this chapter, we have demonstrated parts of the next theorem (or assigned them as exercises):

Theorem 5.12 *Let $(V, \langle\ ,\ \rangle)$ be an n-dimensional inner product space and W a subspace of V. Then the following hold:*

1. $W^\perp$ is subspace of V.

2. $W \cap W^\perp = \{\mathbf{0}\}$.

3. $dim(W) + dim(W^\perp) = n$.

4. $W + W^\perp = V$.

5. $W \oplus W^\perp = V$.

By the definition of direct sum it then follows that for every vector $\boldsymbol{v} \in V$, there are unique vectors $\boldsymbol{w} \in W, \boldsymbol{u} \in W^\perp$ such that $\boldsymbol{v} = \boldsymbol{w} + \boldsymbol{u}$. We make use of this in the following definition:

Definition 5.14 *Let W be a subspace of the n-dimensional inner product space $(V, \langle\ ,\ \rangle)$ and let $\boldsymbol{v} \in V$. Assume that $\boldsymbol{v} = \boldsymbol{w} + \boldsymbol{u}$ with $\boldsymbol{w} \in W, \boldsymbol{u} \in W^\perp$. Then the vector $\boldsymbol{w}$ is called the* **orthogonal projection of $\boldsymbol{v}$ onto** *W and is denoted by $Proj_W(\boldsymbol{v})$. The vector $\boldsymbol{u}$ is called the* **projection of $\boldsymbol{v}$ orthogonal to** *W and is denoted by $Proj_{W^\perp}(\boldsymbol{v})$.*

Remark 5.3 *1) With a direct sum decomposition $V = W \oplus W^{\perp}$ we previously defined a linear transformation $Proj_{(W,W^{\perp})}$. The transformation $Proj_{(W,W^{\perp})}$ and $Proj_W$ are the same transformation. Likewise, $Proj_{(W^{\perp},W)} = Proj_{W^{\perp}}$.*

2) For a vector $\boldsymbol{w} \in W, Proj_W(\boldsymbol{w}) = \boldsymbol{w}$. Since for any vector $\boldsymbol{v} \in V, Proj_W(\boldsymbol{v}) \in W$ we conclude that $Proj_W^2(\boldsymbol{v}) = (Proj_W \circ Proj_W)(\boldsymbol{v}) = Proj_W(Proj_W(\boldsymbol{v})) = Proj_W(\boldsymbol{v})$.

The next example in real Euclidean space shows how to find the orthogonal projection of a vector $\boldsymbol{u}$ onto a subspace W when given a basis of W.

Example 5.9 *Let $\boldsymbol{w}_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \boldsymbol{w}_2 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix}$, and $\boldsymbol{w}_3 = \begin{pmatrix} 1 \\ 1 \\ -2 \\ 1 \end{pmatrix}$ and denote by W the span of $(\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}_3)$. Compute $Proj_W(\boldsymbol{u})$ if $\boldsymbol{u} = \begin{pmatrix} 6 \\ 6 \\ -3 \\ 2 \end{pmatrix}$.*

We want to find the vector $c_1\boldsymbol{w}_1 + c_2\boldsymbol{w}_2 + c_3\boldsymbol{w}_3$ such that $\boldsymbol{u} - (c_1\boldsymbol{w}_1 + c_2\boldsymbol{w}_2 + c_3\boldsymbol{w}_3)$ is in $W^{\perp}$. In particular, for each i we must have

$$[\boldsymbol{u} - (c_1\boldsymbol{w}_1 + c_2\boldsymbol{w}_2 + c_3\boldsymbol{w}_3)] \cdot \boldsymbol{w}_i =$$

$$\boldsymbol{u} \cdot \boldsymbol{w}_i - c_1(\boldsymbol{w}_1 \cdot \boldsymbol{w}_i) - c_2(\boldsymbol{w}_2 \cdot \boldsymbol{w}_i) - c_3(\boldsymbol{w}_3 \cdot \boldsymbol{w}_i) = 0. \tag{5.18}$$

For each i, Equation (5.18) is equivalent to

$$c_1(\boldsymbol{w}_1 \cdot \boldsymbol{w}_i) + c_2(\boldsymbol{w}_2 \cdot \boldsymbol{w}_i) + c_3(\boldsymbol{w}_3 \cdot \boldsymbol{w}_i) = \boldsymbol{u} \cdot \boldsymbol{w}_i. \tag{5.19}$$

This means that $\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix}$ is a solution to the linear system with augmented matrix

$$\left(\begin{array}{ccc|c} \boldsymbol{w}_1 \cdot \boldsymbol{w}_1 & \boldsymbol{w}_2 \cdot \boldsymbol{w}_1 & \boldsymbol{w}_3 \cdot \boldsymbol{w}_1 & \boldsymbol{u} \cdot \boldsymbol{w}_1 \\ \boldsymbol{w}_1 \cdot \boldsymbol{w}_2 & \boldsymbol{w}_2 \cdot \boldsymbol{w}_2 & \boldsymbol{w}_3 \cdot \boldsymbol{w}_2 & \boldsymbol{u} \cdot \boldsymbol{w}_2 \\ \boldsymbol{w}_1 \cdot \boldsymbol{w}_3 & \boldsymbol{w}_2 \cdot \boldsymbol{w}_3 & \boldsymbol{w}_3 \cdot \boldsymbol{w}_3 & \boldsymbol{u} \cdot \boldsymbol{w}_3 \end{array}\right). \tag{5.20}$$

It follows from Exercise (5.1.8) that this system has a unique solution, which we now compute.

In our specific case we must solve the linear system with augmented matrix

$$\begin{pmatrix} 4 & 2 & 1 & | & 11 \\ 2 & 4 & -1 & | & 7 \\ 1 & -1 & 7 & | & 20 \end{pmatrix}. \tag{5.21}$$

This system has the unique solution $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$.

Example (5.9) suggests the following theorem, which provides a method for computing $Proj_W(\boldsymbol{u})$ when given a basis for the subspace W.

Theorem 5.13 *Let W be a subspace of the n-dimensional inner product space $(V, \langle\ ,\ \rangle)$ with basis $\mathcal{B} = (\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_k)$ and let $\boldsymbol{u}$ be a vector in V. Then $Proj_W(\boldsymbol{u}) = c_1\boldsymbol{w}_1 + c_2\boldsymbol{w}_2 + \dots c_k\boldsymbol{w}_k$, where $\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix}$ is the unique solution to the linear system with augmented matrix*

$$\begin{pmatrix} \langle \boldsymbol{w}_1, \boldsymbol{w}_1 \rangle & \langle \boldsymbol{w}_2, \boldsymbol{w}_1 \rangle & \dots & \langle \boldsymbol{w}_k, \boldsymbol{w}_1 \rangle & | & \langle \boldsymbol{u}, \boldsymbol{w}_1 \rangle \\ \langle \boldsymbol{w}_1, \boldsymbol{w}_2 \rangle & \langle \boldsymbol{w}_2, \boldsymbol{w}_2 \rangle & \dots & \langle \boldsymbol{w}_k, \boldsymbol{w}_2 \rangle & | & \langle \boldsymbol{u}, \boldsymbol{w}_2 \rangle \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots \\ \langle \boldsymbol{w}_1, \boldsymbol{w}_k \rangle & \langle \boldsymbol{w}_2, \boldsymbol{w}_k \rangle & \dots & \langle \boldsymbol{w}_k, \boldsymbol{w}_k \rangle & | & \langle \boldsymbol{u}, \boldsymbol{w}_k \rangle \end{pmatrix}. \tag{5.22}$$

When given an orthogonal basis for W, it is much easier to compute the orthogonal projection of a vector $\boldsymbol{v}$ onto W because the matrix of Equation (5.22) becomes a diagonal matrix. We illustrate with an example in the real Euclidean space $\mathbb{R}^4$ with the dot product before formulating this as a theorem.

Example 5.10 *Let* $\boldsymbol{w}_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$, $\boldsymbol{w}_2 = \begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix}$, *and set* $W = Span(\boldsymbol{w}_1, \boldsymbol{w}_2)$.

Find the orthogonal projection of the vector $\boldsymbol{v} = \begin{pmatrix} 1 \\ 3 \\ -4 \\ 6 \end{pmatrix}$ *onto* W.

We claim that $Proj_W(\boldsymbol{v}) = \frac{\boldsymbol{v}\cdot\boldsymbol{w}_1}{\boldsymbol{w}_1\cdot\boldsymbol{w}_1}\boldsymbol{w}_1 + \frac{\boldsymbol{v}\cdot\boldsymbol{w}_2}{\boldsymbol{w}_2\cdot\boldsymbol{w}_2}\boldsymbol{w}_2$.

We compute this vector

$$\frac{\boldsymbol{v}\cdot\boldsymbol{w}_1}{\boldsymbol{w}_1\cdot\boldsymbol{w}_1}\boldsymbol{w}_1+\frac{\boldsymbol{v}\cdot\boldsymbol{w}_2}{\boldsymbol{w}_2\cdot\boldsymbol{w}_2}\boldsymbol{w}_2=\frac{6}{4}\begin{pmatrix}1\\1\\1\\1\end{pmatrix}+\frac{2}{4}\begin{pmatrix}1\\1\\-1\\-1\end{pmatrix}=\begin{pmatrix}2\\2\\1\\1\end{pmatrix}. \tag{5.23}$$

The vector $\boldsymbol{w}=\begin{pmatrix}2\\2\\1\\1\end{pmatrix}$ *is a linear combination of* $\boldsymbol{w}_1$ *and* $\boldsymbol{w}_2$ *and so in* W*. We need to show that the vector* $\boldsymbol{v}-\boldsymbol{w}=\begin{pmatrix}-1\\1\\-5\\5\end{pmatrix}$ *is orthogonal to* $\boldsymbol{w}_1$ *and* $\boldsymbol{w}_2$*.*

$$(\boldsymbol{v}-\boldsymbol{w})\cdot\boldsymbol{w}_1=\begin{pmatrix}-1\\1\\-5\\5\end{pmatrix}\cdot\begin{pmatrix}1\\1\\1\\1\end{pmatrix}=-1+1-5+5=0. \tag{5.24}$$

$$(\boldsymbol{v}-\boldsymbol{w})\cdot\boldsymbol{w}_2=\begin{pmatrix}-1\\1\\-5\\5\end{pmatrix}\cdot\begin{pmatrix}1\\1\\-1\\-1\end{pmatrix}=-1+1+5-5=0. \tag{5.25}$$

Theorem 5.14 *Let* W *be a subspace of the inner product space* $(V,\langle\ ,\ \rangle)$ *and* $\mathcal{B}=(\boldsymbol{w}_1,\boldsymbol{w}_2,\dots,\boldsymbol{w}_k)$ *be an orthogonal basis for* W*. Let* $\boldsymbol{u}$ *be a vector in* V*. Then*

$$Proj_W(\boldsymbol{u})=\sum_{j=1}^{k}\frac{\langle\boldsymbol{u},\boldsymbol{w}_j\rangle}{\langle\boldsymbol{w}_j,\boldsymbol{w}_j\rangle}\boldsymbol{w}_j.$$

Proof *Set* $\boldsymbol{w}=\sum_{i=1}^{k}\frac{\langle\boldsymbol{u},\boldsymbol{w}_i\rangle}{\langle\boldsymbol{w}_i,\boldsymbol{w}_i\rangle}\boldsymbol{w}_i$*, an element of* W*. We need to show that* $\boldsymbol{u}-\boldsymbol{w}$ *is perpendicular to* $\boldsymbol{w}_i$ *for* $i=1,2,\dots,k$*.*

From the additive and scalar properties of the inner product $\langle\ ,\ \rangle$ *we can conclude that* $\langle\boldsymbol{u}-\boldsymbol{w},\boldsymbol{w}_i\rangle=\langle\boldsymbol{u},\boldsymbol{w}_i\rangle-\langle\boldsymbol{w},\boldsymbol{w}_i\rangle$ *for each* i*. From the additive and scalar properties of the inner product, we have*

$$\langle\boldsymbol{w},\boldsymbol{w}_i\rangle=\left\langle\sum_{j=1}^{k}\frac{\langle\boldsymbol{u},\boldsymbol{w}_j\rangle}{\langle\boldsymbol{w}_j,\boldsymbol{w}_j\rangle}\boldsymbol{w}_j,\boldsymbol{w}_i\right\rangle=\sum_{j=1}^{k}\frac{\langle\boldsymbol{u},\boldsymbol{w}_j\rangle}{\langle\boldsymbol{w}_j,\boldsymbol{w}_j\rangle}\langle\boldsymbol{w}_j,\boldsymbol{w}_i\rangle. \tag{5.26}$$

On the right-hand side of (5.26), the only term that is non-zero is $\frac{\langle \boldsymbol{u}, \boldsymbol{w}_i\rangle}{\langle \boldsymbol{w}_i, \boldsymbol{w}_i\rangle}\langle \boldsymbol{w}_i, \boldsymbol{w}_i\rangle = \langle \boldsymbol{u}, \boldsymbol{w}_i\rangle$ *since for* $j \neq i, \langle \boldsymbol{w}_j, \boldsymbol{w}_i\rangle = 0$*. Thus,* $\langle \boldsymbol{w}, \boldsymbol{w}_i\rangle = \langle \boldsymbol{u}, \boldsymbol{w}_i\rangle$*. It now follows that*

$$\langle \boldsymbol{u} - \boldsymbol{w}, \boldsymbol{w}_i\rangle = \langle \boldsymbol{u}, \boldsymbol{w}_i\rangle - \langle \boldsymbol{u}, \boldsymbol{w}_i\rangle = 0$$

as desired.

You might recognize the expression $\frac{\boldsymbol{v}\cdot\boldsymbol{w}_i}{\boldsymbol{w}_i\cdot\boldsymbol{w}_i}\boldsymbol{w}_i$ as the projection of the vector $\boldsymbol{v}$ onto $\boldsymbol{w}_i$. We therefore have the following:

Theorem 5.15 *Let* $(\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_k)$ *be an orthogonal basis for the subspace* W *of* V *and* $\boldsymbol{u}$ *a vector in* V*. Then*

$$Proj_W(\boldsymbol{u}) = Proj_{\boldsymbol{w}_1}(\boldsymbol{u}) + Proj_{\boldsymbol{w}_2}(\boldsymbol{u}) + \cdots + Proj_{\boldsymbol{w}_k}(\boldsymbol{u}).$$

We complete this section with one more result in which we apply what we have obtained to solving the following general problem: Given a subspace W of an inner product space $(V, \langle\ ,\ \rangle)$ and a vector $\boldsymbol{u}$, determine the vector $\boldsymbol{w} \in W$ which has the least distance to $\boldsymbol{u}$. The following theorem is often called the Best Approximation Theorem.

Theorem 5.16 *Let* W *be a subspace of the inner product space* $(V, \langle\ ,\ \rangle)$ *and* $\boldsymbol{u}$ *a vector in* V*. Then for any vector* $\boldsymbol{w} \in W, \boldsymbol{w} \neq Proj_W(\boldsymbol{u})$*, we have*

$$\| \boldsymbol{u} - Proj_W(\boldsymbol{u}) \| \quad < \quad \| \boldsymbol{u} - \boldsymbol{w} \| .$$

Proof *Set* $\widehat{\boldsymbol{w}} = Proj_W(\boldsymbol{u})$*. Then the vector* $\boldsymbol{u} - \widehat{\boldsymbol{w}} \in W^{\perp}$ *and so orthogonal to every vector in W. In particular,* $\boldsymbol{u} - \widehat{\boldsymbol{w}}$ *is orthogonal to* $\widehat{\boldsymbol{w}} - \boldsymbol{w}$*.*

Now $\boldsymbol{u} - \boldsymbol{w} = (\boldsymbol{u} - \widehat{\boldsymbol{w}}) + (\widehat{\boldsymbol{w}} - \boldsymbol{w})$*. Since* $\boldsymbol{u} - \widehat{\boldsymbol{w}}$ *is orthogonal to* $\widehat{\boldsymbol{w}} - \boldsymbol{w}$ *we have*

$$\| \boldsymbol{u} - \boldsymbol{w} \|^2 = \| (\boldsymbol{u} - \widehat{\boldsymbol{w}}) + (\widehat{\boldsymbol{w}} - \boldsymbol{w}) \|^2 = \| \boldsymbol{u} - \widehat{\boldsymbol{w}} \|^2 + \| \widehat{\boldsymbol{w}} - \boldsymbol{w} \|^2 \qquad (5.27)$$

by Theorem (5.3). Since $\boldsymbol{w} \neq Proj_W(\boldsymbol{u}) = \widehat{\boldsymbol{w}}, \widehat{\boldsymbol{w}} - \boldsymbol{w} \neq 0$ *and consequently,* $\| \widehat{\boldsymbol{w}} - \boldsymbol{w} \| \neq 0$*. From (5.27) we conclude that*

$$\| \boldsymbol{u} - \boldsymbol{w} \|^2 \quad > \quad \| \boldsymbol{u} - \widehat{\boldsymbol{w}} \|^2 \qquad (5.28)$$

from which the result immediately follows by taking square roots.

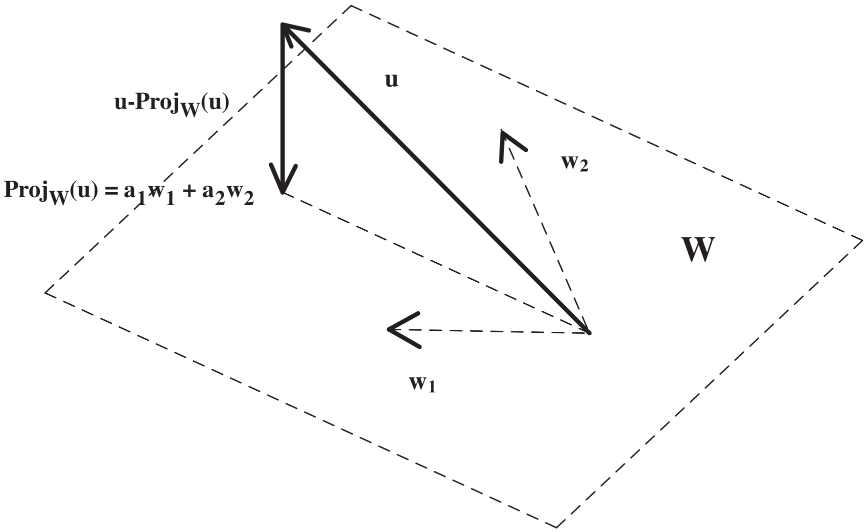

FIGURE 5.1
Projection of vector onto subspace.

In Figure (5.1) we illustrate Theorem (5.16).

Definition 5.15 *Let W be a subspace of the inner product space $(V, \langle\ ,\ \rangle)$ and let $\boldsymbol{u} \in V$. The* **distance of $\boldsymbol{u}$ to W** *is the minimum of $\{\parallel \boldsymbol{u} - \boldsymbol{w} \parallel : \boldsymbol{w} \in W\}$, that is, the shortest distance of the vector $\boldsymbol{u}$ to a vector in W. By Theorem (5.16), this is $\parallel \boldsymbol{u} - Proj_W(\boldsymbol{u}) \parallel$. We denote the distance of the vector $\boldsymbol{u}$ to the subspace W by $dist(\boldsymbol{u}, W)$.*

Exercises

1. Let $W = Span(\begin{pmatrix}1\\1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\0\\1\\0\end{pmatrix})$ and $\boldsymbol{u} = \begin{pmatrix}1\\2\\3\\4\end{pmatrix}$. Compute $Proj_W(\boldsymbol{u})$ and $Proj_{W^\perp}(\boldsymbol{u})$.

2. Let $V = M_{22}(\mathbb{R})$ with the inner product of Example (5.4) and let W be the subspace of trace zero matrices. Find $Proj_W(J_2)$ where J_2 is the all 1 matrix, $J_2 = \begin{pmatrix}1 & 1\\1 & 1\end{pmatrix}$.

3. Let $\mathbb{R}_{(3)}[x]$ be equipped with the inner product $\langle f, g\rangle = \int_0^1 f(t)g(t)dt$ and set $W = Span(1, x, x^2)$. Compute $Proj_W(x^3)$.

4. Find the distance of the point (2,3,4) from the plane $x + 2y - 2z = 5$.

5. Find the distance of the point $(1, -1, 1, -1)$ from the affine hyperplane $x_1 + 2x_2 + 3x_3 + x_4 = 7$.

6. Let L be the line $\{(t + 1, -2t, 3t - 2, -t + 1)|t \in \mathbb{R}\}$. Find the distance of the origin from L.

7. Using the inner product $\langle f, g\rangle = \int_0^1 f(t)g(t)dt$ on the space $C([0, 1])$, find the best approximation to the function $\sqrt{x}$ in the subspace $\mathbb{R}_{(2)}[x]$.

8. Let $(V, \langle\ ,\ \rangle)$ be an n-dimensional real inner product space and $\mathcal{S} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ an orthonormal basis of V. Let W be a subspace of V with an orthonormal basis $\mathcal{B} = (\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_k)$. Set $P = Proj_W$ and $A = ([\boldsymbol{w}_1]_{\mathcal{S}}\ [\boldsymbol{w}_2]_{\mathcal{S}}\ \ldots\ [\boldsymbol{w}_k]_{\mathcal{S}})$. Prove that the matrix of $Proj_W$ with respect to $\mathcal{S}$ is AA^{tr}.

9. Continuing with the hypothesis of Exercise 8, prove that $Q = \mathcal{M}_P(\mathcal{S}, \mathcal{S})$ satisfies $Q^2 = Q$ and $Q^{tr} = Q$.

10. Let $(V, \langle\ ,\ \rangle)$ be an n-dimensional real inner product space and let $\mathcal{S} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ be an orthonormal basis of V. Let Q be a matrix, which satisfies $Q^2 = Q$ and $Q^{tr} = Q$. Assume that $Q = \mathcal{M}_T(\mathcal{S}, \mathcal{S})$ and let $W = Range(T)$ and $U = Ker(T)$. Prove that $U = W^{\perp}$ and $T = Proj_W$.

11. Let W, U be subspaces of the inner product space $(V, \langle\ ,\ \rangle)$. Prove that

$$(Proj_U \circ Proj_W)(\boldsymbol{v}) = Proj_U(Proj_W(\boldsymbol{v})) = \mathbf{0}$$

for every vector $\boldsymbol{v} \in V$ if and only if $W \perp U$.

12. Let W be a subspace of the inner product space $(V, \langle\ ,\ \rangle)$ and $\boldsymbol{u}$ a vector in V. Prove that $\parallel Proj_W(\boldsymbol{u}) \parallel\ \leq\ \parallel \boldsymbol{u} \parallel$ with equality if and only if $\boldsymbol{u} \in W$.

13. Let W be a subspace of the inner product space $(V, \langle\ ,\ \rangle)$ and $\boldsymbol{u}$ a vector in V. Prove that $dist(\boldsymbol{u}, W)\ \leq\ \parallel \boldsymbol{u} \parallel$ with equality if and only if $\boldsymbol{u} \in W^{\perp}$.

5.5 Dual Spaces

What You Need to Know

To make sense of the material in this section you will need a fundamental understanding of the following concepts: finite-dimensional vector space V, basis of a finite-dimensional vector space, linear transformation from a finite-dimensional vector space V to a finite-dimensional vector space W, and the matrix of a linear transformation T from a space V to a space W with respect to bases $\mathcal{B}_V$ of V and $\mathcal{B}_W$ of W.

We begin with a definition:

Definition 5.16 *Let V be a finite-dimensional vector space over a field $\mathbb{F}$. The* **dual space** *of V, denoted by V', is $\mathcal{L}(V, \mathbb{F})$, that is, the vector space of all linear transformations from V to $\mathbb{F}$, the latter regarded as a vector space of dimension one. Elements of V' are called* **linear functionals**.

Lemma 5.4 *Let V be a vector space over $\mathbb{F}$ with basis $\mathcal{B} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$. Then there exists linear functionals $f_1, f_2, \ldots, f_n$ such that*

$$f_j(\boldsymbol{v}_j) = 1, f_j(\boldsymbol{v}_i) = 0, i \neq j. \tag{5.29}$$

Moreover, $\mathcal{B}' = (f_1, f_2, \ldots, f_n)$ is a basis for V'.

Proof *The existence of the function f_i is immediate since for any function $f : \mathcal{B} \to \mathbb{F}$ there exists a unique extension of f to a linear transformation on V by Theorem (2.6).*

To see that $\mathcal{B}'$ is linearly independent, suppose $f = c_1 f_1 + \ldots c_n f_n = 0_{V \to \mathbb{F}}$. Then $f(\boldsymbol{u}) = 0$ for all $\boldsymbol{u} \in V$. In particular, $f(\boldsymbol{v}_j) = c_j = 0$.

To see that $\mathcal{B}'$ spans V', let $f \in V'$. Set $c_j = f(\boldsymbol{v}_j)$ and $g = c_1 f_1 + \ldots c_n f_n$. Since f and g are both linear functionals it suffices to prove that $f(\boldsymbol{v}_j) = g(\boldsymbol{v}_j)$ for all $j = 1, 2, \ldots, n$. We know that $f(\boldsymbol{v}_j) = c_j$. On the other hand, $g(\boldsymbol{v}_j) = \sum_{i=1}^{n} c_i f_i(\boldsymbol{v}_j) = c_j f_j(v_j) = c_j$.

Definition 5.17 *Let V be a vector space with basis $\mathcal{B} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$. The basis $\mathcal{B}' = (f_1, f_2, \ldots, f_n)$ of V' such that Equation (5.29) holds is called the* **basis of V' dual to** $\mathcal{B}$ *or simply the* **dual basis** *to $\mathcal{B}$.*

In the next result, we show how a linear transformation T from a finite-dimensional vector space V to a finite-dimensional vector space W induces a linear transformation T' from W' to V'.

Theorem 5.17 *Let V, W be finite-dimensional vector spaces over the field $\mathbb{F}$ and $T : V \rightarrow W$ be a linear transformation. Define $T' : W' \rightarrow V'$ by $T'(g) = g \circ T$. Then $T' \in \mathcal{L}(W', V')$.*

Proof *First, we must verify that $T'(g) \in V'$. However, this is immediate: Since g and T are linear it follows that the composition $g \circ T$ is linear.*

We also need to show that T' is linear. Suppose $g_1, g_2 \in W'$ and $\boldsymbol{v} \in V$. Then

$$\begin{aligned} T'(g_1 + g_2)(\boldsymbol{v}) &= [(g_1 + g_2) \circ T](\boldsymbol{v}) \\ &= (g_1 + g_2)(T(\boldsymbol{v})) \\ &= g_1(T(\boldsymbol{v})) + g_2(T(\boldsymbol{v})) \\ &= T'(g_1)(\boldsymbol{v}) + T'(g_2)(\boldsymbol{v}) \\ &= [T'(g_1) + T'(g_2)](\boldsymbol{v}). \end{aligned}$$

Thus, $T'(g_1 + g_2) = T'(g_1) + T'(g_2)$.

Now suppose $g \in W', \alpha \in \mathbb{F}$. Then

$$\begin{aligned} T'(\alpha g)(\boldsymbol{v}) &= [(\alpha g) \circ T](\boldsymbol{v}) \\ &= (\alpha g)(T(\boldsymbol{v})) \\ &= \alpha(g(T)(\boldsymbol{v}) \\ &= \alpha(T'(g)(\boldsymbol{v})). \end{aligned}$$

Therefore, $T'(\alpha g) = \alpha T'(g)$.

Definition 5.18 *Let V and W be finite-dimensional vector spaces and $T \in \mathcal{L}(V, W)$. Then the map $T' \in \mathcal{L}(W', V')$ is called the* **transpose** *of T.*

The next theorem relates the transpose of a linear transformation to the transpose of a matrix.

Theorem 5.18 *Let V be a vector space with basis $\mathcal{B}_V = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$, W be a vector space with basis $\mathcal{B}_W = (\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_m)$, and $T \in \mathcal{L}(V, W)$. Let $\mathcal{B}_{V'} = (f_1, f_2, \ldots, f_n)$ be the basis dual to $\mathcal{B}_V$ and $\mathcal{B}_{W'} = (g_1, g_2, \ldots, g_m)$ be the basis dual to $\mathcal{B}_W$. Then $\mathcal{M}_{T'}(\mathcal{B}_{W'}, \mathcal{B}_{V'}) = \mathcal{M}_T(\mathcal{B}_V, \mathcal{B}_W)^{tr}$.*

Proof *Assume that*

$$[T(\boldsymbol{v}_j)]_{\mathcal{B}_W} = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix} \tag{5.30}$$

and

$$[T'(g_i)]_{\mathcal{B}_{V'}} = \begin{pmatrix} b_{1i} \\ b_{2i} \\ \vdots \\ b_{ni} \end{pmatrix}. \tag{5.31}$$

We need to show that $b_{ji} = a_{ij}$. Recall, Equation (5.30) means that

$$T(\boldsymbol{v}_j) = \sum_{k=1}^{m} a_{kj}\boldsymbol{w}_k \tag{5.32}$$

and Equation (5.31) is equivalent to

$$T'(g_i) = \sum_{l=1}^{n} b_{li} f_l. \tag{5.33}$$

Let us apply $T'(g_i)$ to the vector $\boldsymbol{v}_j$. On the one hand,

$$T'(g_i)(\boldsymbol{v}_j) = (g_i \circ T)(\boldsymbol{v}_j) = g_i(T(\boldsymbol{v}_j)) = g_i\left(\sum_{k=1}^{m} a_{kj}\boldsymbol{w}_k\right) = a_{ij}. \tag{5.34}$$

In Equation (5.34) we have used the fact that $g_i(\boldsymbol{w}_i) = 1$ and $g_i(\boldsymbol{w}_k) = 0$ for $k \neq i$. On the other hand,

$$[T'(g_i])(\boldsymbol{v}_j) = \left(\sum_{l=1}^{n} b_{li} f_l)\right)(\boldsymbol{v}_j) = \sum_{l=1}^{n} b_{li} f_l(\boldsymbol{v}_j) = b_{ji}. \tag{5.35}$$

In Equation (5.35) we have used the fact that $f_j(\boldsymbol{v}_j) = 1, f_l(\boldsymbol{v}_j) = 0$ if $l \neq j$.

We have therefore shown that $a_{ij} = b_{ji}$ as required.

Exercises

1. Let $\mathcal{S}' = (f_1, f_2, f_3, f_4)$ be the basis of $(\mathbb{R}^4)'$ that is dual to the standard

basis $\mathcal{S}$ of $\mathbb{R}^4$. Verify that $\mathcal{B} = \left(\begin{pmatrix} 1 \\ 2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \\ 1 \\ 1 \end{pmatrix} \right)$ is a basis for $\mathbb{R}^4$ and find the basis of $(\mathbb{R}^4)'$ dual to $\mathcal{B}$ (expressed as a linear combination of $\mathcal{S}'$).

2. Let V, W be finite-dimensional vector spaces. Show that the transpose map $T \to T'$ from $\mathcal{L}(V, W)$ to $\mathcal{L}(W', V')$ is a vector space isomorphism.

3. Assume V and W are finite-dimensional vector spaces and let $T \to T'$ be the transpose map from $\mathcal{L}(V, W)$ to $\mathcal{L}(W', V')$. Prove that T is one-to-one if and only if T' is onto and T is onto if and only if T' is one-to-one.

4. Assume V and W are finite-dimensional vector spaces and let $T \to T'$ be the transpose map from $\mathcal{L}(V, W)$ to $\mathcal{L}(W', V')$. Prove that T is an isomorphism if and only if T' is an isomorphism.

5. Assume V and W are finite-dimensional vector spaces and let $T \to T'$ be the transpose map from $\mathcal{L}(V, W)$ to $\mathcal{L}(W', V')$. Prove that $rank(T) = rank(T')$.

6. Assume V and W are finite-dimensional vector spaces and let $T \to T'$ be the transpose map from $\mathcal{L}(V, W)$ to $\mathcal{L}(W', V')$. Prove $nullity(T) = nullity(T')$ if and only if $dim(V) = dim(W)$.

7. Let V be an n-dimensional vector space and assume $(f_1, \ldots, f_n)$ is a basis of V'. Prove that the map $T : V \to \mathbb{F}^n$ given by $T(\boldsymbol{v}) = \begin{pmatrix} f_1(\boldsymbol{v}) \\ \vdots \\ f_n(\boldsymbol{v}) \end{pmatrix}$ is an isomorphism.

8. Let $(\pi_1, \ldots, \pi_n)$ be the basis in $(\mathbb{F}^n)'$ dual to the standard basis $\mathcal{S}$. Let $T \in \mathcal{L}(V, \mathbb{F}^n)$ and set $f_i = \pi_i \circ T$. Assume T is an isomorphism. Prove that $(f_1, \ldots, f_n)$ is basis of V'.

9. Let V be an n-dimensional vector space and assume $(f_1, \ldots, f_n)$ is a basis of V'. Prove that there exists $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \in V$ such that $f_j(\boldsymbol{x}_j) = 1$ for $j = 1, 2, \ldots, n$ and $f_j(\boldsymbol{x}_i) = 0$ if $j \neq i$.

10. Let V be a finite-dimensional vector space and U a subspace of V. Set $U' = \{f \in V' | U \subset Ker(f)\}$. Prove that U' is a subspace of V' and that

$$dim(U) + dim(U') = dim(V).$$

11. Let V be an n-dimensional vector space and U, W subspaces of V. Prove that $(U + W)' = U' \cap W', (U \cap W)' = U' + W'$.

12. Assume $V = U \oplus W$ (an external direct sum). Define $\gamma : U' \oplus W' \to (U \oplus W)'$ by $\gamma(f, g)(\boldsymbol{u} + \boldsymbol{w}) = f(\boldsymbol{u}) + g(\boldsymbol{w})$. Prove that γ is an isomorphism.

13. Let V, W, X be finite-dimensional vector spaces over a field $\mathbb{F}$. Assume $T \in \mathcal{L}(V, W)$ and $S \in \mathcal{L}(W, X)$. Prove that $(S \circ T)' = T' \circ S'$.

14. Let V be a finite-dimensional vector space, $T \in \mathcal{L}(V, V)$ and assume that U is a T-invariant subspace of V. Prove that U' is T'-invariant.

15. Let V be a finite-dimensional vector space, $T \in \mathcal{L}(V, V)$. Prove that $\mu_T(x) = \mu_{T'}(x)$.

16. Let V, W be finite-dimensional vector spaces over a field $\mathbb{F}$ and $T \in \mathcal{L}(V, W)$. Prove the following:

i. $Ker(T') = Range(T)'$.

ii. $Range(T') = Ker(T)'$.

iii. $Ker(T) = Range(T')'$.

iv. $Range(T) = Ker(T')'$.

5.6 Adjoints

What You Need to Know

To make sense of the present material, it is essential that you have mastered the following concepts: finite-dimensional inner product space, linear transformation from a vector space V to a vector space W, kernel and range of a linear transformation, dual space of a vector space V, matrix of a linear transformation from a finite-dimensional vector space to a finite-dimensional vector W, dual basis to a basis in a vector space V, and transpose of a linear transformation T from a vector space V to a vector space W.

In our first result we show that in an inner product space $(V, \langle\ ,\ \rangle)$ over $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$ there is a natural correspondence between vectors in the dual space V' and the vectors in V. We will make use of this in defining the adjoint of an operator.

Theorem 5.19 *Let $(V, \langle\ ,\ \rangle)$ be a finite-dimensional inner product space and assume that $f \in V'$. Then there exists a unique vector $\boldsymbol{v} \in V$ such that $f(\boldsymbol{u}) = \langle \boldsymbol{u}, \boldsymbol{v} \rangle$ for all $\boldsymbol{u} \in V$.*

Proof *Let $\mathcal{S} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ be an orthonormal basis for V and assume that $f(\boldsymbol{v}_i) = a_i, i = 1, 2, \dots, n$. Set $\boldsymbol{v} = \overline{a_1}\boldsymbol{v}_1 + \overline{a_2}\boldsymbol{v}_2 + \dots \overline{a_n}\boldsymbol{v}_n$. We claim that $f(\boldsymbol{u}) = \langle \boldsymbol{u}, \boldsymbol{v} \rangle$ for all vectors $\boldsymbol{u} \in V$. Suppose $\boldsymbol{u} = b_1\boldsymbol{v}_1 + b_2\boldsymbol{v}_2 + \dots + b_n\boldsymbol{v}_n \in V$. Then*

$$\begin{aligned} f(\boldsymbol{u}) &= f(b_1\boldsymbol{v}_1 + b_2\boldsymbol{v}_2 + \dots + b_n\boldsymbol{v}_n) \\ &= b_1 f(\boldsymbol{v}_1) + b_2 f(\boldsymbol{v}_2) + \dots b_n f(\boldsymbol{v}_n) \\ &= b_1 a_1 + b_2 a_2 + \dots b_n a_n. \end{aligned}$$

On the other hand,

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle = \langle b_1\boldsymbol{v}_1 + b_2\boldsymbol{v}_2 + \dots + b_n\boldsymbol{v}_n, \overline{a_1}\boldsymbol{v}_1 + \overline{a_2}\boldsymbol{v}_2 + \dots \overline{a_n}\boldsymbol{v}_n \rangle$$

$$= \sum_{i=1}^{n}\sum_{j=1}^{n} \langle b_i\boldsymbol{v}_i, \overline{a_j}\boldsymbol{v}_j \rangle = \sum_{i=1}^{n}\sum_{j=1}^{n} b_i \overline{\overline{a_j}} \langle \boldsymbol{v}_i, \boldsymbol{v}_j \rangle \tag{5.36}$$

$$= b_1 a_1 + b_2 a_2 + \dots b_n a_n. \tag{5.37}$$

In Equation (5.36) we have used the additivity in each argument of $\langle\ ,\ \rangle$, homogeneity in the first argument, as well as conjugate homogeneity in the second *argument. In Equation (5.37) we have used the fact that $\mathcal{S}$ is a orthonormal basis. This proves the existence of $\boldsymbol{v}$.*

Suppose that $f(\boldsymbol{u}) = \langle \boldsymbol{u}, \boldsymbol{x}\rangle$ for all $\boldsymbol{u} \in V$. Then $\langle \boldsymbol{u}, \boldsymbol{v} - \boldsymbol{x}\rangle = 0$ for all $\boldsymbol{u} \in V$. In particular, $\langle \boldsymbol{v} - \boldsymbol{x}, \boldsymbol{v} - \boldsymbol{x}\rangle = 0$ so by positive definiteness, $\boldsymbol{v} - \boldsymbol{x} = \mathbf{0}$, and this proves that $\boldsymbol{v}$ is unique.

Remark 5.4 *Let $(V, \langle\ ,\ \rangle)$ be a finite-dimensional inner product space. For $f \in V'$ let f' denote the vector $\boldsymbol{v}$ in V such that $f(\boldsymbol{u}) = \langle \boldsymbol{u}, \boldsymbol{v}\rangle$. The bijection $f \to f'$ from V' to V is always additive. If the base field is the reals, then the map $f \to f'$ is linear. However, if the base field is the complex numbers, then it is not linear but rather satisfies $(\gamma f)' = \overline{\gamma} f'$.*

Suppose now that V, W are finite inner product spaces and $T \in \mathcal{L}(V, W)$. We make use of the bijection $\prime : V' \to V$ to obtain a map $T^* \in \mathcal{L}(W, V)$ as follows:

Let $\boldsymbol{w} \in W, \boldsymbol{v} \in V$. Define $f(\boldsymbol{v}) = \langle T(\boldsymbol{v}), \boldsymbol{w}\rangle_W$. We claim that $f \in V'$. To validate this claim, we need to show 1)$f(\boldsymbol{v}_1 + \boldsymbol{v}_2) = f(\boldsymbol{v}_1) + f(\boldsymbol{v}_2)$ and 2) $f(c\boldsymbol{v}) = cf(\boldsymbol{v})$.

1) Since T is linear $f(\boldsymbol{v}_1 + \boldsymbol{v}_2) = \langle T(\boldsymbol{v}_1 + \boldsymbol{v}_2), \boldsymbol{w}\rangle_W = \langle T(\boldsymbol{v}_1) + T(\boldsymbol{v}_2), \boldsymbol{w}\rangle_W$. By the additivity of $\langle\ ,\ \rangle_W$ in the first variable, we have

$$\langle T(\boldsymbol{v}_1) + T(\boldsymbol{v}_2), \boldsymbol{w}\rangle_W = \langle T(\boldsymbol{v}_1), \boldsymbol{w}\rangle_W + \langle T(\boldsymbol{v}_2), \boldsymbol{w}\rangle_W = f(\boldsymbol{v}_1) + f(\boldsymbol{v}_2).$$

2) This holds by the linearity of T and the homogeneity of $\langle\ ,\ \rangle_W$ in the first variable.

Since $f \in V'$ there is a vector $f' \in V$ such that $f(\boldsymbol{v}) = \langle T(\boldsymbol{v}), \boldsymbol{w}\rangle_W = \langle \boldsymbol{v}, f'\rangle_V$. We will denote the vector f' by $T^*(\boldsymbol{w})$. In this way, we have obtained a function $T^* : W \to V$ such that for all $\boldsymbol{v} \in V$ and $\boldsymbol{w} \in W$

$$\langle T(\boldsymbol{v}), \boldsymbol{w}\rangle_W = \langle \boldsymbol{v}, T^*(\boldsymbol{w})\rangle_V. \tag{5.38}$$

We claim that $T^* : W \to V$ is a linear map. We show that it is additive: Let $\boldsymbol{w}_1, \boldsymbol{w}_2 \in W$ and let $\boldsymbol{v} \in V$. Then $\langle \boldsymbol{v}, T^*(\boldsymbol{w}_1 + \boldsymbol{w}_2)\rangle_V = \langle T(\boldsymbol{v}), \boldsymbol{w}_1 + \boldsymbol{w}_2\rangle_W$ by Equation (5.38). Since $\langle\ ,\ \rangle_W$ is additive in the second variable we have

$$\begin{aligned}\langle T(\boldsymbol{v}), \boldsymbol{w}_1 + \boldsymbol{w}_2\rangle_W &= \langle T(\boldsymbol{v}), \boldsymbol{w}_1\rangle_W + \langle T(\boldsymbol{v}), \boldsymbol{w}_2\rangle_W \\ &= \langle \boldsymbol{v}, T^*(\boldsymbol{w}_1)\rangle_V + \langle \boldsymbol{v}, T^*(\boldsymbol{w}_2)\rangle_V \\ &= \langle \boldsymbol{v}, T^*(\boldsymbol{w}_1) + T^*(\boldsymbol{w}_2)\rangle_V.\end{aligned}$$

It then follows that $\langle \boldsymbol{v}, T^*(\boldsymbol{w}_1 + \boldsymbol{w}_2) - T^*(\boldsymbol{w}_1) - T^*(\boldsymbol{w}_2)\rangle_V = 0$ for every $\boldsymbol{v} \in V$. In particular, this holds for $\boldsymbol{v} = T^*(\boldsymbol{w}_1 + \boldsymbol{w}_2) - T^*(\boldsymbol{w}_1) - T^*(\boldsymbol{w}_2)$. It then follows by positive definiteness that $T^*(\boldsymbol{w}_1+\boldsymbol{w}_2)-T^*(\boldsymbol{w}_1)-T^*(\boldsymbol{w}_2)=0$ as required.

Now let $\boldsymbol{w}\in W, c\in\mathbb{F}$ and $\boldsymbol{v}\in V$. Then

$$\begin{aligned}\langle \boldsymbol{v}, T^*(c\boldsymbol{w})\rangle_V &= \langle T(\boldsymbol{v}), c\boldsymbol{w}\rangle_W\\ &= \overline{c}\langle T(\boldsymbol{v}), \boldsymbol{w}\rangle_W\\ &= \overline{c}\langle \boldsymbol{v}, T^*(\boldsymbol{w})\rangle_V\\ &= \langle \boldsymbol{v}, cT^*(\boldsymbol{w})\rangle_V.\end{aligned}$$

We can now conclude that for every $\boldsymbol{v}\in V$,

$$0=\langle \boldsymbol{v}, T^*(c\boldsymbol{w})\rangle_V-\langle \boldsymbol{v}, cT^*(\boldsymbol{w})\rangle_V=\langle \boldsymbol{v}, T^*(c\boldsymbol{w})-cT^*(\boldsymbol{w})\rangle_V.$$

In particular, this is true for $\boldsymbol{v}=T^*(c\boldsymbol{w})-cT^*(\boldsymbol{w})$ and then by positive definiteness, $T^*(c\boldsymbol{w})=cT^*(\boldsymbol{w})$ as we needed to show.

Definition 5.19 *Let $(V,\langle\ ,\ \rangle_V)$ and $(W,\langle\ ,\ \rangle_W)$ be finite-dimensional inner product spaces and $T\in\mathcal{L}(V,W)$. The map $T^*\in\mathcal{L}(W,V)$ is called the* **adjoint** *of T. It is the* **unique** *linear map from W to V satisfying Equation (5.38).*

We will refer to Equation (5.38) as the *fundamental equation* defining the adjoint.

Remark 5.5 *We have several times above shown the following: Assume $(V,\langle\ ,\ \rangle)$ is an inner product space, $\boldsymbol{u},\boldsymbol{v}$ are vectors in V, and $\langle\boldsymbol{u},\boldsymbol{x}\rangle=\langle\boldsymbol{v},\boldsymbol{x}\rangle$ for every vector $\boldsymbol{x}\in V$. Then $\boldsymbol{u}=\boldsymbol{v}$. We will hereafter just invoke this rather than repeat the argument.*

The following result enumerates some properties of the map $T\to T^*$ from $\mathcal{L}(V,W)$ to $\mathcal{L}(W,V)$.

Theorem 5.20 *Let $(V,\langle\ ,\ \rangle_V),(W,\langle\ ,\ \rangle_W),(X,\langle\ ,\ \rangle_X)$ be finite-dimensional inner product spaces over the field $\mathbb{F}\in\{\mathbb{R},\mathbb{C}\}$. Then the following hold:*

i) If $S,T\in\mathcal{L}(V,W)$ then $(S+T)^*=S^*+T^*$;

ii) If $T\in\mathcal{L}(V,W)$ and $\gamma\in\mathbb{F}$ then $(\gamma T)^*=\overline{\gamma}T^*.$;

iii) If $S\in\mathcal{L}(V,W)$ and $T\in\mathcal{L}(W,X)$ then $(TS)^*=S^*T^*$;

iv) If $T\in\mathcal{L}(V,W)$ then $(T^*)^*=T$; and

v) $I_V^*=I_V$.

Proof *i) Let $\boldsymbol{v} \in V, \boldsymbol{w} \in W$. Then*

$$\begin{array}{rcl}\langle \boldsymbol{v}, (S+T)^*(\boldsymbol{w})\rangle_V & = & \langle (S+T)(\boldsymbol{v}), \boldsymbol{w}\rangle_W \\ & = & \langle S(\boldsymbol{v}) + T(\boldsymbol{v}), \boldsymbol{w}\rangle_W \\ & = & \langle S(\boldsymbol{v}), \boldsymbol{w}\rangle_W + \langle T(\boldsymbol{v}), \boldsymbol{w}\rangle_W \\ & = & \langle \boldsymbol{v}, S^*(\boldsymbol{w})\rangle_V + \langle \boldsymbol{v}, T^*(\boldsymbol{w})\rangle_V \\ & = & \langle \boldsymbol{v}, S^*(\boldsymbol{w}) + T^*(\boldsymbol{w})\rangle_V \\ & = & \langle \boldsymbol{v}, (S^* + T^*)(\boldsymbol{w})\rangle_V.\end{array}$$

Consequently, $(S+T)^*(\boldsymbol{w}) = S^*(\boldsymbol{w}) + T^*(\boldsymbol{w})$ for all $\boldsymbol{w} \in W$, and therefore, $(S+T)^* = S^* + T^*$.

ii) Let $\boldsymbol{v} \in V, \boldsymbol{w} \in W$ and γ a scalar. Then

$$\begin{array}{rcl}\langle \boldsymbol{v}, (\gamma T)^*(\boldsymbol{w})\rangle_V & = & \langle (\gamma T)(\boldsymbol{v}), \boldsymbol{w}\rangle_W \\ & = & \langle \gamma T(\boldsymbol{v}), \boldsymbol{w}\rangle_W \\ & = & \gamma\langle (T(\boldsymbol{v}), \boldsymbol{w}\rangle_W \\ & = & \gamma\langle \boldsymbol{v}, T^*(\boldsymbol{w})\rangle_V \\ & = & \langle \boldsymbol{v}, \overline{\gamma}T^*(\boldsymbol{w})\rangle_V.\end{array}$$

We can therefore conclude that $(\gamma T)^* = \overline{\gamma}T^*$.

iii) Let $\boldsymbol{v} \in V, \boldsymbol{x} \in X$. Then $ST(\boldsymbol{v}) \in X$ and by the fundamental equation defining $(ST)^*$ we have

$$\begin{array}{rcl}\langle \boldsymbol{v}, (ST)^*(\boldsymbol{x})\rangle_V & = & \langle (ST)(\boldsymbol{v}), \boldsymbol{x}\rangle_X \\ & = & \langle S(T(\boldsymbol{v})), \boldsymbol{x}\rangle_X.\end{array}$$

Since $T(\boldsymbol{v}) \in W$, by the fundamental equation defining S^* we have

$$\langle S(T(\boldsymbol{v})), \boldsymbol{x}\rangle_X = \langle T(\boldsymbol{v}), S^*(\boldsymbol{x})\rangle_W.$$

In turn, since $\boldsymbol{v} \in V$ and $S^*(\boldsymbol{x}) \in W$, we have by the fundamental equation applied to T

$$\begin{array}{rcl}\langle T(\boldsymbol{v}), S^*(\boldsymbol{x})\rangle_W & = & \langle \boldsymbol{v}, T^*(S^*(\boldsymbol{x}))\rangle_V \\ & = & \langle \boldsymbol{v}, (T^*S^*)(\boldsymbol{x})\rangle_V.\end{array}$$

It then follows for all vectors $\boldsymbol{x} \in X$ that $(ST)^*(\boldsymbol{x}) = T^*S^*(\boldsymbol{x})$ as required.

The last two parts are straightforward, and we leave them as exercises.

We next uncover the relationship between the range and kernel of $T \in \mathcal{L}(V, W)$ and the adjoint $T^* \in \mathcal{L}(W, V)$.

Theorem 5.21 *Let $(V, \langle\ ,\ \rangle_V), (W, \langle\ ,\ \rangle_W)$ be finite-dimensional inner product spaces and $T \in \mathcal{L}(V, W)$. Then*

i. $Ker(T^*) = Range(T)^\perp$;

ii. $Range(T^*) = Ker(T)^\perp$;

iii. $Ker(T) = Range(T^*)^\perp$; and

iv. $Range(T) = Ker(T^*)^\perp$.

Proof *i) Suppose $\boldsymbol{w} \in Ker(T^*)$. Then $\langle \boldsymbol{v}, T^*(\boldsymbol{w})\rangle_V = \langle \boldsymbol{v}, \boldsymbol{0}_V\rangle_V = 0$ for all $\boldsymbol{v} \in V$. By the definition of $T^*, \langle \boldsymbol{v}, T^*(\boldsymbol{w})\rangle_V = \langle T(\boldsymbol{v}), \boldsymbol{w}\rangle_W$. This implies that $\boldsymbol{w} \perp T(\boldsymbol{v})$ for all $\boldsymbol{v} \in V$ and hence $\boldsymbol{w} \in Range(T)^\perp$. Thus, $Ker(T^*) \subset Range(T)^\perp$.*

Let $\boldsymbol{w} \in Range(T)^\perp$. Then for all $\boldsymbol{v} \in V, \langle T(\boldsymbol{v}), \boldsymbol{w}\rangle_W = 0$. But then by the definition of $T^*, \langle \boldsymbol{v}, T^*(\boldsymbol{w})\rangle_V = 0$. In particular, $\langle T^*(\boldsymbol{w}), T^*(\boldsymbol{w})\rangle_V = 0$ so by positive definiteness, $T^*(\boldsymbol{w}) = 0_V$ and $\boldsymbol{w} \in Ker(T^*)$.

Since $(T^*)^* = T$ it follows that iii) holds as a consequence of i). From i) we also deduce that $Ker(T^*)^\perp = [Range(T)^\perp]^\perp = Range(T)$ and consequently iv) holds. Finally, since $Ker(T) = Range(T^*)^\perp$, we have $Ker(T)^\perp = [Range(T^*)^\perp]^\perp = Range(T^*)$ so that also ii) holds.

We come to our final theorem, which relates the matrix of T and T^* when they are computed with respect to orthonormal bases of V and W.

Theorem 5.22 *Let $(V, \langle\ ,\ \rangle_V)$ and $(W, \langle\ ,\ \rangle_W)$ be inner product spaces with orthonormal bases $\mathcal{B}_V = (\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n)$ and $\mathcal{B}_W = (\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_m)$ for V and W, respectively. Let $A = \mathcal{M}_T(\mathcal{B}_V, \mathcal{B}_W)$ and $B = \mathcal{M}_{T^*}(\mathcal{B}_W, \mathcal{B}_V)$. Then $B = \overline{A}^{tr}$.*

Proof *Set $[T(\boldsymbol{v}_j)]_{\mathcal{B}_W} = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$ and $[T^*(\boldsymbol{w}_i)]_{\mathcal{B}_V} = \begin{pmatrix} b_{1i} \\ b_{2i} \\ \vdots \\ b_{ni} \end{pmatrix}$. We can interpret the former to mean that*

$$T(\boldsymbol{v}_j) = a_{1j}\boldsymbol{w}_1 + a_{2j}\boldsymbol{w}_2 + \cdots + a_{mj}\boldsymbol{w}_m. \tag{5.39}$$

On the other hand, as a consequence of the latter, we can conclude that

$$T^*(\boldsymbol{w}_i) = b_{1i}\boldsymbol{v}_1 + b_{2i}\boldsymbol{v}_2 + \cdots + b_{ni}\boldsymbol{v}_n. \tag{5.40}$$

We need to prove that $b_{ji} = \overline{a_{ij}}$ *or equivalently, that* $a_{ij} = \overline{b_{ji}}$. *We do so by computing each of* $\langle T(\boldsymbol{v}_j), \boldsymbol{w}_i\rangle_W = \langle \boldsymbol{v}_j, T^*(\boldsymbol{w}_i)\rangle_V$ *making use of Equations (5.39) and (5.40).*

On the one hand,

$$\begin{aligned}\langle T(\boldsymbol{v}_j), \boldsymbol{w}_i\rangle_W &= \left\langle \sum_{k=1}^m a_{kj}\boldsymbol{w}_k, \boldsymbol{w}_i \right\rangle_W \\ &= \sum_{k=1}^m a_{kj}\langle \boldsymbol{w}_k, \boldsymbol{w}_i\rangle_W = a_{ij},\end{aligned}$$

the latter equality since $\mathcal{B}_W$ *is an orthonormal basis of W. On the other hand,*

$$\begin{aligned}\langle \boldsymbol{v}_j, T^*(\boldsymbol{w}_i)\rangle_V &= \left\langle \boldsymbol{v}_j, \sum_{l=1}^n b_{li}\boldsymbol{v}_l \right\rangle_V \\ &= \sum_{l=1}^m \overline{b_{li}}\langle \boldsymbol{v}_j, \boldsymbol{v}_l\rangle_V = \overline{b_{ji}}.\end{aligned}$$

Thus, $a_{ij} = \overline{b_{ji}}$ *as required.*

Exercises

1. Let $\mathbb{R}^3$ be equipped with the usual inner product (dot product). Let $f : \mathbb{R}^3 \to \mathbb{R}$ be the linear form $f\begin{pmatrix} x \\ y \\ z \end{pmatrix} = 2x + 3y - z$. Find a vector $\boldsymbol{v} \in \mathbb{R}^3$ such that $f(\boldsymbol{u}) = \boldsymbol{u} \cdot \boldsymbol{v}$.

2. Let $\mathbb{R}_{(2)}[x]$ be equipped with the inner product $\langle f, g\rangle = \int_0^1 f(t)g(t)dt$. Let $\gamma : \mathbb{R}_{(2)}[x] \to \mathbb{R}$ be given by $\gamma(f) = -f(1) - f(2)$. Find a vector $p(x) \in \mathbb{R}_{(2)}[x]$ such that $\gamma(f) = \langle f(x), p(x)\rangle$.

3. Let $V = M_{22}(\mathbb{C})$ equipped with the inner product of Example (5.4). Let $\pi : M_{22} \to \mathbb{C}$ be the map:

$$\pi\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11} - a_{22}.$$

Find a vector $A \in M_{22}(\mathbb{C})$ such that $\pi(B) = \langle B, A\rangle = Trace(B^{tr}\overline{A})$.

4. Prove part iii) of Theorem (5.20).

5. Prove part iv) of Theorem (5.20).

6. Let $T \in \mathcal{L}(V, V)$ and $\lambda \in \mathbb{F}$. Prove that λ is an eigenvalue of T if and only if $\overline{\lambda}$ is an eigenvalue of T^*.

7. Assume $T : V \to W$ is an invertible linear transformation where V, W are finite-dimensional inner product spaces. Prove that $T^* : W \to V$ is invertible and $(T^*)^{-1} = (T^{-1})^*$.

8. Assume $(V, \langle\ ,\ \rangle_V)$ and $(W, \langle\ ,\ \rangle_W)$ are finite-dimensional inner product spaces and $T : V \to W$ is an injective linear transformation. Prove that $T^*T : V \to V$ is bijective.

9. Assume $(V, \langle\ ,\ \rangle_V)$ and $(W, \langle\ ,\ \rangle_W)$ are finite-dimensional inner product spaces and $T : V \to W$ is a surjective linear transformation. Prove that $TT^* : W \to W$ is bijective.

10. Assume $(V, \langle\ ,\ \rangle)$ is an inner product space, $T \in \mathcal{L}(V, V)$, and U is a subspace of V. Prove that U is T-invariant if and only if $U^\perp$ is T^*-invariant.

11. Let $(V, \langle\ ,\ \rangle)$ be an inner product space and $T \in \mathcal{L}(V, V)$. Assume $\boldsymbol{v} \in Ker(T^*T)$. Prove that $T(\boldsymbol{v}) = \mathbf{0}$.

12. Let $(V, \langle\ ,\ \rangle)$ be a finite-dimensional inner product space. Make $V \oplus V$ into an inner product space by defining $\langle(\boldsymbol{x}_1, \boldsymbol{y}_1), (\boldsymbol{x}_2, \boldsymbol{y}_2)\rangle = \langle \boldsymbol{x}_1, \boldsymbol{x}_2\rangle + \langle \boldsymbol{y}_1, \boldsymbol{y}_2\rangle$. Let $S : V \oplus V \to V \oplus V$ be defined by $S(\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{y}, -\boldsymbol{x})$. Compute S^*.

13. Let $(V, \langle\ ,\ \rangle_V)$ and $(W, \langle\ ,\ \rangle_V)$ be finite-dimensional inner product spaces and $T \in \mathcal{L}(V, W)$. Prove that $rank(T) = rank(T^*)$.

14. Let $(V, \langle\ ,\ \rangle)$ be a finite-dimensional complex inner product space with an orthonormal basis $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$. Prove that there exists a nonsingular operator $S : V \to V$ such that $S(\boldsymbol{v}_1) = \boldsymbol{x}, S^*(\boldsymbol{y}) = \boldsymbol{v}_1$ if and only if $\langle \boldsymbol{x}, \boldsymbol{y}\rangle = 1$.

5.7 Normed Vector Spaces

In this section we generalize from the notion of a norm in an inner product space to an abstract norm on a vector space which can be thought of as assigning a length or magnitude to each vector. We will give several examples. We will define the concept of equivalent norms and prove that any two norms on a finite-dimensional real or complex space are equivalent. We will also give a characterization of the norm which arises from an inner product space. This material is the foundation for the field of function analysis.

What You Need to Know

Understanding the new material in this section depends on mastery of the following concepts: real and complex inner product space, norm of a vector in an inner product space, unit vector in an inner product space, the space $\mathbb{R}^n$, the space $\mathbb{C}^n$. You will also need to be familiar with the notion of a topological space, a metric space, the limit of a sequence in a topological space, a Cauchy sequence in a metric space, a continuous function between topological spaces, and a compact subset of a topological space. A brief introduction to these concepts can be found in Appendix A.

Assume $(V, \langle\ ,\ \rangle)$ is an inner product space and $\parallel \cdot \parallel$ is the norm defined on V by $\parallel \boldsymbol{v} \parallel = \sqrt{\langle \boldsymbol{v}, \boldsymbol{v} \rangle}$. Then we showed that $\parallel \cdot \parallel$ satisfies the following:

1. For every vector $\boldsymbol{v}$, $\parallel \boldsymbol{v} \parallel$ is a non-negative real number and $\parallel \boldsymbol{v} \parallel = 0$ if and only if $\boldsymbol{v} = \mathbf{0}$.

2. If c is a scalar and $\boldsymbol{v}$ a vector then $\parallel c\boldsymbol{v} \parallel = |c| \ \parallel \boldsymbol{v} \parallel$.

3. If $\boldsymbol{u}, \boldsymbol{v}$ are vectors then $\parallel \boldsymbol{u} + \boldsymbol{v} \parallel \ \leq \ \parallel \boldsymbol{u} \parallel \ + \ \parallel \boldsymbol{v} \parallel$.

Property 3 was referred to as the **triangle inequality**. We generalize from the notion of a norm defined by an inner product to that of an abstract norm by taking these properties as its axioms.

Definition 5.20 *Let V be a vector space over $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. A* **norm** *on V is a function $\parallel \cdot \parallel$ from V to $\mathbb{R}$ which satisfies the following:*

1. For every vector $\boldsymbol{v}$, $\parallel \boldsymbol{v} \parallel$ is a non-negative real number and $\parallel \boldsymbol{v} \parallel = 0$ if and only if $\boldsymbol{v} = \mathbf{0}$.

2. If c is a scalar and $\boldsymbol{v}$ a vector then $\parallel c\boldsymbol{v} \parallel = |c| \parallel \boldsymbol{v} \parallel$.

3. If $\boldsymbol{u}, \boldsymbol{v}$ are vectors then $\parallel \boldsymbol{u} + \boldsymbol{v} \parallel \leq \parallel \boldsymbol{u} \parallel + \parallel \boldsymbol{v} \parallel$.

A pair $(V, \parallel \cdot \parallel)$ consisting of a real or complex vector space V and a norm on V is referred to as a **normed vector space**.

Definition 5.21 *Let $(V, \parallel \ \ \parallel)$ be a normed space. For vectors $\boldsymbol{x}, \boldsymbol{y}$ define the* **distance**, *$d(\boldsymbol{x}, \boldsymbol{y},)$ between $\boldsymbol{x}$ and $\boldsymbol{y}$ to be $d(\boldsymbol{x}, \boldsymbol{y}) = \parallel \boldsymbol{x} - \boldsymbol{y} \parallel$.*

.

The following is nearly immediate:

Theorem 5.23 *Let $d(\ , \ )$ be the distance function defined by a norm $\parallel \ \ \parallel$ on a vector space V. Then the following are satisfied:*

1. $d(\boldsymbol{x}, \boldsymbol{y}) \geq 0$ with equality if and only if $\boldsymbol{x} = \boldsymbol{y}$.
2. $d(\boldsymbol{x}, \boldsymbol{y}) = d(\boldsymbol{y}, \boldsymbol{x})$.
3. $d(\boldsymbol{x}, \boldsymbol{z}) \leq d(\boldsymbol{x}, \boldsymbol{y}) + d(\boldsymbol{y}, \boldsymbol{z})$.

We leave these as exercises.

Theorem (5.23) says that the distance function defined on a normed space $(V, \parallel \ \ \parallel)$ is a **metric**. This can be used to define a topology on V which allows us to introduce such concepts as the limit of a sequence, continuity of functions, and so on. We now enumerate some examples.

Example 5.11 *Let $(V, \langle \ , \ \rangle)$ be an inner product space. We have seen that $\parallel \boldsymbol{v} \parallel = \sqrt{\langle \boldsymbol{v}, \boldsymbol{v} \rangle}$ is a norm. This is the* **norm on V induced by the inner product $\langle \ , \ \rangle$**.

As a specific example, let $V = \mathbb{F}^n$ where $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. Recall the Euclidean inner product on V is defined by $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \boldsymbol{x}^{tr}\overline{\boldsymbol{y}}$. The norm induced by this inner product is given by

$$\parallel \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \parallel = \sqrt{x_1\overline{x_1} + \cdots + x_n\overline{x_m}} = (|x_1|^2 + \ldots |x_n|^2)^{\frac{1}{2}}.$$

Example 5.12 *Let $V = \mathbb{F}^n$ where $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$ and p be a real number $p \geq 1$. Set*

$$\parallel \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \parallel_p = (|x_1|^p + \cdots + |x_n|^p)^{\frac{1}{p}}.$$

This is the l_p-**norm on** *V. Note that when $p = 2$ this is the norm of Example (5.11).*

Let $V = \mathbb{F}^n$ with $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$ and p be a real number, $p \geq 1$. Clearly, $\| \boldsymbol{x} \|_p \geq 0$ with equality if and only if $\boldsymbol{x} = \boldsymbol{0}$. Also, $\| c\boldsymbol{x} \|_p = |c| \quad \| \boldsymbol{x} \|_p$ for any scalar c. Thus, to establish that $\| \quad \|_p$ is a norm requires proving that the triangle inequality holds. That is, we need to prove for $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \boldsymbol{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ then

$$\left(\sum_{k=1}^{n} |x_k + y_k|^p \right)^{\frac{1}{p}} \leq \left(\sum_{k=1}^{n} |x_k|^p \right)^{\frac{1}{p}} + \left(\sum_{k=1}^{n} |y_k|^p \right)^{\frac{1}{p}}. \qquad (5.41)$$

The inequality in (5.41) is known as Minkowski's inequality. A proof can be found in ([4, p. 136]).

Apart from the l_2-norm, another important example is the l_1-norm which is defined as follows:

$$\| \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \|_1 = \sum_{k=1}^{n} |x_k|.$$

Yet another common norm is the l_∞-norm. This is defined by

$$\| \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \|_\infty = max\{|x_1|, \ldots, |x_n|\}. \qquad (5.42)$$

We leave it as an exercise to verify that Equation (5.42) defines a norm.

As mentioned above, in a normed space $(V, \| \quad \|)$ the distance function defined by the norm is a metric and it can be used to define the notion of an open set, whence a topology on V.

Definition 5.22 *Let $(V, \| \quad \|)$ be a normed vector space with induced distance function d. Let $\boldsymbol{u} \in V$ and r be a positive real number. The* **open ball centered at $\boldsymbol{u}$ with radius** *r, denoted by $B_r(\boldsymbol{u})$, is the set of all $\boldsymbol{v} \in V$ such that $d(\boldsymbol{u}, \boldsymbol{v}) < r$. A subset X of V is said to be* **open** *if for every $\boldsymbol{x} \in X$ there is a positive real number r (which may depend on $\boldsymbol{x}$) such that $B_r(\boldsymbol{x})$ is contained in X.*

Remark 5.6 *If $\mathcal{T}$ is the set of open subsets of V then $(V, \mathcal{T})$ is a topological space.*

In the next several examples we illustrate what the open balls look like for the three norms $\| \quad \|_p$ where $p \in \{1, 2, \infty\}$ for $V = \mathbb{R}^2$.

Example 5.13 *The open ball of radius 1 centered at* $\begin{pmatrix}0\\0\end{pmatrix}$ *in the normed space* $(\mathbb{R}^2, \|\quad\|_1)$ *consists of all those vectors* $\boldsymbol{x} = \begin{pmatrix}x_1\\x_2\end{pmatrix}$ *such that* $\| \boldsymbol{x} \|_1$ $|x_1| + |x_2| < 1$. *This is shown in Figure (5.2).*

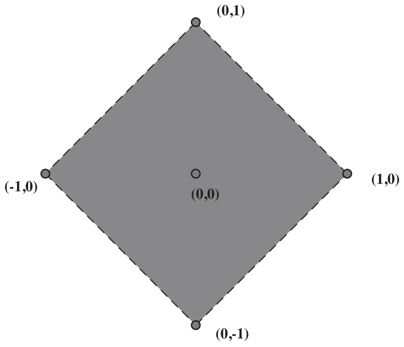

FIGURE 5.2
Unit ball with respect to l_1-norm.

Example 5.14 *The open ball of radius 1centered at* $\begin{pmatrix}0\\0\end{pmatrix}$ *in the normed space* $(\mathbb{R}^2, \|\quad\|_2)$ *consists of all those vectors* $\boldsymbol{x} = \begin{pmatrix}x_1\\x_2\end{pmatrix}$ *such that* $\| \boldsymbol{x} \| = \sqrt{x_1^2 + x_2^2} < 1$, *equivalently,* $x_1^2 + x_2^2 < 1$. *This is shown in Figure (5.3).*

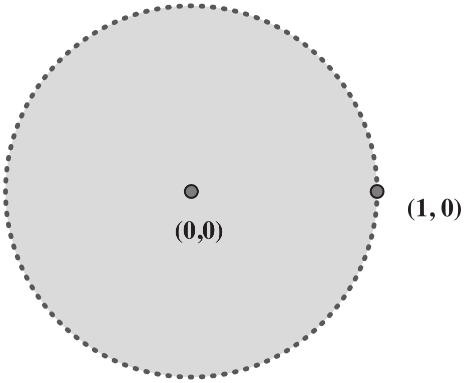

FIGURE 5.3
Unit ball with respect to l_2-norm.

Example 5.15 *The open ball of radius 1 centered at* $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ *in the normed space* $(\mathbb{R}^2, \| \quad \|_\infty)$ *consists of all those vectors* $\boldsymbol{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ *such that* $\| \boldsymbol{x} \| = max\{|x_1|, |x_2\} < 1$. *This is shown in Figure (5.4).*

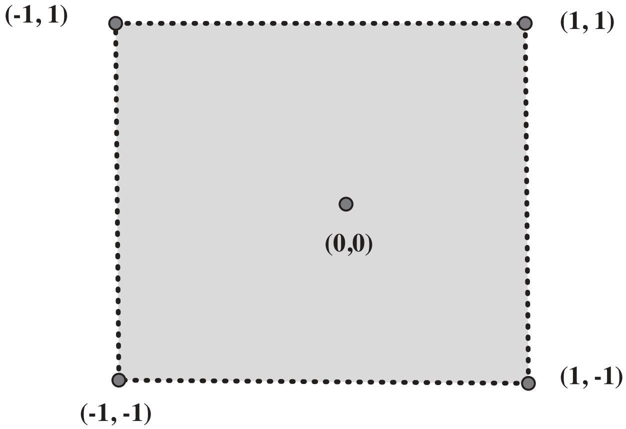

FIGURE 5.4
Unit ball with respect to l_∞-norm.

Because there is a metric on V, we can define such concepts as the limit of a sequence, a Cauchy sequence, continuous function between normed vector spaces as well as other notions from analysis. We refer the reader unfamiliar with these notions to Appendix A.

Definition 5.23 *A normed vector space* $(V, \| \quad \|)$ *is said to be a* **complete normed space** *if every Cauchy sequence has a limit. A complete normed vector space is referred to as a* **Banach space**.

Each of our examples of normed spaces is a Banach space. We prove this for the l_2-norm and leave the others as exercises.

Theorem 5.24 *Let* $V = \mathbb{F}^n, \mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. *Then* $(V, \| \quad \|_2)$ *is a Banach space.*

Proof *Assume* $\{\boldsymbol{x}_k\}_{k=1}^\infty$ *is a Cauchy sequence. Suppose* $\boldsymbol{x}_k = \begin{pmatrix} \boldsymbol{x}_{1k} \\ \vdots \\ x_{nk} \end{pmatrix}$. *We* *claim for each $j, 1 \leq j \leq n$, that $\{x_{jk}\}_{k=1}^{\infty}$ is a Cauchy sequence. This follows since $|x_{jk} - x_{jl}|^2 \leq \sum_{i=1}^{n} |x_{ik} - x_{il}|^2 =\| \boldsymbol{x}_k - \boldsymbol{x}_l \|_2^2$ and the fact that $\{\boldsymbol{x}_k\}_{k=1}^{\infty}$ is a Cauchy sequence. Since $\mathbb{R}$ and $\mathbb{C}$ are complete it follows that the sequence $\{x_{jk}\}_{k=1}^{\infty}$ has a limit which we denote by x_j. Set $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. We claim that $lim_{k\to\infty}\boldsymbol{x}_k = \boldsymbol{x}$. Thus, let $\epsilon > 0$. Since $lim_{k\to\infty}x_{jk} = x_j$ there is an N_j such that if $k \geq N_j$ then $|x_j - x_{jk}| < \frac{\epsilon}{\sqrt{n}}$. Set $N = max\{N_1, \ldots, N_n\}$ and suppose $k > N$. Then $|x_j - x_{jk}|^2 < \frac{\epsilon^2}{n}$. Consequently, $\| \boldsymbol{x} - \boldsymbol{x}_k \|_2^2 = \sum_{j=1} |x_j - x_{jk}|^2 < \epsilon^2$ from which we conclude that $\| \boldsymbol{x} - \boldsymbol{x}_k \|_2 < \epsilon$.*

Because we will need it shortly, we recall the definition of a continuous function between normed vector spaces.

Definition 5.24 *Let $(V, \| \ \|_V)$ and $(W, \| \ \|_W)$ be two normed spaces over the same field $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$ and $f : V \to W$ a function. The function f is said to be* **continuous at $\boldsymbol{x}_0$** *if for every $\epsilon > 0$ there is a δ (which may depend on ϵ) such that if $\| \boldsymbol{x} - \boldsymbol{x}_0 \|_V < \delta$ then $\| f(\boldsymbol{x}) - f(\boldsymbol{x}_0) \|_W < \epsilon$. The function f is* **continuous** *if it is continuous at $\boldsymbol{x}$ for every $\boldsymbol{x} \in V$.*

In a subsequent section (in Chapter 12) we define the concepts of operator and matrix norms we will show that a linear function between two finite-dimensional normed spaces is continuous. Our immediate goal, however, is to define the notion of equivalent norms on a space and to show that all norms on $\mathbb{F}^n, \mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$ are equivalent.

Definition 5.25 *Let $\| \ \|$ and $\| \ \|_\star$ be norms on a real or complex vector space V. We say that $\| \ \|$ is* **equivalent** *to $\| \ \|_\star$ if there are positive real numbers c and d such that $c \| \boldsymbol{x} \|_\star \leq \| \boldsymbol{x} \| \leq d \| \boldsymbol{x} \|_\star$ for every vector $\boldsymbol{x}$.*

The following is entirely straightforward.

Theorem 5.25 *Equivalence of norms on a vector space V over $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$ is an equivalence relation.*

Our next objective is to prove that all norms on a finite-dimensional real or complex vector space V are equivalent. We begin with a definition.

Definition 5.26 *A subset C of a normed linear space $(V, \| \ \|)$ is* **bounded** *if there exists a positive real number r such that $C \subset B_r(\mathbf{0})$.*

The following theorem is usually proved in a first course in analysis. It is known as the real Heine–Borel theorem.

Theorem 5.26 *A subset C of $\mathbb{R}$ is compact if and only if C is closed and bounded.*

In a first course in functional analysis, Theorem (5.26) is extended to an arbitrary finite-dimensional normed space $(V, \| \quad \|)$:

Theorem 5.27 *Let $(V, \| \quad \|)$ be a finite-dimensional normed space. A subset C of V is compact if and only if C is closed and bounded.*

We can conclude from Theorem(5.26), Theorem (5.27), and Theorem (A.3) the following:

Theorem 5.28 *Let $(V, \| \quad \|)$ be a finite-dimensional normed space and C a compact subset of V. Then there exists elements $m, M \in C$ such that*

$$\| m \| \leq \| x \| \leq \| M \|$$

for every $x \in C$.

Before proving the equivalence of norms we will need the following lemma.

Lemma 5.5 *Let $(V, \| \quad \|)$ be normed space and $\boldsymbol{x}, \boldsymbol{y} \in V$. Then*

$$| \| \boldsymbol{x} \| - \| \boldsymbol{y} \| | \quad \leq \quad \| \boldsymbol{x} - \boldsymbol{y} \| .$$

Proof *For any vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ we have*

$$\begin{aligned} \| \boldsymbol{x} \| &= \| (\boldsymbol{x} - \boldsymbol{y}) + \boldsymbol{y} \| \\ &\leq \| \boldsymbol{x} - \boldsymbol{y} \| + \| \boldsymbol{y} \| . \end{aligned}$$

Consequently,

$$\| \boldsymbol{x} \| - \| \boldsymbol{y} \| \leq \| \boldsymbol{x} - \boldsymbol{y} \| .$$

By interchanging $\boldsymbol{x}$ and $\boldsymbol{y}$ we get

$$\begin{aligned} \| \boldsymbol{y} \| - \| \boldsymbol{x} \| &\leq \| \boldsymbol{y} - \boldsymbol{x} \| \\ &= \| \boldsymbol{x} - \boldsymbol{y} \| . \end{aligned}$$

Thus,

$$\left| \; \| \boldsymbol{x} \| - \| \boldsymbol{y} \| \; \right| \leq \; \| \boldsymbol{x} - \boldsymbol{y} \| .$$

As an immediate corollary we have:

Corollary 5.1 *Let $(V, \| \ \|)$ be a normed space. Then the function $\| \ \|: V \to \mathbb{R}$ is continuous.*

Before proceeding to the proof that all norms on a finite-dimensional space over $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$ are equivalent, we state a lemma which we will need. We leave its proof as an exercise.

Lemma 5.6 *Let $\| \cdot \|$ be an arbitrary norm on $\mathbb{F}^n$, where $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. Let S_1^∞ be the collection of all vectors $\boldsymbol{x} \in \mathbb{F}^n$ such that $\| \boldsymbol{x} \|_\infty = 1$. Then S_1^∞ is closed and bounded in $(V, \| \cdot \|)$.*

Theorem 5.29 *Let V be a finite-dimensional real or complex vector space. Then all norms on V are equivalent.*

Proof *Assume V has dimension n and choose a basis $\mathcal{B} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ for V. Let $T : \mathbb{F}^n \to V$ be the linear transformation defined by*

$$T\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right) = x_1\boldsymbol{v}_1 + \cdots + x_n\boldsymbol{v}_n.$$

T is an isomorphism. If $\| \ \|$ is a norm on V then define a norm ϕ on $\mathbb{F}^n$ by $\phi(\boldsymbol{x}) = \| T(\boldsymbol{x}) \|$. Suppose now that $\| \ \|_\star$ is a second norm on V and $\phi_\star$ is defined by $\phi_\star(\boldsymbol{x}) = \| T(\boldsymbol{x}) \|_\star$. Then $\| \ \|$ and $\| \ \|_\star$ are equivalent if and only if ϕ and $\phi_\star$ are equivalent and therefore we may assume that $V = \mathbb{F}^n$. We will show that an arbitrary norm $\| \ \|$ on $\mathbb{F}^n$ is equivalent to the ∞-norm.

As in Lemma (5.6), let S_1^∞ consist of those vectors $\boldsymbol{v} \in V$ such that $\| \boldsymbol{v} \|_\infty = 1$. By Lemma (5.6), S_1^∞ is compact in $(V, \| \cdot \|)$. Since $\| \ \|: V \to \mathbb{F}$ is continuous, $\{\| \boldsymbol{x} \| \, | \boldsymbol{x} \in S_1^\infty\}$ has a minimum and a maximum which are both positive since $\boldsymbol{0} \notin S_1^\infty$. Let c and d be the minimum and maximum, respectively. Then for any non-zero vector $\boldsymbol{x} \in V$, $\frac{1}{\|\boldsymbol{x}\|_\infty}\boldsymbol{x}$ is a unit vector with respect to the l_∞-norm. Consequently

$$c \ \leq \ \| \frac{1}{\| \boldsymbol{x} \|_\infty}\boldsymbol{x} \| \ \leq \ d.$$

Whence

$$c \ \leq \ \frac{\| \boldsymbol{x} \|}{\| \boldsymbol{x} \|_\infty} \ \leq d \ .$$

Now multiply by $\| \boldsymbol{x} \|_\infty$ to obtain

$$c \parallel \boldsymbol{x} \parallel_\infty \quad \leq \quad \parallel \boldsymbol{x} \parallel \quad \leq \; d \parallel \boldsymbol{x} \parallel_\infty$$

as was to be shown.

In our final result of this section we characterize the norms which arise from an inner product. Recall when $(V, \langle\ ,\rangle)$ is an inner product space and $\parallel\ \ \parallel$ is the norm induced by $\langle\ ,\ \rangle$ the parallelogram property holds: For $\boldsymbol{x}, \boldsymbol{y} \in V$

$$\parallel \boldsymbol{x} + \boldsymbol{y} \parallel^2 + \parallel \boldsymbol{x} - \boldsymbol{y} \parallel^2 = 2(\parallel \boldsymbol{x} \parallel^2 + \parallel \boldsymbol{y} \parallel^2).$$

It is easy to see that this does not hold for the l_1-norm or the l_∞-norm. In our final result of this section we characterize norms that arise from an inner product as those that satisfy the parallelogram property.

Theorem 5.30 *Let $(V, \parallel\ \ \parallel)$ be a finite-dimensional normed space. Then $\parallel\ \ \parallel$ is induced by an inner product if and only if the parallelogram property holds.*

Proof *We have already seen in Theorem (5.6), if $\parallel\ \ \parallel$ is induced by an inner product then the parallelogram property holds, so we must prove the converse. We do so in the case that V is a complex space. The real case can be deduced from this. For $\boldsymbol{x}, \boldsymbol{y} \in V$ set*

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \frac{1}{4}(\parallel \boldsymbol{x} + \boldsymbol{y} \parallel^2 - \parallel \boldsymbol{x} - \boldsymbol{y} \parallel^2 + i \parallel \boldsymbol{x} + i\boldsymbol{y} \parallel^2 - i \parallel \boldsymbol{x} - i\boldsymbol{y} \parallel^2).$$

We will show that $\langle\ ,\ \rangle$ is an inner product and the norm induced by it is $\parallel\ \ \parallel$. We do this in a series of steps.

1. We claim that $\langle \boldsymbol{x}, \boldsymbol{x} \rangle = \parallel \boldsymbol{x} \parallel^2$. We compute:

$$\begin{aligned} \langle \boldsymbol{x}, \boldsymbol{x} \rangle &= \frac{1}{4}(4 \parallel \boldsymbol{x} \parallel^2 + i|1+i|^2 \parallel \boldsymbol{x} \parallel^2 - i|1-i|^2 \parallel \boldsymbol{x} \parallel^2) \\ &= \frac{1}{4} \parallel \boldsymbol{x} \parallel^2 (4 + 4i - 4i) \\ &= \parallel \boldsymbol{x} \parallel^2 . \end{aligned}$$

2. We next show that $\langle \boldsymbol{y}, \boldsymbol{x} \rangle = \overline{\langle \boldsymbol{x}, \boldsymbol{y} \rangle}$. Note that

$$\parallel \boldsymbol{x} + i\boldsymbol{y} \parallel^2 = \parallel \boldsymbol{y} - i\boldsymbol{x} \parallel^2, \parallel \boldsymbol{x} - \boldsymbol{y} \parallel^2 = \parallel \boldsymbol{y} - \boldsymbol{x} \parallel^2,$$

$$\parallel \boldsymbol{x} + \boldsymbol{y} \parallel^2 = \parallel \boldsymbol{y} + \boldsymbol{x} \parallel^2, \parallel \boldsymbol{x} - i\boldsymbol{y} \parallel^2 = \parallel \boldsymbol{y} + i\boldsymbol{x} \parallel^2 .$$

Then

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \frac{1}{4}(i \parallel \boldsymbol{y} - i\boldsymbol{x} \parallel^2 - \parallel \boldsymbol{y} - \boldsymbol{x} \parallel^2 - i \parallel \boldsymbol{y} + i\boldsymbol{x} \parallel^2 + \parallel \boldsymbol{y} + \boldsymbol{x} \parallel^2).$$

Consequently,

$$\begin{aligned} \overline{\langle \boldsymbol{x}, \boldsymbol{y} \rangle} &= \frac{1}{4}(-i \parallel \boldsymbol{y} - i\boldsymbol{x} \parallel^2 - \parallel \boldsymbol{y} - \boldsymbol{x} \parallel^2 + i \parallel \boldsymbol{y} + i\boldsymbol{x} \parallel^2 + \parallel \boldsymbol{y} + \boldsymbol{x} \parallel^2) \\ &= \langle \boldsymbol{y}, \boldsymbol{x} \rangle. \end{aligned}$$

3. For any vector $\boldsymbol{x}, \langle \boldsymbol{x}, \boldsymbol{0} \rangle = 0$. *We compute*

$$\langle \boldsymbol{x}, \boldsymbol{0} \rangle = \frac{1}{4}(\parallel \boldsymbol{x} \parallel^2 - \parallel \boldsymbol{x} \parallel^2 - i \parallel \boldsymbol{x} \parallel^2 + i \parallel \boldsymbol{x} \parallel^2) = 0.$$

4. Let $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{u}, \boldsymbol{v} \in V$. *Then*

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle + \langle \boldsymbol{u}, \boldsymbol{v} \rangle = 2[\langle \frac{\boldsymbol{x}+\boldsymbol{u}}{2}, \frac{\boldsymbol{y}+\boldsymbol{v}}{2} \rangle + \langle \frac{\boldsymbol{x}-\boldsymbol{u}}{2}, \frac{\boldsymbol{y}-\boldsymbol{v}}{2} \rangle], \tag{5.43}$$

This is where we use the parallelogram property. The left-hand side is equal to

$$\frac{1}{4}(\parallel \boldsymbol{x} + i\boldsymbol{y} \parallel^2 - \parallel \boldsymbol{x} - \boldsymbol{y} \parallel^2 - i \parallel \boldsymbol{x} - i\boldsymbol{y} \parallel^2 + \parallel \boldsymbol{x} + \boldsymbol{y} \parallel^2) +$$
$$\frac{1}{4}(\parallel \boldsymbol{u} + i\boldsymbol{v} \parallel^2 - \parallel \boldsymbol{u} - \boldsymbol{v} \parallel^2 - i \parallel \boldsymbol{u} - i\boldsymbol{v} \parallel^2 + \parallel \boldsymbol{u} + \boldsymbol{v} \parallel^2).$$

We now compute the right-hand side. Note that $\langle a\boldsymbol{w}, a\boldsymbol{z} \rangle = |a|^2 \langle \boldsymbol{w}, \boldsymbol{z} \rangle$. *As a consequence we have*

$$\frac{1}{2}(\langle \frac{\boldsymbol{x}+\boldsymbol{u}}{2}, \frac{\boldsymbol{y}+\boldsymbol{v}}{2} \rangle) + \frac{1}{2}\langle \frac{\boldsymbol{x}-\boldsymbol{u}}{2}, \frac{\boldsymbol{y}-\boldsymbol{v}}{2} \rangle) = \frac{1}{8}(\langle \boldsymbol{x}+\boldsymbol{u}, \boldsymbol{y}+\boldsymbol{v} \rangle + \langle \boldsymbol{x}-\boldsymbol{u}, \boldsymbol{y}-\boldsymbol{v} \rangle).$$

$$\langle \boldsymbol{x}+\boldsymbol{u}, \boldsymbol{y}+\boldsymbol{v} \rangle + \langle \boldsymbol{x}-\boldsymbol{u}, \boldsymbol{y}-\boldsymbol{v} \rangle =$$

$$\parallel (\boldsymbol{x}+\boldsymbol{u}) + i(\boldsymbol{y}+\boldsymbol{v}) \parallel^2 - \parallel (\boldsymbol{x}+\boldsymbol{u}) - (\boldsymbol{y}+\boldsymbol{v}) \parallel^2 - \parallel (\boldsymbol{x}+\boldsymbol{u}) - i(\boldsymbol{y}+\boldsymbol{v}) \parallel^2 +$$

$$\parallel (\boldsymbol{x}+\boldsymbol{u}) + (\boldsymbol{y}+\boldsymbol{v}) \parallel^2 + \parallel (\boldsymbol{x}-\boldsymbol{u}) + i(\boldsymbol{y}-\boldsymbol{v}) \parallel^2 - \parallel (\boldsymbol{x}-\boldsymbol{u}) - (\boldsymbol{y}-\boldsymbol{v}) \parallel^2 -$$

$$\| (\boldsymbol{x}-\boldsymbol{u}) - i(\boldsymbol{y}-\boldsymbol{v}) \|^2 + \| (\boldsymbol{x}-\boldsymbol{u}) + (\boldsymbol{y}-\boldsymbol{v}) \|^2 .$$

By the parallelogram property we have

$$\| (\boldsymbol{x}+\boldsymbol{u}) + i(\boldsymbol{y}+\boldsymbol{v}) \|^2 + \| (\boldsymbol{x}-\boldsymbol{u}) + i(\boldsymbol{y}-\boldsymbol{v}) \|^2 =$$

$$\| (\boldsymbol{x}+i\boldsymbol{y}) + (\boldsymbol{u}+i\boldsymbol{v}) \|^2 + \| (\boldsymbol{x}+i\boldsymbol{y}) - (\boldsymbol{u}+i\boldsymbol{v}) \|^2 =$$

$$2(\| \boldsymbol{x}+i\boldsymbol{y} \|^2 + \| \boldsymbol{u}+i\boldsymbol{v} \|^2); \tag{5.44}$$

$$\| (\boldsymbol{x}+\boldsymbol{u}) - (\boldsymbol{y}+\boldsymbol{v}) \|^2 + \| (\boldsymbol{x}-\boldsymbol{u}) - (\boldsymbol{y}-\boldsymbol{v}) \|^2 =$$

$$\| (\boldsymbol{x}-\boldsymbol{y}) + (\boldsymbol{u}-\boldsymbol{v}) \|^2 + \| (\boldsymbol{x}-\boldsymbol{y}) - (\boldsymbol{u}-\boldsymbol{v}) \|^2 =$$

$$2(\| \boldsymbol{x}-\boldsymbol{y} \|^2 + \| \boldsymbol{u}-\boldsymbol{v} \|^2) \tag{5.45}$$

$$\| (\boldsymbol{x}+\boldsymbol{u}) - i(\boldsymbol{y}+\boldsymbol{v}) \|^2 + \| (\boldsymbol{x}-\boldsymbol{u}) - i(\boldsymbol{y}-\boldsymbol{v}) \|^2 =$$

$$\| (\boldsymbol{x}-i\boldsymbol{y}) + (\boldsymbol{u}-i\boldsymbol{v}) \|^2 + \| (\boldsymbol{x}-i\boldsymbol{y}) - (\boldsymbol{u}-i\boldsymbol{v}) \|^2 =$$

$$2(\| \boldsymbol{x}-i\boldsymbol{y} \|^2 + \| \boldsymbol{u}-i\boldsymbol{v} \|^2) \tag{5.46}$$

$$\| (\boldsymbol{x}+\boldsymbol{u}) + (\boldsymbol{y}+\boldsymbol{v}) \|^2 + \| (\boldsymbol{x}-\boldsymbol{u}) + (\boldsymbol{y}-\boldsymbol{v}) \|^2 =$$

$$\| (\boldsymbol{x}+\boldsymbol{y}) + (\boldsymbol{u}+\boldsymbol{v}) \|^2 + \| (\boldsymbol{x}+\boldsymbol{y}) - (\boldsymbol{u}+\boldsymbol{v}) \|^2 =$$

$$2(\| \boldsymbol{x}+\boldsymbol{y} \|^2 + \| \boldsymbol{u}+\boldsymbol{v} \|^2). \tag{5.47}$$

Multiply both sides in Equation (5.44) by $\frac{i}{8}$, *both sides of Equation (5.45) by* $-\frac{1}{8}$, *both sides of Equation (5.46) by* $-\frac{i}{8}$, *and both sides of Equation of (5.47) by* $\frac{1}{8}$, *and add. The identity of Equation (5.43) is obtained.*

5. For any vectors $\boldsymbol{x}, \boldsymbol{y}$ *we have* $\langle 2\boldsymbol{x}, \boldsymbol{y} \rangle = 2\langle \boldsymbol{x}, \boldsymbol{y} \rangle$. *In Equation (5.43) take* $\boldsymbol{x} = \boldsymbol{x}, \boldsymbol{y} = \boldsymbol{y}, \boldsymbol{u} = \boldsymbol{x}, \boldsymbol{v} = \boldsymbol{0}$. *We then have*

$$\begin{aligned}
\langle \boldsymbol{x}, \boldsymbol{y} \rangle &= \langle \boldsymbol{x}, \boldsymbol{y} \rangle + \langle \boldsymbol{x}, \boldsymbol{0} \rangle \\
&= 2(\langle \frac{2\boldsymbol{x}}{2}, \frac{\boldsymbol{y}}{2} \rangle + \langle \boldsymbol{0}, \frac{\boldsymbol{y}}{2} \rangle) \\
&= 2\langle \frac{2\boldsymbol{x}}{2}, \frac{\boldsymbol{y}}{2} \rangle \\
&= \frac{1}{2}\langle 2\boldsymbol{x}, \boldsymbol{y} \rangle.
\end{aligned}$$

It follows that $\langle 2\boldsymbol{x}, \boldsymbol{y} \rangle = 2\langle \boldsymbol{x}, \boldsymbol{y} \rangle$.

6. For any vectors $\boldsymbol{x}, \boldsymbol{u}, \boldsymbol{y}$ *we have*

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle + \langle \boldsymbol{u}, \boldsymbol{y} \rangle = \langle \boldsymbol{x} + \boldsymbol{u}, \boldsymbol{y} \rangle.$$

In Equation (5.43) set $\boldsymbol{x} = \boldsymbol{x}, \boldsymbol{u} = \boldsymbol{u}, \boldsymbol{y} = \boldsymbol{y}, \boldsymbol{v} = \boldsymbol{y}$. *We then have*

$$\begin{aligned}
\langle \boldsymbol{x}, \boldsymbol{y} \rangle + \langle \boldsymbol{u}, \boldsymbol{y} \rangle &= 2(\langle \frac{\boldsymbol{x} + \boldsymbol{u}}{2}, \frac{2\boldsymbol{y}}{2} \rangle + \langle \frac{\boldsymbol{x} - \boldsymbol{u}}{2}, \frac{\boldsymbol{0}}{2} \rangle) \\
&= \frac{1}{2}\langle \boldsymbol{x} + \boldsymbol{u}, 2\boldsymbol{y} \rangle \\
&= \frac{1}{2} \cdot \overline{\langle 2\boldsymbol{y}, \boldsymbol{x} + \boldsymbol{u} \rangle} \\
&= \frac{1}{2} \cdot (\overline{2\langle \boldsymbol{y}, \boldsymbol{x} + \boldsymbol{u} \rangle}) \\
&= (\frac{1}{2} \cdot 2)\overline{\langle \boldsymbol{y}, \boldsymbol{x} + \boldsymbol{u} \rangle} \\
&= \overline{\langle \boldsymbol{y}, \boldsymbol{x} + \boldsymbol{u} \rangle} \\
&= \langle \boldsymbol{x} + \boldsymbol{u}, \boldsymbol{y} \rangle.
\end{aligned}$$

7. For any vectors $\boldsymbol{x}, \boldsymbol{y}, \langle -\boldsymbol{x}, \boldsymbol{y} \rangle = -\langle \boldsymbol{x}, \boldsymbol{y} \rangle$. *By step 6 we have*

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle + \langle -\boldsymbol{x}, \boldsymbol{y} \rangle = \langle \boldsymbol{0}, \boldsymbol{y} \rangle.$$

By step 3 $\langle \boldsymbol{0}, \boldsymbol{y} \rangle = 0$.

8. For any vectors $\boldsymbol{x}, \boldsymbol{y}$ *and natural number* $m, \langle m\boldsymbol{x}, \boldsymbol{y} \rangle = m\langle \boldsymbol{x}, \boldsymbol{y} \rangle$. *We prove this by induction. The base case is clear and we have already established this for* $m = 2$. *Suppose for some* $m \geq 2$ *that* $\langle m\boldsymbol{x}, \boldsymbol{y} \rangle = m\langle \boldsymbol{x}, \boldsymbol{y} \rangle$. *Now* $(m+1)\langle \boldsymbol{x}, \boldsymbol{y} \rangle = m\langle \boldsymbol{x}, \boldsymbol{y} \rangle + \langle \boldsymbol{x}, \boldsymbol{y} \rangle$. *By the inductive hypothesis* $m\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \langle m\boldsymbol{x}, \boldsymbol{y} \rangle$. *By step 6 we have* $\langle m\boldsymbol{x}, \boldsymbol{y} \rangle + \langle \boldsymbol{x}, \boldsymbol{y} \rangle = \langle m\boldsymbol{x} + \boldsymbol{x}, \boldsymbol{y} \rangle = \langle (m+1)\boldsymbol{x}, \boldsymbol{y} \rangle$ *as was to be shown.*

9. Let m, n *be natural numbers. Then* $\langle \frac{m}{n}, \boldsymbol{y} \rangle = \frac{m}{n}\langle \boldsymbol{x}, \boldsymbol{y} \rangle$. *We first prove this for* $m = 1$. *We have*

$$\begin{aligned}\langle \boldsymbol{x},\boldsymbol{y}\rangle &= \langle (n\cdot\frac{1}{n})\boldsymbol{x},\boldsymbol{y}\rangle\\ &= \langle n\cdot(\frac{1}{n}\cdot\boldsymbol{x}),\boldsymbol{y}\rangle\\ &= n\langle\frac{1}{n}\cdot\boldsymbol{x},\boldsymbol{y}\rangle.\end{aligned}$$

Now divide both sides by n *to get* $\frac{1}{n}\cdot\langle\boldsymbol{x},\boldsymbol{y}\rangle = \langle\frac{1}{n}\cdot\boldsymbol{x},\boldsymbol{y}\rangle$.

We apply this to the general case:

$$\begin{aligned}\langle\frac{m}{n}\cdot\boldsymbol{x},\boldsymbol{y}\rangle &= \langle m\cdot(\frac{1}{n}\cdot\boldsymbol{x}),\boldsymbol{y}\rangle\\ &= m\cdot\langle\frac{1}{n}\cdot\boldsymbol{x},\boldsymbol{y}\rangle\\ &= m\cdot(\frac{1}{n}\cdot\langle\boldsymbol{x},\boldsymbol{y}\rangle)\\ &= (m\cdot\frac{1}{n})\cdot\langle\boldsymbol{x},\boldsymbol{y}\rangle\\ &= \frac{m}{n}\cdot\langle\boldsymbol{x},\boldsymbol{y}\rangle.\end{aligned}$$

10. Putting steps 7 and 9 together, it follows for any rational number q *that* $\langle q\boldsymbol{x},\boldsymbol{y}\rangle = q\langle\boldsymbol{x},\boldsymbol{y}\rangle$.

11. Fix $\boldsymbol{y}$. *Then the function that takes* $\boldsymbol{x}$ *to* $\langle\boldsymbol{x},\boldsymbol{y}\rangle$ *is a continuous function. Define a function* $f: V\to\mathbb{R}$ *by* $f(\boldsymbol{x}) = \parallel \boldsymbol{x}+\boldsymbol{y}\parallel$. *Then* f *is continuous. This is immediate since* $\mid \parallel\boldsymbol{x}+\boldsymbol{y}\parallel - \parallel\boldsymbol{x}'+\boldsymbol{y}\parallel \mid \leq \parallel\boldsymbol{x}-\boldsymbol{x}'\parallel$. *It follows that each of the following functions is continuous:*

$$\boldsymbol{x}\to\parallel\boldsymbol{x}+\boldsymbol{y}\parallel^2, \boldsymbol{x}\to\parallel\boldsymbol{x}-\boldsymbol{y}\parallel^2,$$

$$\boldsymbol{x}\to\parallel\boldsymbol{x}+i\boldsymbol{y}\parallel^2, \boldsymbol{x}\to\parallel\boldsymbol{x}-i\boldsymbol{y}\parallel^2 .$$

Since any linear combination of continuous functions is continuous, it follows that $\boldsymbol{x}\to\langle\boldsymbol{x},\boldsymbol{y}\rangle$ *is continuous.*

12. If β *is a real number then* $\langle\beta\boldsymbol{x},\boldsymbol{y}\rangle = \beta\langle\boldsymbol{x},\boldsymbol{y}\rangle$. *Let* $\{q_n\}_{n=1}^{\infty}$ *be a sequence of rational numbers such that*

$$\lim_{n\to\infty} q_n = \beta.$$

Since $\langle\cdot,\boldsymbol{y}\rangle$ *is a continuous function we have*

$$\lim_{n\to\infty}\langle q_n\boldsymbol{x},\boldsymbol{y}\rangle = \langle \lim_{n\to\infty} q_n\boldsymbol{x},\boldsymbol{y}\rangle = \langle \beta\boldsymbol{x},\boldsymbol{y}\rangle.$$

However, $\langle q_n\boldsymbol{x},\boldsymbol{y}\rangle = q_n\langle\boldsymbol{x},\boldsymbol{y}\rangle$ *and therefore*

$$\lim_{n\to\infty}\langle q_n\boldsymbol{x},\boldsymbol{y}\rangle = \lim_{n\to\infty} q_n\langle\boldsymbol{x},\boldsymbol{y}\rangle = \beta\langle\boldsymbol{x},\boldsymbol{y}\rangle.$$

13. For any vectors $\boldsymbol{x}$ *and* $\boldsymbol{y}$, $\langle i\boldsymbol{x},\boldsymbol{y}\rangle = i\langle\boldsymbol{x},\boldsymbol{y}\rangle$.

By the definition of $\langle\ ,\ \rangle$ *we have*

$$\begin{aligned}
\langle i\boldsymbol{x},\boldsymbol{y}\rangle &= \frac{1}{4}(\| i\boldsymbol{x}+i\boldsymbol{y}\|^2 - \| i\boldsymbol{x}-\boldsymbol{y}\|^2 - i\| i\boldsymbol{x}-i\boldsymbol{y}\|^2 + \| i\boldsymbol{x}+\boldsymbol{y}\|^2)\\
&= \frac{1}{4}(i\|\boldsymbol{x}+\boldsymbol{y}\|^2 - \|\boldsymbol{x}+i\boldsymbol{y}\|^2 - i\|\boldsymbol{x}-\boldsymbol{y}\|^2 + \|\boldsymbol{x}-i\boldsymbol{y}\|^2)\\
&= i\cdot(\frac{1}{4}\|\boldsymbol{x}+\boldsymbol{y}\|^2 + i\|\boldsymbol{x}+i\boldsymbol{y}\|^2 - \|\boldsymbol{x}-\boldsymbol{y}\|^2 - i\|\boldsymbol{x}-i\boldsymbol{y}\|^2)\\
&= i\langle\boldsymbol{x},\boldsymbol{y}\rangle.
\end{aligned}$$

14. For any vectors $\boldsymbol{x},\boldsymbol{y}$ *and complex number* γ *we have* $\langle\gamma\boldsymbol{x},\boldsymbol{y}\rangle = \gamma\langle\boldsymbol{x},\boldsymbol{y}\rangle$. *Let* $\alpha,\beta\in\mathbb{R}$ *such that* $\gamma=\alpha+i\beta$. *Then*

$$\begin{aligned}
\langle\gamma\boldsymbol{x},\boldsymbol{y}\rangle &= \langle(\alpha+i\beta)\boldsymbol{x},\boldsymbol{y}\rangle\\
&= \langle\alpha\boldsymbol{x}+i\beta\boldsymbol{x},\boldsymbol{y}\rangle\\
&= \langle\alpha\boldsymbol{x},\boldsymbol{y}\rangle + \langle i\beta\boldsymbol{x},\boldsymbol{y}\rangle\\
&= \alpha\langle\boldsymbol{x},\boldsymbol{y}\rangle + i\langle\beta\boldsymbol{x},\boldsymbol{y}\rangle\\
&= \alpha\langle\boldsymbol{x},\boldsymbol{y}\rangle + i\beta\langle\boldsymbol{x},\boldsymbol{y}\rangle\\
&= (\alpha+i\beta)\langle\boldsymbol{x},\boldsymbol{y}\rangle\\
&= \gamma\langle\boldsymbol{x},\boldsymbol{y}\rangle.
\end{aligned}$$

A good source for further reading on this topic is ([4]).

Exercises

1. Compute the l_p -norm with $p\in\{1,2,\infty\}$ of the following vectors:

a) $\begin{pmatrix}-4\\2\\-1\\2\end{pmatrix}$ b) $\begin{pmatrix}3\\-6\\0\\2\end{pmatrix}$

2. Find the distance between the two vectors of Exercise 1 with respect to the l_p-norm with $p\in\{1,2,\infty\}$.

3. Find the distance from the origin to the line $x+2y=3$ with respect to the l_∞-norm.

4. Prove Theorem (5.23).

5. Prove that the function $\| \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \|$

$el_\infty = max\{|x_1|, \ldots, |x_n|\}$ is a norm.

6. Prove that the topology defined on $\mathbb{R}^2$ by the l_2-norm and by the l_∞-norm are identical.

7. Prove that $(\mathbb{R}^n, \| \quad \|_1)$ is a Banach space.

8. Prove that $(\mathbb{R}^n, \| \quad \|_\infty)$ is a Banach space.

9. Prove Theorem (5.25).

10. Let $1 \leq p \leq \infty$. Let $\boldsymbol{e}_1, \boldsymbol{e}_2$ be the first two standard basis vectors of $\mathbb{R}^n$. Prove that $\| \boldsymbol{e}_1 + \boldsymbol{e}_2 \|_p^2 + \| \boldsymbol{e}_1 - \boldsymbol{e}_2 \|_p^2 = 2(\| \boldsymbol{e}_1 \|_p^2 + \| \boldsymbol{e}_2 \|_p^2)$ if and only if $p=2$.

11. Prove Lemma (5.6).

This page intentionally left blank

6

Linear Operators on Inner Product Spaces

CONTENTS

In this chapter we study two special types of operators on an inner product space: self-adjoint and normal. We completely characterize these operators and determine how the underlying space decomposes with respect to such an operator. In the first section we assume that $(V, \langle\ ,\ \rangle)$ is a finite-dimensional inner product space and we define the concepts of a normal and self-adjoint operator. Many properties of normal and self-adjoint operators are uncovered in preparation for proving the spectral theorems. We also characterize the matrix of normal and self-adjoint operators with respect to an orthonormal basis. In the second section we characterize self-adjoint operators on a finite-dimensional inner product spaces as well as normal operators on a finite-dimensional complex inner product space. In particular, we show that these operators are diagonalizable with respect to an orthonormal basis. This has consequences for the similarity classes of Hermitian and real symmetric matrices. In section three we consider a normal, but not self-adjoint, operator on a finite-dimensional real inner product space. The most important result is that T is completely reducible. From this we will be able to deduce that a real normal operator has a particularly nice generalized Jordan canonical form with respect to an orthonormal basis. In section four we define the concept of an isometry on an inner product space and obtain several characterizations. It is shown that the collection of isometries on an inner product space is a group. When the inner product space is real, this is the orthogonal group; when it is complex it is the unitary group. In the last section, we introduce the notion of a positive operator on a inner product space $(V, \langle\ ,\ \rangle)$. We characterize the positive operators and show that every positive operator has a unique positive square root. We make use of the square root to get the polar decomposition of an arbitrary operator and then prove the singular value theorem for real and complex linear transformations.

6.1 Self-Adjoint and Normal Operators

Throughout this section, we assume that $(V, \langle\ ,\ \rangle)$ is a finite-dimensional inner product space. We define the concepts of a normal and self-adjoint operator on a finite-dimensional inner product space. Many properties of normal and self-adjoint operators are uncovered in preparation for proving the spectral theorems of the next section. The matrix of a normal or self-adjoint operator with respect to an orthonormal basis is characterized.

What You Need to Know

You will need to have mastery of the following concepts to make sense of the material in this section: real and complex inner product space, orthonormal basis of a finite-dimensional inner product space, linear operator, adjoint of a linear operator on an inner product space, and the matrix of a linear operator on a finite-dimensional vector space with respect to a basis.

We begin with several definitions of various types of operators in real and complex inner product spaces. We then spend the rest of the section uncovering the basic properties of these operators.

Definition 6.1 *An operator $T \in \mathcal{L}(V, V)$ is said to be* **self-adjoint** *if $T^* = T$. A complex self-adjoint operator is referred to as a* **Hermitian** *operator; a real self-adjoint operator is called a* **symmetric** *operator.*

Remark 6.1 *For any operator T on V, the product T^*T is self-adjoint by parts iii) and iv) of Theorem (5.20).*

Definition 6.2 *Let T be an operator on a complex inner product space $(V, \langle\ ,\ \rangle)$. If $T^* = -T$, then T is said to be* **skew-Hermitian**. *If $(V, \langle\ ,\ \rangle)$ is a real inner product space and $T^* = -T$, then T is* **skew-symmetric**.

Definition 6.3 *Let A be an $n \times n$ complex matrix. Then A is a* **Hermitian** *matrix if $A^{tr} = \overline{A}$. A real Hermitian matrix satisfies $A^{tr} = A$ and is a* **symmetric** *matrix.*

Our very first theorem connects self-adjoint operators with Hermitian matrices.

Theorem 6.1 *Let $T \in \mathcal{L}(V,V)$ and $\mathcal{B} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ be a orthonormal basis. Then T is self-adjoint if and only if $\mathcal{M}_T(\mathcal{B},\mathcal{B})$ is a Hermitian matrix.*

Proof *Set $A = \mathcal{M}_T(\mathcal{B},\mathcal{B})$. By Theorem (5.22), the matrix of T^* with respect to $\mathcal{B}$ is given by $\mathcal{M}_{T^*}(\mathcal{B},\mathcal{B}) = \overline{A}^{tr}$. If A is Hermitian then $\mathcal{M}_T(\mathcal{B},\mathcal{B}) = \mathcal{M}_{T^*}(\mathcal{B},\mathcal{B})$ so that $T = T^*$. If $T = T^*$ then $\overline{A}^{tr} = \mathcal{M}_{T^*}(\mathcal{B},\mathcal{B}) = \mathcal{M}_T(\mathcal{B},\mathcal{B}) = A$ and A is a Hermitian matrix.*

Our next result constrains the kinds of eigenvalues a self-adjoint operator can have, more specifically, they must be real.

Theorem 6.2 *Let T be a self-adjoint operator on V, and let λ an eigenvalue of T. Then $\lambda \in \mathbb{R}$.*

Proof *Assume $\mathbf{0} \neq \boldsymbol{v}$ is a eigenvector of T with eigenvalue λ. Then*

$$\begin{aligned}\lambda \parallel \boldsymbol{v} \parallel^2 &= \langle \lambda\boldsymbol{v}, \boldsymbol{v}\rangle = \langle T(\boldsymbol{v}), \boldsymbol{v}\rangle = \langle \boldsymbol{v}, T^*(\boldsymbol{v})\rangle \\ &= \langle \boldsymbol{v}, T(\boldsymbol{v})\rangle = \langle \boldsymbol{v}, \lambda\boldsymbol{v}\rangle = \overline{\lambda}\langle \boldsymbol{v}, \boldsymbol{v}\rangle = \overline{\lambda} \parallel \boldsymbol{v} \parallel^2 .\end{aligned}$$

Since $\boldsymbol{v} \neq \mathbf{0}, \parallel \boldsymbol{v} \parallel \neq 0$, and consequently, $\lambda = \overline{\lambda}$ so that λ is real.

Corollary 6.1 *Let A be an $n \times n$ Hermitian matrix. Then the eigenvalues of A are real.*

Proof *Let $(V, \langle\ ,\ \rangle)$ be a complex inner product space and $\mathcal{S}$ an orthonormal basis of V. Let T be the operator on V such that $\mathcal{M}_T(\mathcal{S},\mathcal{S}) = A$. Then by Theorem (6.1), T is a self-adjoint operator. By Theorem (6.2), the eigenvalues of T are real. Then by Exercise 15 of Section (4.1) the eigenvalues of A are real.*

Remark 6.2 *Since a real symmetric matrix is a Hermitian matrix it is a consequence of Corollary (6.1) that the eigenvalues of a real symmetric matrix are real.*

In our next definition, we introduce another important class of operators, which includes self-adjoint operators.

Definition 6.4 *Let T be an operator on an inner product space $(V, \langle\ ,\ \rangle)$. T is* **normal** *if T and T^* commute: $TT^* = T^*T$. Clearly self-adjoint operators are normal.*

The next lemma will be crucial for proving the complex spectral theorem.

Lemma 6.1 *Let $(V, \langle\ ,\ \rangle)$ be a complex inner product space and $T : V \to V$ a normal operator. Then there exists a non-zero vector $\boldsymbol{v}$, which is an eigenvector for T and for T^*. Moreover, if $T(\boldsymbol{v}) = \lambda\boldsymbol{v}$, then $T^*(\boldsymbol{v}) = \overline{\lambda}\boldsymbol{v}$.*

Proof *Since T is an operator on a complex space there is a $\lambda \in \mathbb{C}$ such that $V_\lambda = \{\boldsymbol{u} \in V | T(\boldsymbol{u}) = \lambda\boldsymbol{u}\} \neq \{\boldsymbol{0}\}$. Assume $\boldsymbol{u} \in V_\lambda$. Then $T(T^*(\boldsymbol{u})) = (TT^*)(\boldsymbol{u}) = (T^*T)(\boldsymbol{u})$, the latter since $TT^* = T^*T$. However, $(T^*T)(\boldsymbol{u}) = T^*(T(\boldsymbol{u})) = T^*(\lambda\boldsymbol{u}) = \lambda T^*(\boldsymbol{u})$. We have therefore shown that V_λ is T^*-invariant. Again, since the field is the complex numbers, the operator T^* restricted to V_λ must have a non-zero eigenvector, $\boldsymbol{v}$. It remains to show that $T^*(\boldsymbol{v}) = \overline{\lambda}(\boldsymbol{v})$. Assume $T^*(\boldsymbol{v}) = \beta\boldsymbol{v}$. We then have*

$$\begin{aligned} \lambda\langle \boldsymbol{v}, \boldsymbol{v}\rangle &= \langle \lambda\boldsymbol{v}, \boldsymbol{v}\rangle = \langle T(\boldsymbol{v}), \boldsymbol{v}\rangle \\ &= \langle \boldsymbol{v}, T^*(\boldsymbol{v})\rangle = \langle \boldsymbol{v}, \beta\boldsymbol{v}\rangle = \overline{\beta}\langle \boldsymbol{v}, \boldsymbol{v}\rangle. \end{aligned}$$

It now follows that $\overline{\beta} = \lambda$, so $\beta = \overline{\lambda}$.

Exercises

1. Prove if $S, T \in \mathcal{L}(V, V)$ are self-adjoint then $S + T$ is self-adjoint.

2. Prove if T is self-adjoint and $\gamma \in \mathbb{R}$ then γT is self-adjoint.

3. Let T be an arbitrary operator on a finite-dimensional inner product space $(V, \langle\ ,\ \rangle)$. Set $R = \frac{1}{2}(T^* + T), S = \frac{1}{2}i(-T + T^*)$. Prove the following:

i. R and S are self adjoint;

ii. $T = R + iS$; and

iii. if $T = R_1 + iS_1$, where R_1, S_1 are self-adjoint, then $R_1 = R, S_1 = S$.

4. Let T be an arbitrary operator on a finite-dimensional inner product space $(V, \langle\ ,\ \rangle)$. Set $R = \frac{1}{2}(T^* + T), S = \frac{i}{2}(-T + T^*)$. Prove that T is normal if and only if $RS = SR$.

5. By Exercises 1 and 2, the collection of self-adjoint operators in $\mathcal{L}(V, V)$ is a real vector space. If $dim(V) = n$, determine the dimension of this space.

6. Let $(V, \langle\ ,\ \rangle)$ be an inner product space and $S, T \in \mathcal{L}(V, V)$ be self-adjoint operators. Prove ST is self-adjoint if and only if $ST = TS$.

7. Let $(V, \langle\ ,\ \rangle)$ be an inner product space. Give an example of self-adjoint operators $S, T \in \mathcal{L}(V, V)$ such that ST is not self-adjoint.

8. Let $T \in \mathcal{L}(V, V)$ be a normal operator. Prove that $\parallel T(\boldsymbol{v}) \parallel = \parallel T^*(\boldsymbol{v}) \parallel$ for every $\boldsymbol{v} \in V$.

9. Let $T \in \mathcal{L}(V, V)$ be a normal operator. Prove that $Ker(T) = Ker(T^*)$.

10. Assume $T \in \mathcal{L}(V, V)$ is normal. Prove that $Range(T) = Range(T^*)$.

11. Let T be an operator on the finite-dimensional inner product space $(V, \langle\ ,\ \rangle)$ and assume that $TT^* = T^2$. Prove that T is self-adjoint.

12. Assume T is a normal operator on the inner product space $(V, \langle\ ,\ \rangle)$ and that T is nilpotent. Prove $T = \mathbf{0}_{V \to V}$.

13. Assume T is normal and λ is a scalar. Prove that $T - \lambda I_V$ is normal.

14. Let $(V, \langle\ ,\ \rangle)$ be an inner product space and $V = U \oplus W$ a direct sum. Set $T = Proj_{(U,W)}$. Prove that the following are equivalent:

i. T is normal;

ii. $W = U^{\perp}$;

iii. T is self-adjoint.

6.2 Spectral Theorems

In this section we prove the real and complex spectral theorems. The real spectral theorem states that an operator T on a finite-dimensional real inner product space $(V, \langle\ ,\ \rangle)$ is self-adjoint if and only if there exists an orthonormal basis $\mathcal{B}$ of V consisting of eigenvectors for T. The complex spectral theorem states that an operator T on a finite-dimensional complex inner product space $(V, \langle\ ,\ \rangle)$ is normal if and only if there exists an orthonormal basis $\mathcal{B}$ of V consisting of eigenvectors for T

What You Need to Know

To make sense of the material in this section it is essential that you have mastery of the following concepts: real inner product space, complex inner product space, orthogonal complement of a subspace of an inner product space, operator on a vector space, an invariant subspace of an operator on a vector space, completely reducible operator on a vector space, adjoint of a linear operator on an inner product space, self-adjoint operator on an inner product space, normal operator on an inner product space, orthonormal basis of a finite-dimensional inner product space, and an eigenvector and eigenvalue of an operator on a vector space.

We begin with a definition:

Definition 6.5 *Let V be a finite-dimensional vector space. An operator T on V is* **diagonalizable** *if there is a basis $\mathcal{B}$ for V such that $\mathcal{M}_T(\mathcal{B}, \mathcal{B})$ is a diagonal matrix. This is equivalent to the existence of a basis for V consisting of eigenvectors of T.*

If V is equipped with an inner product then T is **orthogonally diagonalizable** *if there is an orthonormal basis $\mathcal{S}$ of V such that $\mathcal{M}_T(\mathcal{S}, \mathcal{S})$ is a diagonal matrix. This is equivalent to the existence of an orthonormal basis of V consisting of eigenvectors of T.*

Our first result establishes that complex normal operators are orthogonally diagonalizable. This result is referred to as the *complex spectral theorem.*

Theorem 6.3 *Let $(V, \langle\ ,\ \rangle)$ be a complex inner product space and T an operator on V. Then T is normal if and only if T is orthogonally diagonalizable.*

Proof *Assume T is orthogonally diagonalizable and $\mathcal{S} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ is an orthonormal basis of V consisting of eigenvectors for T. Then $\mathcal{M}_T(\mathcal{S}, \mathcal{S}) = diag\{\lambda_1, \dots, \lambda_n\}$ for complex numbers $\lambda_1, \dots, \lambda_n$. Then $\mathcal{M}_{T^*}(\mathcal{S}, \mathcal{S}) = diag\{\overline{\lambda_1}, \dots, \overline{\lambda_n}\}$. It follows that $\mathcal{M}_T(\mathcal{S}, \mathcal{S})$ and $\mathcal{M}_{T^*}(\mathcal{S}, \mathcal{S})$ commute since any two diagonal matrices commute, whence T and T^* commute and T is normal.*

Conversely, assume that T is normal. We prove that T is orthogonally diagonalizable by induction on $dim(V)$. If $dim(V) = 1$, there is nothing to prove. So assume the result is true for complex inner product spaces of dimension $n-1$ and that $dim(V) = n$. By Lemma (6.1), there exists a non-zero vector $\boldsymbol{v}$ and scalar $\lambda \in \mathbb{C}$ such that $T(\boldsymbol{v}) = \lambda\boldsymbol{v}$ and $T^*(\boldsymbol{v}) = \overline{\lambda}\boldsymbol{v}$. Replacing $\boldsymbol{v}$ by $\frac{1}{\|\boldsymbol{v}\|}\boldsymbol{v}$ we may assume that $\boldsymbol{v}$ is a unit vector.

Since $\boldsymbol{v}$ is an eigenvector for T^*, $Span(\boldsymbol{v})$ is T^*-invariant. Then by Exercise 10 of Section (5.6), $\boldsymbol{v}^\perp$ is T-invariant since $(T^*)^* = T$. Since $\boldsymbol{v}$ is also an eigenvector for $T, Span(\boldsymbol{v})$ is T-invariant and again by Exercise 10 of Section (5.6) $\boldsymbol{v}^\perp$ is T^*-invariant.

Let $\widehat{T}$ be the restriction of T to $\boldsymbol{v}^\perp$ and, similarly, let $\widehat{T^*}$ be the restriction of T^* to $\boldsymbol{v}^\perp$. We claim that $\widehat{T}$ is normal and toward that end we show that $(\widehat{T})^* = \widehat{T^*}$ and $\widehat{T}$ commutes with $(\widehat{T})^*$.

Let $\boldsymbol{u}, \boldsymbol{w} \in \boldsymbol{v}^\perp$. Then $\langle \boldsymbol{u}, (\widehat{T})^*(\boldsymbol{w})\rangle = \langle \widehat{T}(\boldsymbol{u}), \boldsymbol{w}\rangle = \langle T(\boldsymbol{u}), \boldsymbol{w}\rangle = \langle \boldsymbol{u}, T^*(\boldsymbol{w})\rangle$. It follows from this that for all $\boldsymbol{u}, \boldsymbol{w} \in \boldsymbol{v}^\perp$ we have $\langle \boldsymbol{u}, (\widehat{T^*} - (\widehat{T})^*)(\boldsymbol{w})\rangle = 0$. This implies that $(\widehat{T^*} - (\widehat{T})^*)(\boldsymbol{w}) = 0$ for all $\boldsymbol{w} \in \boldsymbol{v}^\perp$ and therefore $(\widehat{T})^* = \widehat{T^*}$ on $\boldsymbol{v}^\perp$. Since T and T^* commute, it follows that $\widehat{T}$ and $(\widehat{T})^*$ commute and therefore $\widehat{T}$ is normal.

As a consequence of the normality of $\widehat{T}$, we can apply the induction hypothesis: there is a orthonormal basis of $\boldsymbol{v}^\perp, (\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_{n-1})$ consisting of eigenvectors for T. Set $\boldsymbol{v}_n = \boldsymbol{v}$. Since $Span(\boldsymbol{v}) \cap \boldsymbol{v}^\perp = \{\boldsymbol{0}\}, \boldsymbol{v} \notin Span(\boldsymbol{v}_1, \dots, \boldsymbol{v}_{n-1})$. Then $(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n)$ is linearly independent and thus a basis for V. Since $\boldsymbol{v}_j \perp \boldsymbol{v}_n$ for $j < n$, and $\boldsymbol{v}_n$ is a unit vector, $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ is an orthonormal basis. We have thus shown that there exists an orthonormal basis of V consisting of eigenvectors for T.

We now move on to the real spectral theorem. We begin by proving that a real self-adjoint operator has an eigenvector.

Lemma 6.2 *Let $(V, \langle\ ,\ \rangle)$ be a real inner product space and $T \in \mathcal{L}(V, V)$ be a self-adjoint operator on V. Then T has an eigenvector.*

Proof *Let $\mathcal{S}$ be an orthonormal basis of V and set $A = \mathcal{M}_T(\mathcal{S}, \mathcal{S})$. By Remark (6.2) the eigenvalues of A are real. Let λ be an eigenvalue of A. Then*

$A-\lambda I_n$ is a singular matrix and hence there exists a real $n \times 1$ matrix X such that $(A-\lambda I_n)X = 0_{n\times 1}$. If $\boldsymbol{v}$ is the vector in V such that $[\boldsymbol{v}]_{\mathcal{S}} = X$, then $T(\boldsymbol{v}) = \lambda \boldsymbol{v}$ and $\boldsymbol{v}$ is an eigenvector of T with eigenvalue λ.

Theorem 6.4 *Let $(V, \langle\ ,\ \rangle)$ be a real inner product space and $T \in \mathcal{L}(V,V)$. Then T is self-adjoint if and only if T is orthogonally diagonalizable.*

Proof *Assume first that there exists an orthonormal basis of V consisting of eigenvectors for T. Then $A = \mathcal{M}_T(\mathcal{S},\mathcal{S})$ is a real diagonal matrix. It then follows that $A^{tr} = A$ and hence $T^* = T$.*

Conversely, assume that T is self-adjoint. We prove that T is orthogonally diagonalizable by induction on $dim(V)$. If $dim(V) = 1$, there is nothing to prove, so assume the result is true for spaces of dimension $n-1$ and that $dim(V) = n$. Let $\boldsymbol{v}$ be an eigenvector of T (which we may assume has norm one). Then $Span(\boldsymbol{v})$ is a T-invariant subspace and since T is self-adjoint it follows that $Span(\boldsymbol{v})^{\perp} = \boldsymbol{v}^{\perp}$ is T-invariant. Consider $\widehat{T}$, the restriction of T to $\boldsymbol{v}^{\perp}$. Let $\boldsymbol{u}, \boldsymbol{w} \in \boldsymbol{v}^{\perp}$. Then

$$\langle \widehat{T}(\boldsymbol{u}), \boldsymbol{w}\rangle = \langle T(\boldsymbol{u}), \boldsymbol{u}\rangle = \langle \boldsymbol{u}, T(\boldsymbol{u})\rangle = \langle \boldsymbol{u}, \widehat{T}(\boldsymbol{u})\rangle$$

and therefore $\widehat{T}$ is self-adjoint. By the inductive hypothesis, there exists an orthonormal basis $(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_{n-1})$ for $\boldsymbol{v}^{\perp}$ consisting of eigenvectors for $\widehat{T}$ (hence eigenvectors for T). If we set $\boldsymbol{v}_n = \boldsymbol{v}$, then $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ is an orthonormal basis for V consisting of eigenvectors for T.

Exercises

1. Assume T is a normal operator on a complex inner product space $(V, \langle\ ,\ \rangle)$. Prove that there exists a polynomial $g(x)$ such that $T^* = g(T)$.

2. Assume T is an operator on a complex inner product space $(V, \langle\ ,\ \rangle)$. Prove the following are equivalent:

i) T is normal.

ii) Every T-invariant subspace is T^*-invariant.

iii) If U is T-invariant, then $U^{\perp}$ is T-invariant.

3. Let T be the operator on $\mathbb{C}^2$ such that with respect to the standard orthonormal basis $\mathcal{S} = \left(\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right)$ the matrix of T is $\begin{pmatrix}4 & -i\\ i & 4\end{pmatrix}$. Verify that T is self-adjoint and find an orthonormal basis $\mathcal{B}$ such that $\mathcal{M}_T(\mathcal{B},\mathcal{B})$ is diagonal.

4. Let T be the operator on $\mathbb{R}^3$ such that with respect to the standard orthonormal basis $\mathcal{S}$ the matrix of T is the all 1 matrix, $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$. Find an orthonormal basis $\mathcal{B}$ such that $\mathcal{M}_T(\mathcal{B}, \mathcal{B})$ is diagonal.

5. Assume T is an operator on $\mathbb{R}^3$, that $\mathcal{B} = \left(\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} \right)$ is a basis of eigenvectors for T, and that the corresponding eigenvalues of T are the real numbers a, b, c. Prove that T is self-adjoint if and only if $b = c$.

6. Let T be an operator on $\mathbb{R}^4$ and assume $\left(\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} \right)$ are eigenvectors of T with eigenvalues 2, -3, and 4, respectively. Prove that T is self-adjoint if and only if $\begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix}$ is an eigenvector of T.

7. Let $(V, \langle\ ,\ \rangle)$ be a complex inner product space and T a normal operator on V. Prove that T is self-adjoint if and only if all eigenvalues of T are real.

8. Let $(V, \langle\ ,\ \rangle)$ be a finite inner product space, S, T commuting self-adjoint operators on V. Prove that there exists an orthonormal basis $\mathcal{B} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$, consisting of simultaneous eigenvectors for S and T.

9. Assume T is a normal operator on the complex finite-dimensional inner product space $(V, \langle\ ,\ \rangle)$. Prove that $Range(T^k) = Range(T)$ and $Ker(T^k) = Ker(T)$ for all natural numbers k.

10. Let T be a completely reducible operator on the finite complex inner product space $(V, \langle\ ,\ \rangle)$. Prove that there exists an inner product on V such that T is normal.

11. Let T be an operator on the finite-dimensional inner product $(V, \langle\ ,\ \rangle)$. Assume there exists an invariant subspace U of $V, U \neq V, \{\mathbf{0}\}$ such that $U^\perp$ is T-invariant and $T_{|_U}, T_{|_{U^\perp}}$ are self-adjoint. Prove that T is self-adjoint.

12. Prove or give a counterexample: Assume T is a self-adjoint operator on the finite-dimensional inner product space $(V, \langle\ ,\ \rangle)$ and U, W are T-invariant subspaces such that $V = U \oplus W$. Then $W = U^\perp$.

13. Assume T is an operator on the finite-dimensional inner product space V and the minimum polynomial of T is $x^2 - x$. Let $U = E_1$ be the subspace of fixed vectors and $W = Ker(T)$. Prove that T is self-adjoint if and only if $W = U^\perp$.

14. Assume T is a skew-Hermitian but not a Hermitian operator on a finite-dimensional complex inner product space V. Prove that the non-zero eigenvalues of T are pure imaginary.

15. Assume T is a self-adjoint operator on an inner product space $(V, \langle\ ,\ \rangle)$. Prove that $\langle T(\boldsymbol{u}), \boldsymbol{u}\rangle \in \mathbb{R}$ for all $\boldsymbol{u} \in V$.

6.3 Normal Operators on Real Inner Product Spaces

In this section we study normal operators on a finite-dimensional real inner product space which are not self-adjoint. We first prove that such an operator is completely reducible. We then go on to show that there exists an orthonormal basis, $\mathcal{B}$, such that $\mathcal{M}_T(\mathcal{B},\mathcal{B})$ has a particularly nice form.

What You Need to Know

You will need a mastery of the following concepts to successfully understand the new material of this section: real finite-dimensional inner product space, normal operator on an inner product space, self-adjoint operator on an inner product space, orthonormal basis of a finite-dimensional inner product space, matrix of an operator with respect to a basis, block diagonal matrix, completely reducible linear operator, and the generalized Jordan canonical form of an operator.

We begin with a couple of preparatory lemmas which we require to obtain our main structure theorem. Throughout this section, we assume that $(V, \langle\ ,\ \rangle)$ is a finite-dimensional real inner product space.

Lemma 6.3 *Let T be a normal operator on V. Then for all vectors $\boldsymbol{v} \in V$, $\parallel T(\boldsymbol{v}) \parallel = \parallel T^*(\boldsymbol{v}) \parallel$.*

Proof $\parallel T(\boldsymbol{v}) \parallel^2 = \langle T(\boldsymbol{v}), T(\boldsymbol{v})\rangle = \langle \boldsymbol{v}, (T^*T)(\boldsymbol{v})\rangle = \langle \boldsymbol{v}, (TT^*)(\boldsymbol{v})\rangle = \langle T^*(\boldsymbol{v}), T^*(\boldsymbol{v})\rangle = \parallel T^*(\boldsymbol{v}) \parallel^2$.

Corollary 6.2 *Let T be a normal operator on V and assume that $\boldsymbol{v}$ is an eigenvector of T with eigenvalue λ. Then $\boldsymbol{v}$ is an eigenvector of T^* with eigenvalue λ.*

Proof *Since T is normal the operator $T - \lambda I_V$ is normal by Exercise 13 of Section (6.1). Moreover, since λ is real, $(T - \lambda I_V)^* = T^* - \lambda I_V$. We now have*

$$0 = \parallel (T - \lambda I_V)(\boldsymbol{v}) \parallel = \parallel (T^* - \lambda I_V)(\boldsymbol{v}) \parallel$$

and therefore $T^*(\boldsymbol{v}) = \lambda \boldsymbol{v}$.

Lemma 6.4 *Let $(V, \langle,\rangle)$ be a finite-dimensional real inner product space and T be a normal operator on V. Assume U is a T-invariant subspace of V. Then the following hold:*

i) $U^\perp$ is $T-$invariant.

ii) U is T^*-invariant.

iii) $(T_{|U})^* = (T^*)_{|U}$.

iv) $(T_{|U^\perp})^* = (T^*)_{|U^\perp}$.

v) $T_{|U}$ is normal.

vi) $T_{|U^\perp}$ is normal.

Proof *i) Let $(\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k)$ be an orthonormal basis for U and extend it to an orthonormal basis $\mathcal{S} = (\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n)$ of V. Set $A = \mathcal{M}_T(\mathcal{S}, \mathcal{S})$. Since U is T-invariant, for each $j \leq k$ it follows that $T(\boldsymbol{u}_j) \in U$ and consequently, $T(\boldsymbol{u}_j)$ is a linear combination of $(\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k)$. It follows from this that each $A[\boldsymbol{u}_j]_{\mathcal{S}}$ is a linear combination of $([\boldsymbol{u}_1]_{\mathcal{S}}, [\boldsymbol{u}_2]_{\mathcal{S}}, \ldots, [\boldsymbol{u}_k]_{\mathcal{S}})$.*

We note that $\mathcal{M}_{T^*}(\mathcal{S}, \mathcal{S}) = A^{tr}$. Since $\mathcal{M}_{TT^*}(\mathcal{S}, \mathcal{S}) = AA^{tr}, \mathcal{M}_{T^*T}(\mathcal{S}, \mathcal{S}) = A^{tr}A$, and T is normal, it follows that $AA^{tr} = A^{tr}A$.

Let $(W, \langle\ ,\ \rangle)$ be an n-dimensional complex inner product space with an orthonormal basis $\mathcal{S}_W = (\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_n)$. Let T_W be the operator on W such that $\mathcal{M}_{T_W}(\mathcal{S}_W, \mathcal{S}_W) = A$. It then follows that $\mathcal{M}_{T_W^*}(\mathcal{S}_W, \mathcal{S}_W) = \overline{A}^{tr} = A^{tr}$ since A is a real matrix. Since $AA^{tr} = A^{tr}A$ we can conclude that T_W is normal.

Let X be the subspace of W spanned by $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k)$. By construction, $[T_W(\boldsymbol{w}_j)]_{\mathcal{S}_W} = [T(\boldsymbol{u}_j)]_{\mathcal{S}}$. In particular, since $T(\boldsymbol{u}_j)$ is a linear combination of $(\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k)$ for $j \leq k$, it follows that $T_W(\boldsymbol{w}_j)$ is a linear combination of $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k)$ for $j \leq k$. Therefore, X is a T_W-invariant subspace of W. Since T_W is normal we can conclude by Exercise 2 of Section (6.2) that $X^\perp$ is T_W-invariant. In particular, for $j > k$ the coordinate vector $[T_W(\boldsymbol{w}_j)]_{\mathcal{S}_W}$ begins with k 0's. However, $[T_W(\boldsymbol{w}_j)]_{\mathcal{S}_W} = [T(\boldsymbol{u}_j)]_{\mathcal{S}}$, which implies for $j > k, T(\boldsymbol{u}_j) \in Span(\boldsymbol{u}_{k+1}, \ldots, \boldsymbol{u}_n) = U^\perp$. Thus, $U^\perp$ is T-invariant as claimed.

ii) Since $U^\perp$ is T-invariant by i) it follows that $U = (U^\perp)^\perp$ is T^*-invariant.

iii) Let $S = T_{|U}$ and $\boldsymbol{u}, \boldsymbol{v} \in U$. Then $\langle S(\boldsymbol{u}), \boldsymbol{v}\rangle = \langle T(\boldsymbol{u}), \boldsymbol{v}\rangle = \langle \boldsymbol{u}, T^*(\boldsymbol{v})\rangle$. Since $T^*(\boldsymbol{v}) \in U$ it follows that $S^* = (T^*)_{|U}$.

iv) The proof of this is exactly the same as iii).

v) This follows from iii) and the fact that T is normal.

vi) This follows from iv) and the fact that T is normal.

Since for any subspace U of an inner product space $(V, \langle\ ,\ \rangle), V = U \oplus U^\perp$ the following is an immediate consequence of Lemma (6.4):

Corollary 6.3 *Let T be normal operator on the real inner product space $(V, \langle\ ,\ \rangle)$. Then T is completely reducible.*

As a consequence of Corollary (6.3), if $U = \langle T, \boldsymbol{u}\rangle$ is indecomposable, then $\mu_{T,\boldsymbol{u}}(x)$ is an irreducible polynomial. This then implies that $\mu_{T,\boldsymbol{u}}(x)$ is either a linear polynomial, $x - \lambda$, or else a quadratic of the form $x^2 + bx + c$, where $b^2 - 4c < 0$. We will show that the matrix of $T_{|U}$ with respect to an orthonormal basis of U takes a particularly simple form.

Lemma 6.5 *Assume that $(V, \langle\ ,\ \rangle)$ is a two-dimensional real inner product space. Then the following are equivalent:*

1) T is normal but not self-adjoint.

2) There exists an orthonormal basis $\mathcal{S}$ for V such that $\mathcal{M}_T(\mathcal{S}, \mathcal{S}) = \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix}$, where $\beta > 0$.

Proof *1) implies 2). Assume T is normal and let $\mathcal{S} = (\boldsymbol{v}_1, \boldsymbol{v}_2)$ be an orthonormal basis and assume $A = \mathcal{M}_T(\mathcal{S}, \mathcal{S}) = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$. Then $\mathcal{M}_{T^*}(\mathcal{S}, \mathcal{S}) = A^{tr} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$.*

Since T is normal,

$$\alpha^2 + \beta^2 = \| T(\boldsymbol{v}_1) \|^2 = \| T^*(\boldsymbol{v}_1) \|^2 = \alpha^2 + \gamma^2.$$

It then follows that $\beta^2 = \gamma^2$. If $\beta = \gamma$, then $A = A^{tr}$ and T is self-adjoint, contrary to assumption. Therefore, $\gamma = -\beta$.

Since T is normal, we must have

$$\begin{pmatrix} \alpha & -\beta \\ \beta & \delta \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ -\beta & \delta \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ -\beta & \delta \end{pmatrix} \begin{pmatrix} \alpha & -\beta \\ \beta & \delta \end{pmatrix}$$

$$\begin{pmatrix} \alpha^2 + \beta^2 & \beta(\alpha - \delta) \\ \beta(\alpha - \delta) & \beta^2 + \delta^2 \end{pmatrix} = \begin{pmatrix} \alpha^2 + \beta^2 & \beta(\delta - \alpha) \\ \beta(\delta - \alpha) & \beta^2 + \delta^2 \end{pmatrix}.$$

Then $\beta(\alpha - \delta) = \beta(\delta - \alpha)$. If $\beta = 0$, then A is symmetric, contrary to assumption. Therefore $\alpha - \delta = \delta - \alpha$, which implies that $\alpha = \delta$.

It remains to show that we can choose the basis such that $\beta > 0$. Of course, if $\beta > 0$ there is nothing more to do, so assume $\beta < 0$.

In this case, replace $\mathcal{S}$ with $\mathcal{S}' = (\boldsymbol{v}_1, -\boldsymbol{v}_2)$. Then $\mathcal{M}_T(\mathcal{S}', \mathcal{S}') = \begin{pmatrix} \alpha & -\delta \\ \delta & \alpha \end{pmatrix}$, where $\delta = -\beta > 0$.

2) implies 1): If $\mathcal{M}_T(\mathcal{S},\mathcal{S}) = A = \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix}$, then $\mathcal{M}_{T^*}(\mathcal{S},\mathcal{S}) = A^{tr} = \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}$. By straightforward multiplication we obtain

$$AA^{tr} = \begin{pmatrix} \alpha^2+\beta^2 & 0 \\ 0 & \alpha^2+\beta^2 \end{pmatrix} = A^{tr}A.$$

Since $\mathcal{M}_{TT^*}(\mathcal{S},\mathcal{S}) = \mathcal{M}_{T^*T}(\mathcal{S},\mathcal{S})$ it follows that $TT^* = T^*T$ and T is normal.

We now get a characterization of normal operators, which are not self-adjoint, on a real inner product space:

Theorem 6.5 *Let T be an operator on $(V, \langle\ ,\ \rangle)$, a finite-dimensional real inner product space. Then the following are equivalent:*

1) T is normal and not self-adjoint.

2) There is an orthonormal basis $\mathcal{S}$ such that $\mathcal{M}_T(\mathcal{S},\mathcal{S})$ is a block diagonal matrix and each diagonal block is either $1 times 1$ or 2×2 of the form $\begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix}$ where $\beta > 0$. Moreover, some block is 2×2.

Proof *We first prove that 2) implies 1). It is straightforward to see that if $\mathcal{S}$ is an orthonormal basis and $A = \mathcal{M}_T(\mathcal{S},\mathcal{S})$ has the given form, then A^{tr} commutes with A: A^{tr} is also block diagonal and it has 1×1 blocks where A does with identical entries and these clearly commute. Where A has a 2×2 matrix $\begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix}$, A^{tr} has the block $\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}$ and, as we have previously seen in Lemma (6.5), these two matrices commute. Since A and A^{tr} commute it follows that T and T^* commute.*

1) implies 2). The proof is by the second principle of mathematical induction on dim(V). The first non-trivial case is dim$(V) = 2$. This is the content of Lemma (6.5). So assume that dim$(V) = n > 2$ and the result is true for any normal, non-self-adjoint operator acting on a real inner product space of dimension less than n.

Suppose T has an eigenvector, $\boldsymbol{v}$, with eigenvalue λ. Without loss of generality, we can assume $\parallel \boldsymbol{v} \parallel = 1$. By Corollary (6.2), $\boldsymbol{v}$ is an eigenvector for T^* and by Lemma (6.4), $\boldsymbol{v}^\perp$ is T-invariant and T^*-invariant. Moreover, $T_{|\boldsymbol{v}^\perp}$ is normal. By the induction hypothesis, there exists an orthonormal basis $\mathcal{S} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{n-1})$ of $\boldsymbol{v}^\perp$ such that the matrix B of $T_{|\boldsymbol{v}^\perp}$ with respect to $\mathcal{S}$ is block diagonal with each diagonal block is 1×1 or 2×2 of the form $\begin{pmatrix} \alpha & -\beta \\ \beta & a \end{pmatrix}$. Set $\boldsymbol{v}_n = \boldsymbol{v}$ and $\mathcal{S}' = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$. Then

$$\mathcal{M}_T(\mathcal{S}',\mathcal{S}') = \begin{pmatrix} B & 0_{n-1\times 1} \\ 0_{1\times n-1} & \lambda \end{pmatrix}.$$

Note if all the blocks are 1×1 then the matrix is symmetric and the operator T is self-adjoint. Therefore, at least one block is 2×2 and the matrix has the required form.

Assume then that T does not have an eigenvector. Let U be a T-invariant subspace with dim(U) minimal. Then as V is a real vector space and T is completely reducible, as previously remarked, dim$(U) = 2$. By Lemma (6.4), $U^\perp$ is T-invariant and T^*-invariant and $T_{|U}, T_{|U^\perp}$ are normal. It follows from Lemma (6.5) that there is an orthonormal basis $\mathcal{S}_U$ for U such that $A = \mathcal{M}_{T_{|U}}(\mathcal{S}_U,\mathcal{S}_U) = \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix}$ with $\beta > 0$. Since dim$(U^\perp) <$ dim(V), $T_{|U^\perp}$ is normal, and $T_{|U}$ has no eigenvectors, it follows that there is an orthonormal basis $\mathcal{S}_{U^\perp}$ for $U^\perp$ such that $B = \mathcal{M}_{T_{|U^\perp}}(\mathcal{S}_{U^\perp},\mathcal{S}_{U^\perp})$ is block diagonal and every block is of the form $\begin{pmatrix} \gamma & -\delta \\ \delta & \gamma \end{pmatrix}$ where $\delta > 0$. Set $\mathcal{S} = \mathcal{S}_U \sharp \mathcal{S}_{U^\perp}$. Then $\mathcal{S}$ is an orthonormal basis of V and

$$\mathcal{M}_T(\mathcal{S},\mathcal{S}) = \begin{pmatrix} A & 0_{2\times n-2} \\ 0_{n-2\times 2} & B \end{pmatrix},$$

which has the required form.

Exercises

1. Give an example of a normal operator T on a four-dimensional real inner product space, which does not have an eigenvector and has exactly four invariant subspaces.

2. Give an example of a normal operator T on a four-dimensional real inner product space such that i) T has no eigenvectors, and ii) T has infinitely many invariant subspaces.

3. Let $(V, \langle\ ,\ \rangle)$ be a real inner product space of dimension two and $T \in \mathcal{L}(V,V)$ a normal operator, which is not self-adjoint. Prove that there is a real linear polynomial $f(x)$ such that $T^* = f(T)$.

4. Let $(V, \langle\ ,\ \rangle)$ be a real inner product space and $T \in \mathcal{L}(V,V)$ a normal operator. Assume that the minimal polynomial of T is a real irreducible quadratic. Prove that there is a real linear polynomial $f(x)$ such that $T^* = f(T)$.

5. Let $(V, \langle\ ,\ \rangle)$ be a real inner product space and $T \in \mathcal{L}(V,V)$ a normal operator, which is not self-adjoint. Prove there is a polynomial $f(x)$ such that $T^* = f(T)$.

6. Let $(V, \langle\ ,\ \rangle)$ be a real inner product space and $T \in \mathcal{L}(V,V)$ a normal

operator, which is not self-adjoint. Let $S \in \mathcal{L}(V,V)$. Prove that $TS = ST$ if and only if $ST^* = T^*S$.

7. Let $(V, \langle\ ,\ \rangle)$ be a real inner product space of dimension 2 and $T \in \mathcal{L}(V,V)$ a normal operator, which is not self-adjoint. Assume $S \in \mathcal{L}(V,V)$ commutes with T. Prove that S is a linear combination of T and I_V and consequently normal.

8. Let T be a normal operator on the real finite-dimensional inner product space V and assume all the eigenvalues of T are complex and distinct. Let $S \in \mathcal{L}(V,V)$ commute with T, that is, $ST = TS$. Prove if U is a T-invariant subspace, then U is S-invariant.

9. Let T be a normal operator on a real finite-dimensional inner product space and assume all the eigenvalues of T are complex and distinct. Let $S \in \mathcal{L}(V,V)$ commute with T, that is, $ST = TS$. Prove that S is normal.

10. Let T be a normal operator on the real finite-dimensional inner product space and assume all the eigenvalues of T are complex and distinct. Set $C(T) = \{S \in \mathcal{L}(V,V) | ST = TS\}$. Prove that $dim(C(T)) = dim(V)$ and is even.

11. Assume T is a normal operator on $\mathbb{R}^4$ equipped with the dot product and assume the minimal polynomial of T is $x^2 - 2x + 3$. Determine $dim(C(T))$.

12. Assume T is an invertible skew-symmetric operator on a finite-dimensional real inner product space $(V, \langle\ ,\ \rangle)$. Prove that every eigenvalue of T is purely imaginary.

6.4 Unitary and Orthogonal Operators

In this section we define the notion of an isometry of an inner product space and prove that the collection of all isometries on an inner product space $(V, \langle\ ,\ \rangle)$ is a group. We then go on to characterize the isometries of a finite-dimensional inner product space.

What You Need to Know

You will need to have a mastery of the following concepts: inner product space, orthonormal basis of a finite-dimensional inner product space, self-adjoint operator on an inner product space, matrix of a linear transformation, and eigenvalues and eigenvectors of an operator. Also, you should be familiar with the concept of a group, which can be found in Appendix B.

We begin with a definition:

Definition 6.6 *Let $(V, \langle\ ,\ \rangle)$ be a finite-dimensional inner product space. An operator T on V is an* **isometry** *if for all $\boldsymbol{v} \in V, \parallel T(\boldsymbol{v}) \parallel = \parallel \boldsymbol{v} \parallel$. An isometry of a complex inner product space is also referred to as a* **unitary operator** *and an isometry of a real inner product space is called an* **orthogonal operator**.

The following theorem is a simple application of the definition:

Theorem 6.6 *Let $(V, \langle\ ,\ \rangle)$ be a finite-dimensional inner product space. Then the following hold:*

i) If T is an isometry then T is bijective and T^{-1} is also an isometry.

ii) If S, T are isometries then ST is an isometry.

We leave these as exercises.

Remark 6.3 *It is a consequence of Theorem (6.6) that the collection of all isometries of an inner product space $(V, \langle\ ,\ \rangle)$ is a* **group**. *When V is real we denote this group by $O(V, \langle\ ,\ \rangle)$ and when the space complex by $U(V, \langle\ ,\ \rangle)$.*

Before proceeding to our first main result, we need a lemma concerning complex inner products.

Lemma 6.6 *Let $(V, \langle\ ,\ \rangle)$ be a complex inner product space and $\boldsymbol{u}, \boldsymbol{v} \in V$. Then the following hold:*

i) $\parallel \boldsymbol{u} + \boldsymbol{v} \parallel^2 - \parallel \boldsymbol{u} - \boldsymbol{v} \parallel^2 = 2[\langle \boldsymbol{u}, \boldsymbol{v}\rangle + \overline{\langle \boldsymbol{u}, \boldsymbol{v}\rangle}]$.

ii) $i(\parallel \boldsymbol{u} + i\boldsymbol{v} \parallel^2 - \parallel \boldsymbol{u} - i\boldsymbol{v} \parallel^2) = 2[\langle \boldsymbol{u}, \boldsymbol{v}\rangle - \overline{\langle \boldsymbol{u}, \boldsymbol{v}\rangle}]$.

iii) $\parallel \boldsymbol{u} + \boldsymbol{v} \parallel^2 - \parallel \boldsymbol{u} - \boldsymbol{v} \parallel^2 + i \parallel \boldsymbol{u} + i\boldsymbol{v} \parallel^2 - i \parallel \boldsymbol{u} - i\boldsymbol{v} \parallel^2 = 4\langle \boldsymbol{u}, \boldsymbol{v}\rangle$.

Proof *i)*

$$\begin{array}{rcl}\| \boldsymbol{u}+\boldsymbol{v} \|^2 - \| \boldsymbol{u}-\boldsymbol{v} \|^2 & = & \langle \boldsymbol{u}+\boldsymbol{v}, \boldsymbol{u}+\boldsymbol{v}\rangle - \langle \boldsymbol{u}-\boldsymbol{v}, \boldsymbol{u}-\boldsymbol{v}\rangle \\ & = & (\| \boldsymbol{u} \|^2 + \| \boldsymbol{v} \|^2 + \langle \boldsymbol{u}, \boldsymbol{v}\rangle + \langle \boldsymbol{v}, \boldsymbol{u}\rangle) \\ & - & (\| \boldsymbol{u} \|^2 + \| \boldsymbol{v} \|^2 - \langle \boldsymbol{u}, \boldsymbol{v}\rangle - \langle \boldsymbol{v}, \boldsymbol{u}\rangle) \\ & = & 2[\langle \boldsymbol{u}, \boldsymbol{v}\rangle + \langle \boldsymbol{v}, \boldsymbol{u}\rangle] = 2[\langle \boldsymbol{u}, \boldsymbol{v}\rangle + \overline{\langle \boldsymbol{u}, \boldsymbol{v}\rangle}].\end{array}$$

We have therefore shown that

$$\| \boldsymbol{u}+\boldsymbol{v} \|^2 - \| \boldsymbol{u}-\boldsymbol{v} \|^2 = 2[\langle \boldsymbol{u}, \boldsymbol{v}\rangle + \overline{\langle \boldsymbol{u}, \boldsymbol{v}\rangle}]. \tag{6.1}$$

ii) Substituting $i\boldsymbol{v}$ *for* $\boldsymbol{v}$ *we get*

$$\begin{array}{rcl}\| \boldsymbol{u}+i\boldsymbol{v} \|^2 - \| \boldsymbol{u}-i\boldsymbol{v} \|^2 & = & 2[\langle \boldsymbol{u}, i\boldsymbol{v}\rangle + \overline{\langle \boldsymbol{u}, i\boldsymbol{v}\rangle}] \\ & = & -2i[\langle \boldsymbol{u}, \boldsymbol{v}\rangle - \overline{\langle \boldsymbol{u}, \boldsymbol{v}\rangle}].\end{array}$$

Multiplying by i, *we obtain*

$$i(\| \boldsymbol{u}+i\boldsymbol{v} \|^2 - \| \boldsymbol{u}-i\boldsymbol{v} \|^2) = 2[\langle \boldsymbol{u}, \boldsymbol{v}\rangle - \overline{\langle \boldsymbol{u}, \boldsymbol{v}\rangle}]. \tag{6.2}$$

iii) Adding Equations (6.1) and (6.2) yields iii).

The next theorem establishes a number of equivalences for an operator to be an isometry.

Theorem 6.7 *Let* $(V, \langle\ ,\ \rangle)$ *be a finite-dimensional inner product space and* T *an operator on* V. *Then the following are equivalent:*

1) T *is an isometry.*

2) $\langle T(\boldsymbol{u}), T(\boldsymbol{v})\rangle = \langle \boldsymbol{u}, \boldsymbol{v}\rangle$ *for all* $\boldsymbol{u}, \boldsymbol{v} \in V$.

3) $T^*T = I_V$.

4) If $\mathcal{S} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ *is an orthonormal basis of* V, *then* $T(\mathcal{S}) = (T(\boldsymbol{v}_1), \ldots, T(\boldsymbol{v}_n))$ *is an orthonormal basis.*

5) There exists an orthonormal basis $\mathcal{S} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ *of* V *such that* $T(\mathcal{S}) = (T(\boldsymbol{v}_1), \ldots, T(\boldsymbol{v}_n))$ *is an orthonormal basis.*

6) T^* *is an isometry.*

7) $\langle T^*(\boldsymbol{u}), T^*(\boldsymbol{v})\rangle = \langle \boldsymbol{u}, \boldsymbol{v}\rangle$ *for all* $\boldsymbol{u}, \boldsymbol{v} \in V$.

8) $TT^* = I_V$.

9) If $\mathcal{S} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n)$ is an orthonormal basis of V, then $T^*(\mathcal{S}) = (T^*(\boldsymbol{v}_1), \dots, T^*(\boldsymbol{v}_n))$ is an orthonormal basis.

10) There exists an orthonormal basis $\mathcal{S} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n)$ of V such that $T^*(\mathcal{S}) = (T^*(\boldsymbol{v}_1), \dots, T^*(\boldsymbol{v}_n))$ is an orthonormal basis.

Proof *We prove, cyclically, that 1)–5) are equivalent. This will also imply that 6)–10) are equivalent. We then show that 3) and 8) are equivalent.*

1) implies 2): Suppose V is a real inner product space. Then

$$\begin{aligned}4\langle T(\boldsymbol{u}), T(\boldsymbol{v})\rangle &= \| T(\boldsymbol{u}) + T(\boldsymbol{v}) \|^2 - \| T(\boldsymbol{u}) - T(\boldsymbol{v}) \|^2 \\ &= \| T(\boldsymbol{u}+\boldsymbol{v}) \|^2 - \| T(\boldsymbol{u}-\boldsymbol{v}) \|^2 \\ &= \| \boldsymbol{u}+\boldsymbol{v} \|^2 - \| \boldsymbol{u}-\boldsymbol{v} \|^2 = \langle \boldsymbol{u}, \boldsymbol{v}\rangle.\end{aligned}$$

Suppose V is a complex inner product space. Then by Lemma (6.6)

$$\begin{aligned}4\langle T(\boldsymbol{u}), T(\boldsymbol{v})\rangle &= \| T(\boldsymbol{u}) + T(\boldsymbol{v}) \|^2 - \| T(\boldsymbol{u}) - T(\boldsymbol{v}) \|^2 \\ &+ \ i \ \| T(\boldsymbol{u}) + iT(\boldsymbol{v}) \|^2 - i \ \| T(\boldsymbol{u}) - iT(\boldsymbol{v}) \|^2 \\ &= \| T(\boldsymbol{u}+\boldsymbol{v}) \|^2 - \| T(\boldsymbol{u}-\boldsymbol{v}) \|^2 \\ &+ \ i \ \| T(\boldsymbol{u}_i\boldsymbol{v}) \|^2 - i \ \| T(\boldsymbol{u}-i\boldsymbol{v}) \|^2 \\ &= \| \boldsymbol{u}+\boldsymbol{v} \|^2 - \| \boldsymbol{u}-\boldsymbol{v} \|^2 \\ &+ \ i \ \| \boldsymbol{u}+i\boldsymbol{v} \|^2 - i \ \| \boldsymbol{u}-i\boldsymbol{v} \|^2 \\ &= 4\langle \boldsymbol{u}, \boldsymbol{v}\rangle.\end{aligned}$$

2) implies 3): If $\langle T(\boldsymbol{u}), T(\boldsymbol{v})\rangle = \langle \boldsymbol{u}, \boldsymbol{v}\rangle$, then $\langle T^*T(\boldsymbol{u}), \boldsymbol{v}\rangle = \langle \boldsymbol{u}, \boldsymbol{v}\rangle$ for all $\boldsymbol{u}, \boldsymbol{v}$. Then $\langle (T^*T - I_V)(\boldsymbol{u}), \boldsymbol{v}\rangle = 0$ for all $\boldsymbol{u}, \boldsymbol{v}$. Setting $\boldsymbol{v} = (T^*T - I_V)(\boldsymbol{u})$ we get $\| (T^*T - I_V)(\boldsymbol{u}) \| = 0$. Therefore, $(T^*T - I_V)(\boldsymbol{u}) = 0$ for all $\boldsymbol{u} \in V$ and hence $T^*T - I_V = 0_{V \to V}$, which implies that $T^*T = I_V$.

3) implies 4): Assume $\mathcal{S} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n)$ is an orthonormal basis.

$$\| T(\boldsymbol{v}_i) \|^2 = \langle T(\boldsymbol{v}_i), T(\boldsymbol{v}_i)\rangle = \langle T^*T(\boldsymbol{v}_i), \boldsymbol{v}_i\rangle = \langle \boldsymbol{v}_i, \boldsymbol{v}_i\rangle = 1.$$

Assume $i \neq j$ then

$$\langle T(\boldsymbol{v}_i), T(\boldsymbol{v}_j)\rangle = \langle T^*T(\boldsymbol{v}_i), \boldsymbol{v}_j\rangle = \langle \boldsymbol{v}_i, \boldsymbol{v}_j\rangle = 0.$$

Thus, $T(\mathcal{S})$ is an orthonormal basis.

4) implies 5): This is immediate.

5) implies 1). Let $\boldsymbol{v}$ be an arbitrary vector. Assume

$$\boldsymbol{v} = a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \dots a_n\boldsymbol{v}_n.$$

Then

$$\| \boldsymbol{v} \|^2 = \| a_1 \|^2 + \dots + \| a_n \|^2 .$$

$T(\boldsymbol{v}) = T(a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \dots a_n\boldsymbol{v}_n) = a_1T(\boldsymbol{v}_1) + a_2T(\boldsymbol{v}_2) + \dots a_nT(\boldsymbol{v}_n)$. Since $T(\mathcal{S})$ is an orthonormal basis,

$$\| T(\boldsymbol{v}) \|^2 = \| a_1T(\boldsymbol{v}_1) + a_2T(\boldsymbol{v}_2) + \dots a_nT(\boldsymbol{v}_n) \|^2 = \| a_1 \|^2 + \dots + \| a_n \|^2$$

and therefore

$$\| T(\boldsymbol{v}) \|^2 = \| \boldsymbol{v} \|^2 .$$

Finally, for an operator T on a finite-dimensional vector space, $T^*T = I_V$ if and only if $TT^* = I_V$, and therefore 3) and 8) are equivalent.

In our next result we characterize the matrix of an isometry with respect to an orthonormal basis.

Theorem 6.8 *Let $(V, \langle\ ,\ \rangle)$ be a finite-dimensional inner product space, T an operator on V, $\mathcal{S}$ an orthonormal basis, and $A = \mathcal{M}_T(\mathcal{S}, \mathcal{S})$. Then the following hold:*

i) If V is a complex inner product space, then T is an isometry if and only if $A^{-1} = \overline{A}^{tr}$.

ii) If V is a real inner product space, then T is an isometry if and only if $A^{-1} = A^{tr}$.

Proof *i) Assume T is an isometry. Then $T^* = T^{-1}$. Then $A^{-1} = \mathcal{M}_{T^{-1}}(\mathcal{S}, \mathcal{S}) = \mathcal{M}_{T^*}(\mathcal{S}, \mathcal{S}) = \overline{A}^{tr}$.*

Conversely, assume $A^{-1} = \overline{A}^{tr}$. Since $A^{-1} = \mathcal{M}_{T^{-1}}(\mathcal{S}, \mathcal{S})$ and $\overline{A}^{tr} = \mathcal{M}_{T^*}(\mathcal{S}, \mathcal{S})$, it follows that $T^{-1} = T^*$ and therefore $T^*T = I_V$. Thus, T is an isometry by part iii) of Theorem (6.7).

ii) This is similar to i) and left as an exercise.

Definition 6.7 *An $n \times n$ complex matrix is said to be* **unitary** *if $\overline{A}^{tr} = A^{-1}$.*

Definition 6.8 *A square real matrix is said to be* **orthogonal** *if $A^{tr} = A^{-1}$.*

We complete this section with two results, Schur's lemma for operators and Schur's lemma for matrices. The latter will be used in Section (12.4) to establish Schur's inequality for the spectral radius of a complex matrix.

Lemma 6.7 *Let T be an operator on an n-dimensional complex inner product space $(V, \langle\ ,\ \rangle)$. Then there exists an orthonormal basis $\mathcal{B} = (\boldsymbol{w}_1, \dots, \boldsymbol{w}_n)$ such that for each $k, 1 \leq k \leq n$ the subspace $Span(\boldsymbol{w}_1, \dots, \boldsymbol{w}_k)$ is T-invariant.*

Proof *The proof is by induction on n. If $n = 1$, there is nothing to prove so assume that $n > 1$ and that the result is true for operators on spaces of dimension $n-1$. Since $(V, \langle\ ,\ \rangle)$ is a complex inner product space, there exists an eigenvector $\boldsymbol{w}$ for T. If $\langle \boldsymbol{w}, \boldsymbol{w}\rangle \neq 1$ then by replacing $\boldsymbol{w}$ by $\frac{1}{\|\boldsymbol{w}\|}\boldsymbol{w}$ we can assume that $\| \boldsymbol{w} \| = 1$. Set $W = Span(\boldsymbol{w}), U = W^{\perp}$, and $P = Proj_{(U,W)}$. Also let $\widehat{T}$ be the restriction of PT to U. Note that a subspace X of U is $\widehat{T}$-invariant if and only if $X + W$ is T-invariant. By the inductive hypothesis, there exists an orthonormal basis $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_{n-1})$ of U such that for each $k, 1 \leq k \leq n-1$ the subspace $Span(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$ is $\widehat{T}$-invariant. Now for $2 \leq j \leq n$ set $\boldsymbol{w}_j = \boldsymbol{u}_{j-1}$. Since $\boldsymbol{w}_1 \perp \boldsymbol{u}_j$ for $1 \leq j \leq n-1$ it follows that $\mathcal{B} = (\boldsymbol{w}_1, \dots, \boldsymbol{w}_n)$ is an orthonormal basis of V. Let k satisfy $1 \leq k \leq n-1$. Then $Span(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$ is $\widehat{T}$-invariant and therefore $Span(\boldsymbol{w}_1, \boldsymbol{u}_1, \dots, \boldsymbol{u}_k) = Span(\boldsymbol{w}_1, \dots, \boldsymbol{w}_{k+1})$ is T-invariant.*

We now prove the matrix version:

Lemma 6.8 *Let A be an $n \times n$ complex matrix. Then there exists a unitary matrix Q such that QAQ^* is upper triangular.*

Proof *Let $\mathbb{C}^n$ be equipped with the Euclidean inner product:*

$$\left\langle \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \right\rangle = x_1\overline{y_1} + \dots + x_n\overline{y_n}.$$

Let $T_A : \mathbb{C}^n \to \mathbb{C}^n$ be the operator given by $T_A(\boldsymbol{x}) = A\boldsymbol{x}$. Let $\mathcal{S}$ be the standard basis of $\mathbb{C}^n$ so that $\mathcal{M}_{T_A}(\mathcal{S}, \mathcal{S}) = A$. By Schur's lemma for operators, Lemma (6.7), there exists an orthonormal basis $\mathcal{B} = (\boldsymbol{w}_1, \dots, \boldsymbol{w}_n)$ such that for every $k, 1 \leq k \leq n, Span(\boldsymbol{w}_1, \dots, \boldsymbol{w}_k)$ is T_A-invariant. It follows that $\mathcal{M}_{T_A}(\mathcal{B}, \mathcal{B})$ is upper triangular. Let I be the identity operator on $\mathbb{C}^n$ and set $Q = \mathcal{M}_I(\mathcal{B}, \mathcal{S})$. Then Q is a unitary matrix by Exercise 5 below so that $Q^{-1} = Q^*$. Then $\mathcal{M}_{T_A}(\mathcal{B}, \mathcal{B}) = \mathcal{M}_I(\mathcal{B}, \mathcal{S})\mathcal{M}_{T_A}(\mathcal{S}, \mathcal{S})\mathcal{M}_T(\mathcal{S}, \mathcal{B}) = QAQ^*$.

Exercises

1. Prove that an isometry is injective, hence bijective. Prove that the inverse of an isometry is an isometry.

2. Prove that the product (composition) of isometries is an isometry.

3. Let $\mathcal{S} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n)$ be an orthonormal basis of V and let $\lambda_i \in \mathbb{F}$ satisfy $|\lambda_i| = 1$. Define $T : V \to V$ such that $T(\boldsymbol{v}_i) = \lambda_i \boldsymbol{v}_i$. Prove that T is an isometry.

4. Prove part ii) of Theorem (6.8).

5. Let $(V, \langle\ ,\ \rangle)$ be a complex inner product space and assume $\mathcal{S}_1 = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n), \mathcal{S}_2 = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ are orthonormal bases of V. Prove that the change of basis matrix $\mathcal{M}_{I_V}(\mathcal{S}_1, \mathcal{S}_2)$ is a unitary matrix.

6. Let $(V, \langle\ ,\ \rangle)$ be a real inner product space and assume $\mathcal{S}_1 = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n), \mathcal{S}_2 = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ are orthonormal bases of V. Prove that the change of basis matrix $\mathcal{M}_{I_V}(\mathcal{S}_1, \mathcal{S}_2)$ is an orthogonal matrix.

7. Prove the following matrix version of the complex spectral theorem: Let A be a complex $n \times n$ matrix. Prove that $A\overline{A}^{tr} = \overline{A}^{tr} A$ if and only if there is a unitary matrix Q such that QAQ^{-1} is a diagonal matrix. Moreover, if A is Hermitian, that is, $A = \overline{A^{tr}}$, then the diagonal entries of A are real numbers.

8. Prove the following matrix version of the real spectral theorem: Let A be a real $n \times n$ matrix. Then A is symmetric if and only if there is an orthogonal matrix Q such that QAQ^{tr} is a diagonal matrix.

9. Let $(V, \langle\ ,\ \rangle)$ be a real inner product space and T an operator on V. Prove that T is an isometry if and only if there exists an orthonormal basis $\mathcal{S}$ such that $\mathcal{M}_T(\mathcal{S}, \mathcal{S})$ is block diagonal and each block is either 1×1 with entry ± 1 or 2×2 of the form $\begin{pmatrix} cos\ \theta & -sin\ \theta \\ sin\ \theta & cos\ \theta \end{pmatrix}$ for some $\theta, 0 < \theta < \pi$.

10. Assume T is an isometry of the inner product space $(V, \langle\ ,\ \rangle)$ and that T is self-adjoint. Prove that $T^2 = I_V$ and there exists an orthonormal basis $\mathcal{B}$ such that $\mathcal{M}_T(\mathcal{B}, \mathcal{B})$ is diagonal and all the diagonal entries are ± 1.

11. Assume T is a self-adjoint operator on an inner product space $(V, \langle\ ,\ \rangle)$ and $T^2 = I_V$. Prove that T is an isometry.

12. Give an example of a normal operator T on a complex inner product space, which is an isometry but $T^2 \neq I_V$.

13. Let T be a unitary operator of a finite-dimensional inner product space $(V, \langle\ ,\ \rangle)$ and a U a T-invariant subspace. Prove that $U^\perp$ is T-invariant.

14. Let A be a unitary matrix. Assume A is upper triangular. Prove that A is diagonal.

15. Let $(V, \langle\ ,\ \rangle)$ be an $n-$dimensional inner product space. Assume U_1, U_2

are k-dimensional subspaces and $R : U_1 \to U_2$ is a linear map which satisfies $\parallel R(\boldsymbol{u}) \parallel = \parallel \boldsymbol{u} \parallel$. Prove that there exists an isometry S such that $S_{|U_1} = R$.

16. Let V be a real inner product space of odd dimension and $S \in \mathcal{L}(V, V)$ an orthogonal transformation. Prove that there is a vector $\boldsymbol{v}$ such that $S^2(\boldsymbol{v}) = \boldsymbol{v}$.

17. Let $(V, \langle\ ,\ \rangle)$ be a finite-dimensional inner product space and U a subspace, $U \neq V, \{\mathbf{0}\}$. Set $T = Proj_{(U,U^\perp)} - Proj_{(U^\perp,U)}$. Prove that T is a self-adjoint isometry of V.

18. Let S be an operator on $\mathbb{R}^4$ have eigenvectors $\left(\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix}\right)$ with corresponding eigenvalues 2,3,4,5. Let T be the operator on $\mathbb{R}^4$ having eigenvectors $\left(\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}\right)$ with corresponding eigenvalues 2,3,4,5. Prove that there exists an invertible operator Q such that $Q^{-1}SQ = T$, but it is not possible for Q to be an isometry.

6.5 Polar and Singular Value Decomposition

In this section we obtain the polar decomposition of an operator on a finite-dimensional inner product space. It is, in some ways, the generalization of the decomposition of an arbitrary nonzero complex number z as the product of a pair (r, u) where r is a positive real number and u is a complex number with modulus one. In the more general setting, these will be replaced by a semi-positive Hermitian operator (defined below) and a unitary operator, respectively. Polar decomposition is a fundamental tool in the theory of finite-dimensional Lie groups and Lie algebras. We subsequently develop the singular value decomposition of a linear map between two inner product spaces. The singular value decomposition has many applications, in particular to image compression, data mining, text mining, face recognition, as well as many others.

What You Need to Know

You will need to have a mastery of the following concepts: linear transformation from a vector space V to a vector space W, kernel of a linear transformation, linear operator on the vector space V, inner product space, self-adjoint operator on an inner product space, basis of a finite-dimensional vector space, matrix of a linear transformation, and eigenvalues and eigenvectors of an operator.

We begin with a definition:

Definition 6.9 *Let $(V, \langle \ , \ \rangle)$ be an inner product space. An operator T is* **semipositive** *if T is self-adjoint and $\langle T(\boldsymbol{u}), \boldsymbol{u}\rangle \geq 0$ for all $\boldsymbol{u} \in V$. A self-adjoint operator is* **positive** *if $\langle T(\boldsymbol{u}), \boldsymbol{u}\rangle > 0$ for all non-zero vectors $\boldsymbol{u} \in V$.*

Example 6.1 *Let U be a subspace of the inner product space $(V, \langle \ , \ \rangle)$ and let $P = Proj_{(U,U^{\perp})}$, the orthogonal projection onto U. Then P is a semi-positive operator.*

Example 6.2 *Let S be any operator on an inner product space $(V, \langle \ , \ \rangle)$. Then $T = S^*S$ is a semi-positive operator. We have previously seen that S^*S is self-adjoint. We need to show that $\langle (S^*S)(\boldsymbol{v}), \boldsymbol{v}\rangle \geq 0$ for every $\boldsymbol{v} \in V$. We have*

$$\langle (S^*S)(\boldsymbol{v}), \boldsymbol{v}\rangle = \langle S(\boldsymbol{v}), S(\boldsymbol{v})\rangle = \parallel S(\boldsymbol{v}) \parallel^2 \geq 0.$$

Definition 6.10 *Let T be an operator on a space V. An operator S on V is said to be a* **square root** *of T if $S^2 = T$.*

Example 6.3 *If V is a two-dimensional vector space then I_V has infinitely many square roots: in addition to $\pm I_V$ let $(\boldsymbol{v}_1, \boldsymbol{v}_2)$ be any basis of V and let $S(\boldsymbol{v}_1) = \boldsymbol{v}_1, S(\boldsymbol{v}_2) = -\boldsymbol{v}_2$. Then $S^2 = I_V$.*

Following is our main result, characterizing positive operators.

Theorem 6.9 *Let $(V, \langle\ ,\ \rangle)$ be an inner product space and $T \in \mathcal{L}(V, V)$. Then the following are equivalent:*

1. T is a semi-positive operator.

2. T is self adjoint and all the eigenvalues of T are non-negative.

3. T has a semi-positive square root.

4. T has a self-adjoint square root.

5. There is an operator S such that $T = S^*S$.

Proof *1) implies 2): Since T is a semi-positive operator, T is self-adjoint. Suppose $\boldsymbol{v}$ is a eigenvector of T with eigenvalue λ. Then*

$$\lambda \parallel \boldsymbol{v} \parallel = \langle \lambda \boldsymbol{v}, \boldsymbol{v} \rangle = \langle T(\boldsymbol{v}), \boldsymbol{v} \rangle \geq 0$$

since T is semi-positive. Since $\parallel \boldsymbol{v} \parallel > 0$, it follows that $\lambda \geq 0$.

2) implies 3). Since T is self-adjoint, there exists an orthonormal basis $\mathcal{S} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ consisting of eigenvectors of T. Set $\lambda_j = T(\boldsymbol{v}_j)$. By assumption, $\lambda_j \geq 0$. Define S as follows: If $\lambda_j = 0$, then $S(\boldsymbol{v}_j) = \mathbf{0} = \sqrt{\lambda_j}\boldsymbol{v}_j$. If $\lambda_j > 0$, then $S(\boldsymbol{v}_j) = \sqrt{\lambda_j}\boldsymbol{v}_j$.

Since $\mathcal{S}$ is an orthonormal basis and $\mathcal{M}_S(\mathcal{S}, \mathcal{S})$ is diagonal with real entries it follows that S is self-adjoint by the spectral theorem. We need to prove that S is semi-positive. Suppose now that $\boldsymbol{v} = a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_n\boldsymbol{v}_n$. Then

$$\begin{aligned}
\langle S(\boldsymbol{v}), \boldsymbol{v} \rangle &= \langle S(a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_n\boldsymbol{v}_n), a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_n\boldsymbol{v}_n \rangle \\
&= \langle \sqrt{\lambda_1}a_1\boldsymbol{v}_1 + \cdots + \sqrt{\lambda_n}a_n\boldsymbol{v}_n, a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_n\boldsymbol{v}_n \rangle \\
&= \sqrt{\lambda_1}a_1\overline{a_1} + \cdots + \sqrt{\lambda_n}a_n\overline{a_n} \\
&= \sqrt{\lambda_1}|a_1|^2 + \ldots \sqrt{\lambda_n}|a_n|^2 \geq 0,
\end{aligned}$$

since each $\sqrt{\lambda_j} \geq 0$ and $|a_j|^2 \geq 0$. Thus, S is a semi-positive operator.

3) implies 4). Since a semi-positive square root is a self-adjoint square root, this is immediate.

4) implies 5). Let S be a self-adjoint square root of T. Then $S^*S = S^2 = T$.

5) implies 1). Assume $T = S^*S$ for some operator S and let $\boldsymbol{v}$ be an arbitrary vector in V. Then

$$\langle T(\boldsymbol{v}), \boldsymbol{v}\rangle = \langle (S^*S)(\boldsymbol{v}), \boldsymbol{v}\rangle = \langle S(\boldsymbol{v}), S(\boldsymbol{v})\rangle = \parallel S(\boldsymbol{v}) \parallel^2 \geq 0.$$

Theorem 6.10 *Assume T is a semi-positive operator. Then T has a unique semi-positive square root.*

The proof of this result is left as an exercise.

Definition 6.11 *Let T be a semi-positive operator on an inner product space $(V, \langle\ ,\ \rangle)$. The unique semi-positive square root of T will be referred to as the* **square root** *of T and is denoted by $\sqrt{T}$.*

Lemma 6.9 *Let T be a linear operator on the inner product space $(V, \langle\ ,\ \rangle)$. Then for any vector $\boldsymbol{v}$,*

$$\parallel T(\boldsymbol{v}) \parallel = \parallel \sqrt{T^*T}(\boldsymbol{v}) \parallel .$$

Proof *For $\boldsymbol{v} \in V$,*

$$\begin{aligned} \parallel T(\boldsymbol{v}) \parallel^2 &= \langle T(\boldsymbol{v}), T(\boldsymbol{v})\rangle \\ &= \langle (T^*T)(\boldsymbol{v}), \boldsymbol{v}\rangle = \langle (\sqrt{T^*T})^2(\boldsymbol{v}), \boldsymbol{v}\rangle \\ &= \langle \sqrt{T^*T}(\boldsymbol{v}), \sqrt{T^*T}(\boldsymbol{v})\rangle = \parallel \sqrt{T^*T}(\boldsymbol{v}) \parallel^2 . \end{aligned}$$

Corollary 6.4 *Let T be an operator on the inner product space $(V, \langle\ ,\ \rangle)$. Then $Ker(T) = Ker(\sqrt{T^*T})$.*

Proof *A vector $\boldsymbol{v}$ is in $Ker(T)$ if and only if $\parallel T(\boldsymbol{v}) \parallel = 0$ if and only if $\parallel \sqrt{T^*T}(\boldsymbol{v}) \parallel = 0$ if and only if $\boldsymbol{v} \in Ker(\sqrt{T^*T})$.*

The next result shows how we can express an arbitrary operator as a composition of a semi-positive operator and an isometry.

Theorem 6.11 *Let $(V, \langle\ ,\ \rangle)$ be an inner product space and T an operator on V. Then there exists an isometry S on V such that $T = S\sqrt{T^*T}$.*

Proof *By Corollary (6.4), $Ker(T) = Ker(\sqrt{T^*T})$. By Exercise 15 of Section (2.2) the map $R : Range(\sqrt{T^*T}) \to Range(T)$ given by $R(\sqrt{T^*T}(\boldsymbol{v})) = T(\boldsymbol{v})$ is well-defined and linear. By Lemma (6.9), R is an isometry from $Range(\sqrt{T^*T})$ to $Range(T)$. By Exercise 16 of Section (6.4), there exists an isometry S of V such that $S_{|Range(\sqrt{T^*T})} = R$. It is clear from the construction that $S\sqrt{T^*T} = T$.*

Definition 6.12 *Let T be an operator on a finite dimension inner product space $(V, \langle\ ,\ \rangle)$. The decomposition $T = S\sqrt{T^*T}$ is referred to as the* **polar decomposition** *of T.*

The next result gives a particularly nice representation of a linear transformation between two finite-dimensional inner product spaces. It is referred to as the **Singular Value Decomposition** of the transformation.

Theorem 6.12 *Let $(V, \langle\ ,\ \rangle_V)$ and $(W, \langle\ ,\ \rangle_W)$ be finite-dimensional inner product spaces and $T : V \to W$ a linear transformation. Then there exists orthonormal bases $\mathcal{B}_V = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ and $\mathcal{B}_W = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_m)$ and unique positive scalars $s_1 \geq \dots \geq s_r$ such that $T(\boldsymbol{v}_j) = s_j\boldsymbol{u}_j$ if $j \leq r$ and $T(\boldsymbol{v}_j) = \boldsymbol{0}_W$ if $j > r$.*

Proof *First of all, the operator T^*T on V is a semi-positive operator. Let $r = rank(T^*T)$ so that $r \leq n$, the dimension of V. Let $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_r)$ be an orthonormal basis for $Range(T^*T)$ consisting of eigenvectors of T^*T with the notation chosen so that if $(T^*T)(\boldsymbol{v}_j) = \alpha_j$ then $\alpha_1 \geq \dots \geq \alpha_r > 0$. Let $(\boldsymbol{v}_{r+1}, \dots, \boldsymbol{v}_n)$ be an orthonormal basis for $Ker(T^*T)$ so that $\mathcal{B} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ is an orthonormal basis of V consisting of eigenvectors of T^*T.*

Now for $j \leq r$, set $s_j = \sqrt{\alpha_j}$ and $\boldsymbol{u}_j = \frac{1}{s_j}T(\boldsymbol{v}_j)$. We claim that $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_r)$ is an orthonormal sequence from W. For suppose $1 \leq i, j \leq r$, then

$$\begin{aligned}
\langle \boldsymbol{u}_i, \boldsymbol{u}_j \rangle_W &= \langle \frac{1}{s_i}T(\boldsymbol{v}_i), \frac{1}{s_j}T(\boldsymbol{v}_j) \rangle_W \\
&= \frac{1}{s_i s_j}\langle T(\boldsymbol{v}_i), T(\boldsymbol{v}_j) \rangle_W \\
&= \frac{1}{s_i s_j}\langle (T^*T)(\boldsymbol{v}_i), \boldsymbol{v}_j \rangle_V \\
&= \frac{1}{s_i s_j}\langle \alpha_i \boldsymbol{v}_i, \boldsymbol{v}_j \rangle_W \\
&= \frac{s_i^2}{s_i s_j}\langle \boldsymbol{v}_i, \boldsymbol{v}_j \rangle_W.
\end{aligned}$$

Finally, $\langle \boldsymbol{v}_i, \boldsymbol{v}_j \rangle$ is 1 if $i = j$ and 0 otherwise. In the former case, we get $\langle \boldsymbol{u}_i, \boldsymbol{u}_j \rangle_W = \frac{s_i^2}{s_i^2} = 1$ and in the latter case $\langle \boldsymbol{u}_i, \boldsymbol{u}_j \rangle_W = 0$, as required.

Now extend $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r)$ to an orthonormal basis $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m)$ of W. All that remains is to show that $T(\boldsymbol{v}_j) = \mathbf{0}_W$ if $j > r$. However, $(T^*T)(\boldsymbol{v}_j) = \mathbf{0}_V$. This implies that $\langle (T^*T)(\boldsymbol{v}_j), \boldsymbol{v}_j \rangle_V = 0$ whence $\langle T(\boldsymbol{v}_j), T(\boldsymbol{v}_j) \rangle_W = 0$ from which we conclude that $T(\boldsymbol{v}_j) = \mathbf{0}_W$ as desired.

It remains to prove uniqueness. Suppose then that $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n), (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m)$ and $t_1 \geq t_2 \ldots t_r > 0$ satisfy the conclusions of the theorem. Then, for $1 \leq i \leq m$ and $1 \leq j \leq n$, we have

$$\langle T^*(\boldsymbol{y}_i), \boldsymbol{x}_j \rangle_V = \langle \boldsymbol{y}_i, T(\boldsymbol{x}_j) \rangle_W.$$

The latter is t_i if $i = j \leq r$ and 0 otherwise. This implies that $T^*(\boldsymbol{y}_i) = t_i \boldsymbol{x}_i$ if $1 \leq i \leq r$ and is $\mathbf{0}_V$ if $i > r$. We then have for $1 \leq j \leq r$ that

$$(T^*T)(\boldsymbol{x}_j) = T^*(t_j \boldsymbol{y}_j) = t_j T^*(\boldsymbol{y}_j) = t_j^2 \boldsymbol{v}_j.$$

If $j > r$ then $(T^*T)(\boldsymbol{x}_j) = T^*(\mathbf{0}_W) = \mathbf{0}_V$. Consequently, if $1 \leq j \leq r$, then t_j^2 is an eigenvalue of T^*T and therefore, given how $(t_1, \ldots, t_r)$ are ordered, we must have $t_j = s_j$.

Definition 6.13 *Let $(V, \langle \ , \ \rangle_V)$ and $(W, \langle \ , \ \rangle_W)$ be finite-dimensional inner product spaces and $T : V \to W$ a linear transformation. The unique scalars $s_1, \ldots, s_r$ are the* **singular values** *of the transformation T.*

If A is an $m \times n$ complex matrix, the **singular values** *of A are the singular values of the transformation $T_A : \mathbb{C}^n \to \mathbb{C}^m$ given by multiplication on the left by A.*

Theorem (6.12) has the following nice factorization theorem for a matrix. We leave the proof as an exercise.

Corollary 6.5 *Let A be an $m \times n$ matrix of rank r with positive singular values $s_1 \geq \cdots \geq s_r$. Let S be the $m \times n$ matrix whose (i, j)-entry is s_i if $i = j \leq r$ and 0 otherwise. Then there exists an $m \times m$ unitary matrix Q, and $n \times n$ unitary matrix P such that*

$$A = QSP.$$

Definition 6.14 *Let A be an $m \times n$ matrix of rank r with positive singular values $s_1 \geq \cdots \geq s_r$. Let S be the $m \times n$ matrix whose (i, j)-entry is s_i if $i = j \leq r$ and 0 otherwise. The expression $A = QSP$ is referred to as a* **singular value decomposition** *of the matrix A.*

Exercises

1. Prove Theorem (6.10).

2. Let $(V, \langle\ ,\ \rangle)$ be a complex inner product space and $T \in \mathcal{L}(V, V)$ a normal operator. Prove that T has a square root.

3. Let $(V, \langle\ ,\ \rangle)$ be a two-dimensional real inner product space and assume that $T \in \mathcal{L}(V, V)$ is a normal operator but not self-adjoint. Prove that T has a square root.

4. Let $(V, \langle\ ,\ \rangle)$ be a $2n$-dimensional real inner product space. Assume that $T \in \mathcal{L}(V, V)$ is a normal operator and that T does not have any eigenvectors. Prove that T has a square root.

5. Prove that the sum of two semi-positive operators is semi-positive.

6. Assume T is a semi-positive operator on an inner product space $(V, \langle\ ,\ \rangle)$ and $c \in \mathbb{R}^+$. Prove that cT is a semi-positive operator.

7. Prove that a semi-positive operator is invertible if and only if it is positive.

8. Assume T is a positive operator on the inner product space $(V, \langle\ ,\ \rangle)$. Prove that T^{-1} is a positive operator.

9. Assume that T is a positive operator on the inner product space V. Define $[\ ,\ ] : V \times V \to V$ by $[\boldsymbol{v}, \boldsymbol{w}] = \langle T(\boldsymbol{v}), \boldsymbol{w}\rangle$. Prove that $[\ ,\ ]$ is an inner product on V.

10. Assume that T is a positive operator on the inner product space V. Define $[\ ,\ ] : V \times V \to V$ as in Exercise 9. Let S be an operator on V and denote by $S^\star$ the adjoint of S with respect to $[\ ,\ ]$. Prove that $S^\star = T^{-1}S^*T$.

11. Let $(V, \langle\ ,\ \rangle)$ be a finite-dimensional inner product space, R a self-adjoint operator, and T a positive operator. Prove that TR and RT are diagonalizable operators with real eigenvalues.

12. Prove a semi-positive operator T is an isometry if and only if T is the identity operator.

13. Assume S, T are semi-positive operators on the inner product space $(V, \langle\ ,\ \rangle)$. If $ST = TS$, then ST is a semi-positive operator.

14. Give an example of semi-positive operators S, T on a finite-dimensional inner product space $(V, \langle\ ,\ \rangle)$ such that ST is not a semi-positive operator.

15. In the polar decomposition $T = S\sqrt{T^*T}$, with S an isometry, prove that S is unique if and only if T is invertible.

16. Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ be multiplication by the matrix $\begin{pmatrix} 0 & 1 & 1 \\ -1 & 0 & 1 \\ -1 & -1 & 0 \end{pmatrix}$. Find an isometry S such that $T = S\sqrt{T^*T}$.

17. Prove Corollary (6.5).

18. Let T be an operator on an inner product space $(V, \langle\ ,\ \rangle)$. Prove that TT^* and T^*T have the same eigenvalues and that each eigenvalue occurs with the same multiplicity in TT^* and T^*T.

19. Assume T is a semi-positive operator on a finite-dimensional inner product space $(V, \langle\ ,\ \rangle)$. Prove that the singular values of T are the eigenvalues of T.

20. Let T be an operator on a finite-dimensional inner product space $(V, \langle\ ,\ \rangle)$. Assume the polar decomposition of T is $T = SP$ where S is an isometry and P is a semi-positive operator. Prove T is normal if and only if $SP = PS$.

7

Trace and Determinant of a Linear Operator

CONTENTS

In this chapter, we study the trace and determinant of an operator. In the first section, we define the trace of a linear operator T on a finite-dimensional vector space V in terms of the characteristic polynomial, $\chi_T(x)$, of the operator. We also define the trace of a square matrix. We then relate these two concepts of trace by proving that if T is an operator on the finite-dimensional vector space V and $\mathcal{B}$ is any basis of V, then the trace of the operator T and the trace of the matrix $\mathcal{M}_T(\mathcal{B}, \mathcal{B})$ are the same. In the course of this, we establish many of the properties of the trace. In the second section, we introduce the determinant of a linear operator T on a finite-dimensional vector space V, again in terms of the characteristic polynomial, $\chi_T(x)$, of the operator. We also define a determinant of a square matrix. We then relate these two by proving that if T is an operator on the finite-dimensional vector space V and $\mathcal{B}$ is any basis of V, then the determinant of the operator T and the determinant of the matrix $\mathcal{M}_T(\mathcal{B}, \mathcal{B})$ are the same. In the concluding section, we show how the determinant can be used to define an alternating n-linear form on an n-dimensional vector space and prove that this form is unique.

7.1 Trace of a Linear Operator

Let V be a finite-dimensional vector space over the field $\mathbb{F}$ and $T : V \to V$ be a linear operator. In this section we define the concept of the trace of T in terms of the characteristic polynomial of T. Let $\mathcal{B}$ be a basis of V and $A = \mathcal{M}_T(\mathcal{B}, \mathcal{B})$, the matrix of T with respect to $\mathcal{B}$. We previously defined the trace of T. In our main theorem we show that the trace of T and the trace of A are equal. This is then used to prove that the map $Tr : \mathcal{L}(V, V) \to \mathbb{F}$ is a linear transformation.

What You Need to Know

You will need to have a mastery of the following concepts: basis of a finite-dimensional vector space, linear operator on a vector space, matrix of a linear operator with respect to a basis $\mathcal{B}$, the minimal polynomial of an operator, the invariant factors of an operator, the elementary divisors of an operator, the characteristic polynomial of an operator, eigenvalues and eigenvectors of an operator, direct sum decomposition of a vector space, a T-invariant subspace for an operator T on a vector space V, invertible matrix, block diagonal matrix, and the companion matrix of a polynomial.

We begin with a definition:

Definition 7.1 *Let V be a finite-dimensional vector space and T an operator on V. Assume the characteristic polynomial of T is*

$$\chi_T(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

The **trace** *of T, denoted by $Tr(T)$, is defined to be $-a_{n-1}$.*

Remark 7.1 *Suppose the characteristic polynomial $\chi_T(x)$ factors into linear factors (for example, when the field is $\mathbb{C}$):*

$$\chi_T(x) = (x - \lambda_1)(x - \lambda_2) \dots (x - \lambda_n),$$

where λ_i are the eigenvalues of T repeated with their algebraic multiplicity. Then the trace of T is the sum of the eigenvalues of T (taken with their algebraic multiplicity):

$$Tr(T) = \lambda_1 + \lambda_2 + \cdots + \lambda_n.$$

Example 7.1 *Let* $T : \mathbb{C}^3 \to \mathbb{C}^3$ *be multiplication by the matrix* $\begin{pmatrix} 0 & 0 & -5 \\ 1 & 0 & -3 \\ 0 & 1 & 1 \end{pmatrix}$. *Then* $\chi_T(x) = (x+1)(x-[1+2i])(x-[1-2i]) = x^3-x^2+3x+5.$ *In this case, the trace is 1.*

Note that as a real operator the characteristic polynomial is $(x+1)(x^2-2x+5)$.

We will learn shortly how to compute the trace of an operator given a matrix of the operator. Some examples will convince you that it is always the sum of the diagonal entries of such a matrix. Let A be $n \times n$ matrix,

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}.$$

We previously defined the trace of $A, Trace(A) = a_{11} + a_{22} + \cdots + a_{nn}$, the sum of the diagonal entries.

Theorem 7.1 *Assume* A, B *are* $n \times n$ *matrices. Then* $Trace(AB) = Trace(BA)$.

Proof *Let*

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \text{ and } B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{nn} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \dots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{pmatrix}.$$

Then the (i, j)*-entry of* AB *is* $\sum_{k=1}^{n} a_{ik}b_{kj}$ *and therefore*

$$Trace(AB) = \sum_{i=1}^{n}\sum_{k=1}^{n} a_{ik}b_{ki}.$$

By the same reasoning,

$$Trace(BA) = \sum_{k=1}^{n}\sum_{i=1}^{n} b_{ki}a_{ik}.$$

They are identical.

Corollary 7.1 *If C is an $n \times n$ matrix and P is an invertible $n \times n$ matrix, then*

$$Trace(P^{-1}CP) = Trace(C).$$

Corollary 7.2 *Let V be an n-dimensional vector space, T an operator on V, and $\mathcal{B}, \mathcal{B}'$ bases for V. Then*

$$Trace(\mathcal{M}_T(\mathcal{B}, \mathcal{B})) = Trace(\mathcal{M}_T(\mathcal{B}', \mathcal{B}')).$$

Let V be a finite-dimensional vector space, T an operator on V, and $\mathcal{B}$ a basis for V. It is our goal to show that $Tr(T) = Trace(\mathcal{M}_T(\mathcal{B}, \mathcal{B}))$. In light of Corollary (7.2), it suffices to show the existence of at least one basis for which this is so. Before we get to the proof. we first establish a lemma about the characteristic polynomial.

Lemma 7.1 *Let V be a finite-dimensional vector space and T an operator on V. Assume $V = U \oplus W$, where U, W are T-invariant subspaces. Let $T_U = T_{|_U}$ and $T_W = T_{|_W}$. Then*

$$\chi_T(x) = \chi_{T_U}(x)\chi_{T_W}(x).$$

Proof *Let $\mu_T(x) = p_1(x)^{e_1} \dots p_t(x)^{e_t}$ be the minimal polynomial of T. Set $V_i = V_{p_i(x)} = null(p_i(T)^{dim(V)})$ and $m_i = \frac{dim(V_i)}{deg(p_i(x))}$. Then $V = V_1 \oplus V_2 \oplus \dots \oplus V_t$ and it follows from Exercise 13 of Section (4.5) that $\chi_T(x) = p_1(x)^{m_1} \dots p_t(x)^{m_t}$.*

It follows from Theorem (4.14) that $U = (U \cap V_1) \oplus \dots \oplus (U \cap V_t)$ and likewise $W = (W \cap V_1) \oplus \dots \oplus (W \cap V_t)$. Since $V = U \oplus W$, it then follows that $V_i = (V_i \cap U) \oplus (V_i \cap W)$. Therefore, $dim(V_i \cap U) + dim(V_i \cap W) = dim(V_i)$. This holds for each i. It now follows that

$$\chi_T(x) = \chi_{T_U}(x)\chi_{T_W}(x).$$

Corollary 7.3 *Let V be a finite-dimensional vector space and T an operator on V. Assume $V = V_1 \oplus \dots \oplus V_k$ where V_i is T-invariant. Set $T_i = T_{|V_i}$. Then $\chi_T(x) = \chi_{T_1}(x) \dots \chi_{T_k}(x)$.*

Proof *This follows from Lemma (7.1) by induction on k.*

The following is immediate:

Lemma 7.2 *Assume the matrix A is block diagonal with diagonal blocks $A_1, A_2, \ldots, A_k$. Then*

$$Trace(A) = Trace(A_1) + \cdots + Trace(A_k).$$

Theorem 7.2 *Let V be a finite-dimensional vector space, T an operator on V, and $\mathcal{B}$ a base for V. Then*

$$Tr(T) = Trace(\mathcal{M}_T(\mathcal{B}, \mathcal{B})).$$

Proof *Since $Trace(\mathcal{M}_T(\mathcal{B}, \mathcal{B}))$ is independent of the base $\mathcal{B}$, it suffices to prove the result for some base $\mathcal{B}$ of V.*

We have seen that there are vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k \in V$ such that

$$V = \langle T, \boldsymbol{v}_1 \rangle \oplus \langle T, \boldsymbol{v}_2 \rangle \oplus \cdots \oplus \langle T, \boldsymbol{v}_k \rangle.$$

Let $T_i = T_{|_{\langle T, \boldsymbol{v}_i \rangle}}$. Then by Lemma (7.1),

$$\chi_T(x) = \chi_{T_1}(x) \ldots \chi_{T_k}(x).$$

Suppose $\chi_{T_i}(x) = x^{d_i} + a_i x^{d_i - 1} + g_i(x)$ where $g_i(x)$ has degree less than $d_i - 1$. Then

$$\chi_{T_1}(x) \ldots \chi_{T_k}(x) = x^{d_1 + \cdots + d_k} + (a_1 + \cdots + a_k) x^{d_1 + \cdots + d_k - 1} + g(x),$$

where the degree of $g(x)$ is less than $d_1 + \cdots + d_k - 1$.

Consequently, $Tr(T) = a_1 + \cdots + a_k = Tr(T_1) + \cdots + Tr(T_k)$. Let $\mathcal{B}_i$ is a basis for $\langle T, \boldsymbol{v}_i \rangle$ and set $\mathcal{B} = \mathcal{B}_1 \sharp \ldots \sharp \mathcal{B}_k$. Then

$$Trace(\mathcal{M}_T(\mathcal{B}, \mathcal{B})) = Trace(\mathcal{M}_{T_1}(\mathcal{B}_1, \mathcal{B}_1)) + \cdots + Trace(\mathcal{M}_{T_k}(\mathcal{B}_k, \mathcal{B}_k))$$

by Lemma (7.2). Therefore, it suffices to prove the result in the special case that T is cyclic: $V = \langle T, \boldsymbol{v} \rangle$ for some vector $\boldsymbol{v} \in V$.

Assume V is cyclic and $V = \langle T, \boldsymbol{v} \rangle$. Then $\mu_T(x) = \chi_T(x) = \mu_{T,\boldsymbol{v}}(x)$. Suppose $\mu_{T,\boldsymbol{v}}(x) = x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$. We have seen that the following is an independent sequence of vectors and consequently a basis for V:

$$\mathcal{B} = (\boldsymbol{v}, T(\boldsymbol{v}), \ldots, T^{n-1}(\boldsymbol{v})).$$

Then $\mathcal{M}_T(\mathcal{B},\mathcal{B}) = C(x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0) =$

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -b_0 \\ 1 & 0 & 0 & \dots & 0 & -b_1 \\ 0 & 1 & 0 & \dots & 0 & -b_2 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & -b_{n-2} \\ 0 & 0 & 0 & \dots & 1 & -b_{n-1} \end{pmatrix}.$$

Thus, $Trace(\mathcal{M}_T(\mathcal{B},\mathcal{B})) = -b_{n-1}$ *as required.*

Corollary 7.4 *Let* V *be a finite-dimensional vector space and* S, T *operators on* V*. Then*

i) $Tr(S+T) = Tr(S) + Tr(T)$*;*

ii) $Tr(ST) = Tr(TS)$*; and*

iii) for a scalar $c, Tr(cT) = cTr(T)$*.*

Proof *i) Let* $\mathcal{B}$ *be a basis for* V*. Then*

$$\begin{aligned} Tr(S+T) &= Trace(\mathcal{M}_{S+T}(\mathcal{B},\mathcal{B})) \\ &= Trace(\mathcal{M}_S(\mathcal{B},\mathcal{B})) + \mathcal{M}_T(\mathcal{B},\mathcal{B})) \\ &= Trace(\mathcal{M}_S(\mathcal{B},\mathcal{B})) + Trace(\mathcal{M}_T(\mathcal{B},\mathcal{B})) \\ &= Tr(S) + Tr(T). \end{aligned}$$

ii) and iii) are left as exercises.

Exercises

1. Let A and B be $n \times n$ matrices. Prove that $Trace(A+B) = Trace(A) + Trace(B)$.

2. Let A be an $n \times n$ matrix and $c \in \mathbb{F}$ a scalar. Prove that $Trace(cA) = cTrace(A)$.

3. Prove Corollary (7.1).

4. Prove Corollary (7.2).

5. Prove part ii) of Corollary (7.4).

6. Prove part iii) of Corollary (7.4).

7. Prove that $(x_1, x_2, x_3) = (0, 0, 0)$ is the only solution to the system of equations

$$\begin{array}{ccccccc} x_1 & + & x_2 & + & x_3 & = & 0, \\ x_1^2 & + & x_2^2 & + & x_3^2 & = & 0, \\ x_1^3 & + & x_2^3 & + & x_3^3 & = & 0. \end{array}$$

8. Assume A is a 3×3 complex matrix and that $Trace(A) = Trace(A^2) = Trace(A^3) = 0$. Prove that $A^3 = 0_{3\times 3}$. Recall, this means that A is ***nilpotent***.

9. Generalize Exercise 8: Assume A is an $n \times n$ complex matrix and $Trace(A^k) = 0$ for $1 \leq k \leq n$. Prove that A is nilpotent.

10. Let V be a finite-dimensional vector space and T on operator on V. Assume $Tr(ST) = 0$ for all $S \in \mathcal{L}(V, V)$. Prove that $T = 0_{V \to V}$.

11. Assume T is an operator on a finite-dimensional real vector space and all the eigenvalues of T are real. Prove that $Tr(T^2) \geq 0$.

12. Assume T is a complex operator such that $T^2 = T$. Prove that $Tr(T)$ is a non-negative integer.

13. Assume $(V, \langle\ ,\ \rangle)$ is a real finite-dimensional inner product space and T is an operator on V. Prove that $Tr(T^*) = Tr(T)$.

14. Assume $(V, \langle\ ,\ \rangle)$ is a complex finite-dimensional inner product space and T is an operator on V. Prove that $Tr(T^*) = \overline{Tr(T)}$.

15. Let V be a finite-dimensional vector space. Denote by $sl(V)$ the collection of all operators with trace zero: $sl(V) := \{T \in \mathcal{L}(V, V) | Tr(T) = 0\}$. Prove that $sl(V)$ is a subspace of $\mathcal{L}(V, V)$ of dimension $n^2 - 1$.

16. Let T be an operator on an inner product space $(V, \langle\ ,\ \rangle)$. Prove that $Tr(T^*T) > 0$ if $T \neq 0_{V \to V}$.

17. Assume V is a finite-dimensional vector space over a field $\mathbb{F}$ of characteristic zero and T is an operator on V with $Tr(T) = 0$. Prove that there is a basis $\mathcal{B}$ for V such that $\mathcal{M}_T(\mathcal{B}, \mathcal{B})$ has all zeros on the diagonal.

18. Let $\mathbb{F}$ be a field and assume $|\mathbb{F}| \geq n$. Let A be an $n \times n$ matrix all of whose diagonal entries are zero. Prove that there exist matrices B, C such that $BC - CB = A$.

19. Assume V is a finite-dimensional vector space over a field $\mathbb{F}$ of characteristic zero and T is on operator on V with $Tr(T) = 0$. Prove that there are operators R and S such that $T = RS - SR$.

7.2 Determinant of a Linear Operator and Matrix

Let V be a finite-dimensional vector space over a field $\mathbb{F}$ and $T : V \to V$ a linear operator. In this section we define what is meant by the determinant of T in terms of the characteristic polynomial of T. We also define what is meant by the determinant of a square matrix by an explicit formula. In our main theorem we prove that the determinant of T is equal to the determinant of $\mathcal{M}_T(\mathcal{B}, \mathcal{B})$ where $\mathcal{B}$ is any basis of V.

What You Need to Know

You will need to have a mastery of the following concepts: basis of a finite-dimensional vector space, linear operator on a vector space, matrix of a linear operator with respect to a basis $\mathcal{B}$, characteristic polynomial of an operator, eigenvalues and eigenvectors of an operator, direct sum decomposition of a vector space, a T-invariant subspace for an operator T on a space V, upper and lower triangular (square) matrix, invertible matrix, block diagonal matrix, and the companion matrix of a polynomial.

We begin with a definition for the determinant of a linear operator:

Definition 7.2 *Let V be a finite-dimensional vector space and T an operator on V. Assume $\chi_T(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$. Then we define the* **determinant** *of T, denoted by $det(T)$, to be $(-1)^n a_0$.*

Example 7.2 *Assume $T \in \mathcal{L}(V)$ is a diagonalizable operator with eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$. Then*

$$\chi_T(x) = (x - \lambda_1)(x - \lambda_2) \ldots (x - \lambda_n)$$

has constant term $(-1)^n \lambda_1 \lambda_2 \ldots \lambda_n$. In this case,

$$det(T) = (-1)^n(-1)^n \lambda_1 \ldots \lambda_n = \lambda_1 \ldots \lambda_n.$$

More generally, assume over some field the distinct eigenvalues of T are $\lambda_1, \lambda_2, \ldots, \lambda_m$. Set $V_{\lambda_i} = \{\boldsymbol{v} \in V | (T - \lambda_i I_V)^{dim(V)}(\boldsymbol{v}) = \mathbf{0}\}$. It is then the case that

$$V = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_m}.$$

We then have

$$\chi_T(x) = (x - \lambda_1)^{dim(V_{\lambda_1})}(x - \lambda_2)^{dim(V_{\lambda_2})} \ldots (x - \lambda_m)^{dim(V_{\lambda_m})}.$$

Consequently, $\chi_T(x)$ *has constant term* $(-1)^n\lambda_1^{dim(V_{\lambda_1})}\dots\lambda_m^{dim(V_{\lambda_m})}$ *and*

$$det(T) = \lambda_1^{dim(V_1)}\dots\lambda_m^{dim(V_m)}.$$

Lemma 7.3 *Let* V *be a finite-dimensional vector space and* T *an operator on* V*. Assume*

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_k,$$

where the V_i *are* T*-invariant. Set* $T_i = T_{|V_i}$*. Then*

$$det(T) = det(T_1) \times det(T_2) \times \cdots \times det(T_k).$$

Proof *Let* $\chi_{T_i}(x) = g_i(x) = x^{d_i} + \cdots + a_i$ *so that* $det(T_i) = (-1)^{d_i}a_i$*. Note that* $n = dim(V) = deg(\chi_T(x)) = d_1 + d_2 + \cdots + d_k$*. It follows from Corollary (7.3) that*

$$\chi_T(x) = g_1(x)g_2(x)\dots g_k(x) = x^n + \cdots + (a_1a_2\dots a_k).$$

Thus, $det(T) = (-1)^n a_1a_2\dots a_k$*. On the other hand,*

$$\begin{aligned} det(T_1)\times\cdots\times det(T_k) &= (-1)^{d_1}a_1 \times (-1)^{d_2}a_2 \times \cdots \times (-1)^{d_k}a_k \\ &= (-1)^{d_1+d_2+\cdots+d_n}a_1a_2\dots a_k \\ &= = (-1)^n a_0a_1\dots a_k = det(T). \end{aligned}$$

Definition 7.3 *Let* $[1,n]$ *denote the set* $\{1,2,\dots,n\}$ *and* S_n *the collection of bijective functions from* $[1,n]$ *to* $[1,n]$ *whose elements we refer to as permutations. One way to denote such a function is to indicate the image of each element. For example*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 8 & 4 & 1 & 7 & 6 & 2 \end{pmatrix}.$$

We can also write a permutation as a product of "disjoint" cycles: (13825)(4)(67) where it is understood that for distinct elements $i_1,\dots,i_t$ of [1,n] that the cycle $(i_1\ i_2\ \dots\ i_t)$ is to be interpreted as the function which fixes every j which is not in $\{i_1,\dots,i_t\}$ and takes i_1 to i_2, i_2 to i_3 and so on, and finally, i_t to i_1. The product of two such cycles is interpreted as the composition of functions, going from right to left so that (13)(12) = (123).

An easy calculation shows that $(1,m)(1,m-1)\dots(13)(12) = (123\dots m)$.

Therefore, every permutation is a product of 2 cycles, also called ***transpositions***. While the number of transpositions used to write a fixed permutation is not unique, the parity of such an expression is unique. For example,

$(23) = (13)(12)(13)$. To see that parity is preserved, set

$$\Delta = \prod_{1 \leq i < j \leq n} (X_i - X_j).$$

For $\tau \in S_n$, define $\tau(\Delta) = \prod_{j>i}(X_{\tau(i)} - X_{\tau(j)})$. This will be $\pm\Delta$. When τ is a transposition, $\tau = (k, l)$, then $\tau(\Delta) = -\Delta$ which can be seen as follows.

First, if $\{i < j\} \cap \{k, l\} = \emptyset$ then τ leaves $X_j - X_i$ invariant. On the other hand, if $i < k$ then τ takes $(X_k - X_i)(X_l - X_i)$ to $(X_l - X_i)(X_k - X_i)$ and so is invariant. Similarly, τ fixes $(X_i - X_k)(X_i - X_l)$ if $l < i$. Suppose then that $k < i < l$. Then τ takes $(X_i - X_k)(X_l - X_i)$ to $(X_i - X_l)(X_k - X_i) = (X_i - X_k)(X_l - X_i)$ and so is again invariant. There is one remaining term: $X_l - X_k$ which τ takes to $X_k - X_l = (-1)(X_l - X_k)$. Thus, $\tau(\Delta) = -\Delta$ as claimed.

One can also see that for permutations σ, γ that $(\sigma\gamma)(\Delta) = \sigma(\gamma(\Delta)$. From this, the parity claim follows.

Definition 7.4 *Say a permutation is* **even** *if it is a product of an even number of transpositions and* **odd** *otherwise. For a permutation σ, we define the* **sign** *of σ, denoted by $sgn(\sigma)$, to be 1 if if σ is even and $sgn(\sigma) = -1$ if σ is odd. Note if τ is a transposition then $sgn(\tau\sigma) = -sgn(\sigma)$.*

We are now ready to define the determinant of a square matrix.

Definition 7.5 *Let* $A = \begin{pmatrix} a_{11} & a_{12}\cdots & a_{1n} & & \\ a_{21} & a_{22} & \cdots & a_{2n} & \\ & \vdots & \vdots & \cdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} & \end{pmatrix}$. *Then*

$$det(A) = \sum_{\pi \in S_n} sgn(\pi) a_{\pi(1),1} a_{\pi(2),2} \cdots a_{\pi(n),n}.$$

Remark 7.2 *If $\pi \in S_n$, then $sgn(\pi) = sgn(\pi^{-1})$ and*

$$\{(\pi(1), 1), (\pi(2), 2), \ldots, (\pi(n), n)\} = \{(1, \pi^{-1}(1)), (2, \pi^{-1}(2)), \ldots (n, \pi^{-1}(n))\}.$$

Moreover, as π ranges over S_n, so does π^{-1}. Consequently, $det(A)$ is also equal to

$$\sum_{\gamma \in S_n} sgn(\gamma) a_{1,\gamma(1)} a_{2,\gamma(2)} \dots a_{n,\gamma(n)}.$$

Our ultimate goal will be to prove the following theorem and draw inferences from it:

MAIN THEOREM

Let V be a finite-dimensional vector space, T an operator on V, and $\mathcal{B} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n)$ a basis for V. Then $det(T) = det(\mathcal{M}_T(\mathcal{B}, \mathcal{B}))$.

Example 7.3

a) Suppose A is upper triangular, $A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & a_{nn} \end{pmatrix}$. Then $det(A) = a_{11}a_{22}\dots a_{nn}$.

We can see this as follows: Since $a_{i1} = 0$ for $i > 1$ the only permutations π for which the product $a_{\pi(1),1}a_{\pi(2),2}\cdots a_{\pi(n),n} \neq 0$ are those with $\pi(1) = 1$. So we may assume $\pi(1) = 1$ and consequently, $\pi(2) \neq 1$. Since $a_{i2} = 0$ for $i > 2$ the only permutations with $\pi(1) = 1$ and such that the product $a_{\pi(1),1}a_{\pi(2),2}\cdots a_{\pi(n),n} \neq 0$ have $\pi(2) = 2$. We can continue this way and see that the only permutation for which $a_{\pi(1),1}a_{\pi(2),2}\cdots a_{\pi(n),n} \neq 0$ is the identity permutation.

b) Suppose A is lower triangular, $A = \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$. Then $det(A) = a_{11}a_{22}\dots a_{nn}$.

The proof here is similar to a) except we work backwards: We first show if $a_{\pi(1),1}a_{\pi(2),2}\cdots a_{\pi(n),n} \neq 0$ then it must be the case that $\pi(n) = n$, then show that $\pi(n-1) = n-1$, and continue to eventually show that $\pi = Id_{[1,n]}$.

Note that a diagonal matrix is both upper and lower triangular so these examples apply to the case that a matrix is diagonal. In particular, the determinant of I_n is 1.

c) If the matrix $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$ has a row of zeros, then $det(A) = 0$.

This follows since at least one of the factors of $a_{1,\pi(1)}\dots a_{n,\pi(n)}$ is zero and therefore the product is zero.

In the following we introduce types of matrices which will be referred to as elementary matrices. The crux of our proof will be to show that for any elementary matrix E and an arbitrary matrix $A, det(EA) = det(E)det(A)$.

Definition 7.6 .

1) For a scalar c, denote by $T_{ij}(c)$ the matrix obtained from I_n by adding c times the i^{th} row to the j^{th} row.

2) For a pair of natural numbers $1 \leq k < l \leq n$, denote by $P_{kl} = (a_{ij})$ the matrix obtained from I_n by exchanging the k^{th} and l^{th} rows.

3) For a non-zero scalar c and a natural number $i, 1 \leq i \leq n$, denote by $D_i(c)$ the matrix obtained from the identity matrix by multiplying the i^{th} row by c.

The matrices $T_{ij}(c), P_{kl}$, and $D_i(c)$ are referred to as **elementary matrices**.

Remark 7.3 *1) If $i < j$ then $T_{ij}(c)$ is upper triangular with ones on the diagonal. If $i > j$ then $T_{ij}(c)$ is lower triangular with ones on the diagonal. In either case, $det(T_{ij}(c)) = 1$.*

2) The determinant of P_{kl} is -1 as can be seen as follows: Denote the elements of P_{kl} by a_{ij}. Suppose $\pi \in S_n$ and $a_{\pi(1),1}a_{\pi(2),2}\dots a_{\pi(n),n} \neq 0$. Then for $j \notin \{k,l\}$ we must have $\pi(j) = j$. On the other hand $a_{kk} = a_{ll} = 0$ and $a_{kl} = a_{lk} = 1$. It must then be the case that $\pi(k) = l, \pi(l) = k$ and so π is the transposition (kl), which has $sgn((kl)) = -1$. Consequently, $det(P_{kl}) = -1$ as claimed.

3) If $1 \leq i \leq n$ and $c \neq 0$ is a scalar, then $det(D_i(c)) = c$. This follows since $D_i(c)$ is a diagonal matrix all of whose diagonal entries are 1 except one which is c.

Lemma 7.4 *Assume the matrix B is obtained from the matrix A by exchanging the k^{th} and l^{th} rows. Then $det(B) = -det(A)$.*

Proof *Set $B = (b_{ij})$ and $\tau = (kl)$. Then for all i and j, $b_{ij} = a_{\tau(i),j}$. It then follows that for $\pi \in S_n$*

$$b_{\pi(1),1}b_{\pi(2),2}\dots b_{\pi(n),n} = a_{\pi\tau(1),1}a_{\pi\tau(2),2}\dots a_{\pi\tau(n),n}$$

and therefore

$$\begin{aligned} det(B) &= \sum_{\pi \in S_n} sgn(\pi) b_{\pi(1),1}b_{\pi(2),2}\dots b_{\pi(n),n} \\ &= \sum_{\pi \in S_n} sgn(\pi) a_{\pi\tau(1),1}a_{\pi\tau(2),2}\dots a_{\pi\tau(n),n}. \end{aligned}$$

Since $\tau = (kl)$ is a transposition, it follows that $sgn(\pi\tau) = -sgn(\pi)$ and therefore

$$sgn(\pi)a_{\pi\tau(1),1}a_{\pi\tau(2),2}\dots a_{\pi\tau(n),n} = -sgn(\pi\tau)a_{\pi\tau(1),1}a_{\pi\tau(2),2}\dots a_{\pi\tau(n),n}.$$

Also, as π ranges over S_n so does $\pi\tau$. Setting $\gamma = \pi\tau$ we get

$$\sum_{\pi\in S_n} sgn(\pi)a_{\pi\tau(1),1}a_{\pi\tau(2),2}\dots a_{\pi\tau(n),n}$$
$$= -\sum_{\gamma\in S_n} sgn(\gamma)a_{\gamma(1),1}a_{\gamma(2),2}\dots a_{\gamma(n),n} = -det(A).$$

Corollary 7.5 *For a matrix $A, det(P_{kl}A) = det(P_{kl})det(A)$.*

Corollary 7.6 *Assume in the field $\mathbb{F}$ that $1+1\neq 0$. Let $A \in M_{nn}(\mathbb{F})$. If two rows of A are identical then $det(A) = 0$.*

Proof *Suppose rows k and l of A are identical. Then when we switch these two rows the resulting matrix has determinant equal to $-det(A)$. But this matrix is identical to A and therefore $-det(A) = det(A)$. Then $2det(A) = 0$, whence $det(A) = 0$.*

Lemma 7.5 *Assume the characteristic of the field $\mathbb{F}$ is two. Let $A \in M_{nn}(\mathbb{F})$. If two rows of A are identical then $det(A) = 0$.*

Proof *Note that since the characteristic of $\mathbb{F}$ is two, $1 = -1$ and so we can drop the sign in the expression of the determinant. Also note that it is now the case if a matrix B is obtained from the matrix A by exchanging two rows then $det(B) = det(A)$. Assume now that the $i^{th} < j^{th}$ rows are identical. By exchanging the i^{th} row with the $(n-1)^{st}$ row and the j^{th} row with the n^{th} row, we may may assume that $(n-1)^{st}$ and n^{th} rows are identical. Now let π an arbitrary permutation. Let π' be the permutation defined as follows: $\pi'(k) = \pi(k)$ if $k < n-1, \pi'(n-1) = \pi(n)$, and $\pi'(n) = \pi(n-1)$, that is $\pi' = (\pi(n-1)\pi(n))\pi$. By the way we have defined π', it follows that*

$$a_{1,\pi(1)}\dots a_{n-1,\pi(n-1)}a_{n,\pi(n)} = a_{1,\pi'(1)}\dots a_{n-1,\pi'(n-1)}a_{n,\pi'(n)}.$$

Consequently, the sum of these two terms is zero since the characteristic is two. Summing over all such pairs it then follows that $det(A) = 0$.

Lemma 7.6 *Let the matrix B be obtained from the matrix A by multiplying the k^{th} row of A by the scalar c. Then $det(B) = c\ det(A)$.*

Proof *We use the expression*

$$det(A) = \sum_{\gamma \in S_n} sgn(\gamma) a_{1,\gamma(1)} a_{2,\gamma(2)} \dots a_{n,\gamma(n)}$$

for computing the determinant.

Note that each $b_{ij} = a_{ij}$ if $i \neq k$ and $b_{kj} = ca_{kj}$. Then for each γ

$$sgn(\gamma) b_{1,\gamma(1)} \dots b_{n,\gamma(n)}$$

$$= sgn(\gamma) a_{1,\gamma(1)} \dots a_{k-1,\gamma(k-1)} (ca_{k,\gamma(k)}) a_{k+1,\gamma(k+1)} \dots a_{n,\gamma(n)}$$
$$= c \times sgn(\gamma) a_{1,\gamma(1)} a_{2,\gamma(2)} \dots a_{n,\gamma(n)}.$$

Summing over all $\gamma \in S_n$ we get $det(B) = c \times det(A)$ as required.

Corollary 7.7 *Let $D_k(c)$ be the matrix obtained from I_n by multiplying the k^{th} row by the scalar c. Then for any matrix A,*

$$det(D_k(c)A) = c\ det(A) = det(D_k(c)) \times det(A).$$

Lemma 7.7 *Let the $n \times n$ matrix A have rows $\boldsymbol{a}_i$, the matrix B have rows $\boldsymbol{b}_i$, and assume that $\boldsymbol{a}_i = \boldsymbol{b}_i$ for $i \neq k$. Suppose C is the matrix with rows $\boldsymbol{c}_i$, where $\boldsymbol{c}_i = \boldsymbol{a}_i = \boldsymbol{b}_i$ for $i \neq k$ and $\boldsymbol{c}_k = \boldsymbol{a}_k + \boldsymbol{b}_k$. Then*

$$det(C) = det(A) + det(B).$$

Proof *We use the expression*

$$det(C) = \sum_{\gamma \in S_n} sgn(\gamma) c_{1,\gamma(1)} c_{2,\gamma(2)} \dots c_{n,\gamma(n)}$$

for computing the determinant.

Each term $c_{1,\gamma(1)} c_{2,\gamma(2)} \dots c_{n,\gamma(n)}$ has the form

$$a_{1,\gamma(1)} \dots a_{k-1,\gamma(k-1)} c_{k,\gamma(k)} a_{k+1,\gamma(k+1)} \dots a_{n,\gamma(n)}$$

since $c_{ij} = a_{ij}$ for $i \neq k$. On the other hand, $c_{kj} = a_{kj} + b_{kj}$ whence

$$c_{1,\gamma(1)}c_{2,\gamma(2)}\cdots c_{n,\gamma(n)}$$

$$= a_{1,\gamma(1)}\cdots a_{k-1,\gamma(k-1)}(a_{k,\gamma(k)} + b_{k,\gamma(k)})a_{k+1,\gamma(k+1)}\cdots a_{n,\gamma(n)}$$

$$= a_{1,\gamma(1)}\cdots a_{k-1,\gamma(k-1)}a_{k,\gamma(k)}a_{k+1,\gamma(k+1)}\cdots a_{n,\gamma(n)}$$

$$+a_{1,\gamma(1)}\cdots a_{k-1,\gamma(k-1)}b_{k,\gamma(k)}a_{k+1,\gamma(k+1)}\cdots a_{n,\gamma(n)}$$

$$= a_{1,\gamma(1)}\cdots a_{k-1,\gamma(k-1)}a_{k,\gamma(k)}a_{k+1,\gamma(k+1)}\cdots a_{n,\gamma(n)}$$

$$+b_{1,\gamma(1)}\cdots b_{k-1,\gamma(k-1)}b_{k,\gamma(k)}b_{k+1,\gamma(k+1)}\cdots b_{n,\gamma(n)}$$

since $b_{ij} = a_{ij}$ for $i \neq k$. Multiplying by $sgn(\gamma)$ and summing over all $\gamma \in S_n$ we get the desired result.

Corollary 7.8 *Assume the matrix C is obtained from the matrix A by adding c times the l^{th} row of A to the k^{th} row of A. Then $det(C) = det(A)$.*

Proof *Let the rows of A be $\boldsymbol{a}_i, 1 \leq i \leq n$. Let the rows of the matrix B be $\boldsymbol{b}_i$ with $\boldsymbol{b}_i = \boldsymbol{a}_i$ for $i \neq k$ and $\boldsymbol{b}_k = c\boldsymbol{a}_l$. From Lemma (7.7), $det(C) = det(A) + det(B)$. Let B' be the matrix with rows $\boldsymbol{b}'_i$ where $\boldsymbol{b}'_i = \boldsymbol{b}_i$ for $i \neq k$ and $\boldsymbol{b}'_k = \boldsymbol{b}_l$. Then $det(B) = c\ det(B')$ by Lemma (7.6). However, B' has two identical rows and therefore $det(B') = 0$ by Corollary (7.6) and Lemma (7.5). Thus, $det(B) = 0$ and $det(C) = det(A)$ as claimed.*

Corollary 7.9 *Let A be an $n \times n$ matrix. If $i \neq j$ and c is scalar, then*

$$det(T_{ij}(c)A) = det(A) = det(T_{ij}(c))det(A).$$

Putting Corollaries (7.5), (7.7), and (7.9) together we have the following:

Theorem 7.3 *Let A be an $n \times n$ matrix and E be an $n \times n$ elementary matrix. Then $det(EA) = det(E)det(A)$.*

Remark 7.4 *a) If E is an elementary matrix, then E is invertible and the inverse of E is of the same type:*

$$D_i(c)^{-1} = D_i\left(\frac{1}{c}\right), P_{ij}^{-1} = P_{ij}, T_{ij}(c)^{-1} = T_{ij}(-c).$$

b) If E is an elementary matrix then the transpose of E, E^{tr}, is an elementary matrix of the same type and $det(E^{tr}) = det(E)$:

$$D_i(c)^{tr} = D_i(c), P_{ij}^{tr} = P_{ij}, T_{ij}(c)^{tr} = T_{ji}(c).$$

The following result is usually proved in an elementary linear algebra course:

Lemma 7.8 *i) The reduced echelon form of an $n \times n$ invertible matrix A is I_n.*

ii) If A is a non-invertible $n \times n$ matrix then the reduced echelon form of A has a zero row.

The following is a consequence of this lemma:

Corollary 7.10 *Every invertible matrix is a product of elementary matrices.*

A consequence of Corollary (7.10) is

Corollary 7.11 *Let B be an $n \times n$ matrix. Then B is invertible if and only if $det(B) \neq 0$.*

Proof *Write $B = E_k E_{k-1} \dots E_1 I_n$, where E_i are elementary. We have already proved for an elementary matrix E and a matrix A that $det(EA) = det(E) \times det(A)$. Then for each $i < k$,*

$$det(E_{i+1}(E_i \dots E_1 I_n)) = det(E_{i+1}) det(E_i \dots E_1 I_n)$$

and, consequently,

$$det(A) = det(E_k) \times det(E_{k-1}) \times \cdots \times det(E_1) \times det(I_n).$$

Since $det(E_i) \neq 0$ for each $i, det(A) \neq 0$.

On the other hand, suppose B is not invertible. Let R be the reduced echelon form of B. Then there are elementary matrices $E_1, \dots, E_k$ so that $B = E_k E_{k-1} \dots E_1 R$. By the same reasoning as above,

$$det(B) = det(E_k) \times det(E_{k-1}) \times \cdots \times det(E_1) \times det(R).$$

However, R has a zero row and so $det(R) = 0$. Therefore $det(B) = 0$.

We can now prove a fundamental theorem about determinants of matrices:

Theorem 7.4 *For $n \times n$ matrices A and B, $det(AB) = det(A)det(B)$.*

Proof *Suppose A or B is not invertible then AB is not invertible. Then by Corollary (7.11) $det(AB) = 0$. Also by the aforementioned corollary, either $det(A) = 0$ or $det(B) = 0$, whence $det(A)det(B) = 0$. We may therefore suppose A and B are invertible. Write A as a product of elementary matrices: $A = E_kE_{k-1}\dots E_1$. Then*

$$\begin{aligned} det(AB) &= det(E_kE_{k-1}\dots E_1B) \\ &= det(E_k)det(E_{k-1}\dots E_1B) \\ &\vdots \\ &= det(E_k)det(E_{k-1}\dots det(E_1)det(B) = det(A)det(B). \end{aligned}$$

Corollary 7.12 *Assume A and B are $n \times n$ matrices and $AB = I_n$. Then $det(B) = \dfrac{1}{det(A)}$.*

In the next result, we show that the determinant of a matrix and its transpose are the same. This has an important implication: anything that we have proved about the relationship of the determinant of a matrix to its rows is equally true of its columns. For example, if a matrix B is obtained from a matrix A by exchanging two columns, then $det(B) = -det(A)$.

Corollary 7.13 *Let A be an $n \times n$ matrix. Then $det(A^{tr}) = det(A)$.*

Proof *If A is not invertible, then neither is A^{tr} and then $det(A) = 0 = det(A^{tr})$ by Corollary (7.12). Thus, we may assume that A is invertible. Then there are elementary matrices $E_1, E_2, \dots, E_k$ such that $A = E_k \dots E_1$ and, as in the proof of Theorem (7.4), we have $det(A) = det(E_k)\dots det(E_1)$. Now $A^{tr} = (E_k \dots E_1)^{tr} = E_1^{tr} \dots E_k^{tr}$ and $det(A^{tr}) = det(E_1^{tr})\dots det(E_k^{tr})$. However, as noted in part b) of Remark (7.4), for an arbitrary elementary matrix E, $det(E^{tr}) = det(E)$. In particular, for $1 \leq i \leq k, det(E_i) = det(E_i^{tr})$ and therefore $det(A) = det(E_k)\dots det(E_1) = det(E_1^{tr})\dots det(E_k^{tr}) = det(A^{tr})$.*

The next result tells us that similar matrices have the same determinant:

Corollary 7.14 *If A is an $n \times n$ matrix and Q is an invertible $n \times n$ matrix then $det(Q^{-1}AQ) = det(A)$.*

Proof *By Theorem (7.4), $det(Q^{-1}AQ) = det(Q^{-1})det(A)det(Q) = det(Q^{-1})det(Q)det(A) = det(A)$ by Corollary (7.12).*

An immediate consequence of Corollary (7.14) is:

Corollary 7.15 *Let V be a finite-dimensional vector space, T an operator on V, and $\mathcal{B}, \mathcal{B}'$ bases for V. Then $det(\mathcal{M}_T(\mathcal{B}, \mathcal{B})) = det(\mathcal{M}_T(\mathcal{B}', \mathcal{B}'))$.*

The next result expresses the determinant of a block diagonal matrix with two diagonal blocks in terms of the determinants of the blocks.

Lemma 7.9 *Assume C is a block diagonal matrix with two diagonal blocks A and B. Then $det(C) = det(A) \times det(B)$.*

Proof *Let A be a $k \times k$-matrix and B be an $l \times l$-matrix so that $n = k + l$. Let the entries of A be (a_{ij}) and the entries of B be (b_{ij}). Then the entries of C are (c_{ij}), where*

$c_{ij} = a_{ij}$ if $1 \leq i, j \leq k$, $c_{ij} = 0$ if $1 \leq i \leq k, j > k$ or $1 \leq j \leq k, i > k$ and

$c_{ij} = b_{i+k,j+k}$ for $k + 1 \leq i, j \leq n = k + l$.

Now if $\sigma \in S_n$ and $c_{\sigma(1),1} \dots c_{\sigma(n),n} \neq 0$, then it must be the case that σ leaves $[1, k]$ and $[k + 1, n]$ invariant. In this case set,

$$\sigma_1 = \sigma_{|_{[1,k]}}, \sigma_2 = \sigma_{|_{[k+1,n]}}.$$

Also, let $\sigma_2' \in S_l$ be given by $\sigma_2'(j) = \sigma_2(j + l) - l$. Note that $sgn(\sigma) = sgn(\sigma_1\sigma_2) = sgn(\sigma_1)sgn(\sigma_2) = sgn(\sigma_1)sgn(\sigma_2')$.

Now we have

$$\begin{aligned} det(C) &= \sum_{\sigma \in S_n} sgn(\sigma) c_{\sigma(1),1} \dots c_{\sigma(n),n} \\ &= \sum_{\sigma \in S_n} sgn(\sigma) c_{\sigma_1(1),1} \dots c_{\sigma_1(k),k} c_{\sigma_2(k+1),k+1} \dots c_{\sigma_2(n),n} \\ &= \sum_{\sigma_1 \in S_k} \sum_{\sigma_2' \in S_l} sgn(\sigma_1\sigma_2') a_{\sigma_1(1),1} \dots a_{\sigma_1(k),k} b_{\sigma_2'(1),1} \dots b_{\sigma_2'(l),l} \\ &= \left(\sum_{\sigma_1 \in S_k} sgn(\sigma_1) a_{\sigma_1(1),1} \dots a_{\sigma_1(k),k} \right) \left(\sum_{\sigma_2' \in S_l} sgn(\sigma_2') b_{\sigma_2'(1),1} \dots b_{\sigma_2'(l),l} \right) \\ &= det(A) \times det(B). \end{aligned}$$

Theorem 7.5 *Let A be a block diagonal matrix with diagonal blocks $A_1, A_2, \ldots, A_k$. Then $det(A) = det(A_1) \times det(A_2) \times det(A_k)$.*

Proof *This follows from Lemma (7.9) by induction on k.*

We are now in a position to prove our main theorem:

Theorem 7.6 *Let V be a finite-dimensional vector space, T an operator on V, and $\mathcal{B}$ a basis for V. Then $det(T) = det(\mathcal{M}_T(\mathcal{B}, \mathcal{B}))$.*

Proof *In light of Corollary (7.15) we need only show that there exists some basis $\mathcal{B}$ of V such that $det(T) = det(\mathcal{M}_T(\mathcal{B}, \mathcal{B}))$. Since we can decompose V into a direct sum of T-invariant subspaces on which T is cyclic, by Lemma (7.3) and Theorem (7.5), it suffices to prove the result when T is cyclic, that is, when there is a vector $\boldsymbol{v} \in V$ such that $V = \langle T, \boldsymbol{v} \rangle$.*

Let $\mu_{T,\boldsymbol{v}}(x) = \chi_T(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Set $\boldsymbol{v}_1 = \boldsymbol{v}$ and $\boldsymbol{v}_k = T^{k-1}(\boldsymbol{v})$ for $2 \leq k \leq n$. Then $\mathcal{B} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ is a basis for V and $\mathcal{M}_T(\mathcal{B}, \mathcal{B}) = C(\mu_T(x))$, the companion matrix of $\mu_T(x)$. To complete the proof, we must show that

$$det(C(\mu_T(x)) = (-1)^n a_0.$$

Recall,

$$C(\mu_T(x)) = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & -a_{n-2} \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}.$$

The only term that is non-zero in the expansion of this determinant is

$$a_{21}a_{32}\ldots a_{n,n-1}a_{1n} = 1^{n-1}(-a_0).$$

The corresponding permutation is the n-cycle $\pi = (123\ldots n)$. The permutation π is even if n is odd and odd if n is even. In particular, $sgn(\pi) = (-1)^{n-1}$. Therefore,

$$det(C(\mu_T(x)) = -a_0 \times (-1)^{n-1} = (-1)^n \times a_0$$

as required.

We can make use of Theorem (7.6) together with the properties we have established for the determinant of a matrix to show that the same properties hold for the determinant of an operator. In our first result, we prove that the determinant of a product of operators is the product of the determinants.

Corollary 7.16 *Let V be a finite-dimensional vector space and S, T linear operators on V. Then $det(ST) = det(S)det(T)$.*

Proof *Let $\mathcal{B}$ be a basis for V. Then $det(ST) = det(\mathcal{M}_{ST}(\mathcal{B}, \mathcal{B})) = det(\mathcal{M}_S(\mathcal{B}, \mathcal{B})\mathcal{M}_T(\mathcal{B}, \mathcal{B})) = det(\mathcal{M}_S(\mathcal{B}, \mathcal{B}))det(\mathcal{M}_T(\mathcal{B}, \mathcal{B})) = det(S)det(T)$.*

We next show that an operator is invertible if and only if it has non-zero determinant.

Corollary 7.17 *Let V be a finite-dimensional vector space and T an operator on V. Then the following hold:*

i) T is invertible if and only if $det(T) \neq 0$.

ii) If T is invertible, then $det(T^{-1}) = \frac{1}{det(T)}$.

Proof *i) Let $\mathcal{B}$ be a basis for V. Then T is invertible if and only if $\mathcal{M}_T(\mathcal{B}, \mathcal{B})$ is invertible. But $\mathcal{M}_T(\mathcal{B}, \mathcal{B})$ is invertible if and only if $det(\mathcal{M}_T(\mathcal{B}, \mathcal{B})) \neq 0$. Since $det(T) = det(\mathcal{M}_T(\mathcal{B}, \mathcal{B})), T$ is invertible if and only if $det(T) \neq 0$.*

ii) Assume T is invertible. Then $1 = det(I_V) = det(TT^{-1}) = det(T)det(T^{-1})$ and consequently, $det(T^{-1}) = \frac{1}{det(T)}$.

Theorem 7.7 *Let V be a finite-dimensional vector space, T an operator on V, and $\mathcal{B}$ a basis for V. Set $A = \mathcal{M}_T(\mathcal{B}, \mathcal{B})$. Then $\chi_T(x) = det(xI_n - A)$.*

Proof *By our theorems on the characteristic polynomial and determinants of block diagonal matrices, it suffices to prove this when T is cyclic. Thus, assume that $V = \langle T, \boldsymbol{v} \rangle$ and let $\mu_T(x) = \chi_T(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Set $\boldsymbol{v}_1 = \boldsymbol{v}$, $\boldsymbol{v}_k = T^{k-1}(\boldsymbol{v})$ for $2 \leq k \leq n$ and $\mathcal{B} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$, a basis for V. As shown in the proof of Theorem (7.6), the matrix of T with respect to $\mathcal{B}$ is the companion matrix of $\mu_T(x)$:*

$$\mathcal{M}_T(\mathcal{B},\mathcal{B}) = C(\mu_T(x)) = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & -a_{n-2} \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix}.$$

To complete the proof, we have to show that

$$det \begin{pmatrix} x & 0 & \dots & 0 & a_0 \\ -1 & x & \dots & 0 & a_1 \\ \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & \dots & x & a_{n-2} \\ 0 & 0 & \dots & -1 & x+a_{n-1} \end{pmatrix} = \mu_T(x) = \chi_T(x).$$

Set $B = xI_n - A$ and denote the (i,j)-entry of B by b_{ij}. We then have

$$det(B) = \sum_{\sigma \in S_n} sgn(\sigma) b_{\sigma(1),1} \dots b_{\sigma(n),n}. \tag{7.1}$$

Suppose $\sigma(n) = 1$. Look at the matrix obtained when the row and column of b_{1n} are deleted. This matrix is upper triangular with -1's on the diagonal. So there is only one permutation σ with $\sigma(n) = 1$, such that $b_{\sigma(1),1} \dots b_{\sigma(n),n} \neq 0$, namely, the $n-$cycle $(12\dots n)$ which has sign $(-1)^{n-1}$. Thus, the only term in Equation (7.1) containing b_{1n} which is not zero is $(-1)^{n-1}(-1)^{n-1}b_{1n} = a_0$.

Next suppose that $\sigma(n) = 2$. The matrix obtained when the row and column of b_{2n} are deleted is upper triangular with one x and $(n-2)$ -1's on the diagonal. Thus there is a unique permutation σ with $\sigma(n) = 2$ giving a non-zero value, namely, $\sigma = (1)(23\dots n)$. The sign of this permutation is $(-1)^{n-2}$ and the term we get is $(-1)^{n-2}x(-1)^{n-2}b_{2n} = a_1 x$. In a similar fashion, we get the only possibly non-zero term in the determinant containing b_{kn} with $k < n$ is $b_{kn}x^k = a_k x^k$.

On the other hand, consider terms of Equation (7.1) which contain $b_{nn} = x + a_{n-1}$. Suppose a permutation σ fixes $n, \sigma(n) = n$. The matrix obtained by deleting the n^{th} row and n^{th} column is lower triangular with x's on the diagonal. This implies that the only possible permutation σ for which the term $b_{\sigma(1),1} \dots b_{\sigma(n-1),n-1} b_{n,n}$ is not zero is the identity permutation. In this case, the sign is +1 and the product of the entries is $x^{n-1}(x + b_{nn}) = x^{n-1}(x + a_{n-1}) = x^n + a_{n-1}x^{n-1}$. Adding all the non-zero terms we get $x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 = \mu_T(x) = \chi_T(x)$.

As a consequence of Theorem (7.7), there is now some real meaning to the Cayley–Hamilton theorem: If T is an operator on a finite-dimensional vector space and we set $\chi_T(x) = det(xI_V - T)$, then $\chi_T(T) = 0_{V \to V}$.

We complete this section by proving a useful formula for computing the determinant of a square matrix. It is known as the **cofactor expansion** in the n^{th} row.

Theorem 7.8 *Let A be an $n \times n$ matrix. For a pair (i,j) with $1 \leq i,j \leq n$ let A_{ij} denote the $(n-1) \times (n-1)$ matrix obtained from A by deleting the i^{th} row and the j^{th} column. Set $M_{ij}(A) = det(A_{ij})$ and $C_{ij} = C_{ij}(A) = (-1)^{i+j}M_{ij}(A)$. Then*

$$det(A) = a_{n1}C_{n1} + a_{n2}C_{n2} + \cdots + a_{nn}C_{nn}.$$

Proof *For $1 \leq j \leq n$, let $S_{n,j}$ denote the collection of permutations $\sigma \in S_n$ such that $\sigma(j) = n$. Then $S_n = S_{n,1} \cup S_{n,2} \cup \cdots \cup S_{n,n}$ and for $i \neq j$, $S_{n,j} \cap S_{n,k} = \emptyset$. Therefore,*

$$det(A) = \sum_{j=1}^{n} \left[\sum_{\sigma \in S_{n,j}} sgn(\sigma) a_{\sigma(1),1} \dots a_{\sigma(n),n} \right].$$

Since for $\sigma \in S_{n,j}, \sigma(j) = n$, we have

$$\sum_{j=1}^{n} \left[\sum_{\sigma \in S_{n,j}} sgn(\sigma) a_{\sigma(1),1} \dots a_{\sigma(n),n} \right]$$

$$= \sum_{j=1}^{n} a_{nj} \sum_{\sigma \in S_{n,j}} sgn(\sigma) a_{\sigma(1),1} \dots a_{\sigma(j-1),j-1} a_{\sigma(j+1),j+1} \dots a_{\sigma(n),n}.$$

Setting

$$\kappa_j = \sum_{\sigma \in S_{n,j}} sgn(\sigma) a_{\sigma(1),1} \dots a_{\sigma(j-1),j-1} a_{\sigma(j+1),j+1} \dots a_{\sigma(n),n}$$

it suffices to prove that $\kappa_j = C_{nj}$.

Now set $\tau_n = I_{[1,n]}$, the identity element of S_n, and for $j < n$ let τ_j be the transposition which interchanges j and n and fixes all other $k, 1 \leq k \leq n-1$. Also, let H be the subgroup of S_n of those permutations which fix n. Then H is isomorphic to S_{n-1} by the map, which takes $\sigma \in H$ to its restriction to $\{1, 2, \dots, n-1\}$. It is then the case that $S_{n,j} = H\tau_j = \{\sigma\tau_j | \sigma \in H\}$.

We next show that $\kappa_n = C_{nn} = (-1)^{n+n}det(A_{nn}) = det(A_{nn})$. This follows immediately since

$$\kappa_n = \sum_{\sigma \in H} sgn(\sigma) a_{\sigma(1),1} \dots a_{\sigma(n-1),n-1} = det(A_{nn}).$$

Now assume that $j < n$. *If* $i \neq j, i < n$, *and* $\sigma \in H$, *then* $\tau_j(i) = i$ *and therefore* $(\sigma\tau_j)(i) = \sigma(i)$. *On the other hand,* $(\sigma\tau_j)(n) = \sigma(j)$. *Therefore, if we set* $\gamma = \sigma\tau_j$ *we have*

$$a_{\gamma(1),1} \cdots a_{\gamma(j-1),j-1} a_{\gamma(j+1),j+1} \cdots a_{\gamma(n),n}$$

$$= a_{\sigma(1),1} \cdots a_{\sigma(j-1),j-1} a_{\sigma(j+1),j+1} \cdots a_{\sigma(j),n}.$$

Thus,

$$\kappa_j = \sum_{\sigma \in H} sgn(\sigma\tau_j) a_{\sigma(1),1} \cdots a_{\sigma(j-1),j-1} a_{\sigma(j+1),j+1} \cdots a_{\sigma(j),n}.$$

Since $sgn(\sigma\tau_j) = sgn(\sigma) sgn(\tau_j)$ *and* $sgn(\tau_j) = -1$ *we have* $\kappa_j = -C_j$, *where*

$$C_j = \sum_{\sigma \in H} sgn(\sigma) a_{\sigma(1),1} \cdots a_{\sigma(j-1),j-1} a_{\sigma(j+1),j+1} \cdots a_{\sigma(j),n}.$$

Now C_j *is nothing more than the determinant of the matrix obtained from* A_{nj} *by placing the* $(n-1)^{st}$ *column of* A_{nj} *after the* $(j-1)^{st}$ *column of* A_{nj}. *This can be realized by* $n - j - 1$ *exchanges of columns, and therefore* $C_j = (-1)^{n-j-1} det(A_{nj})$, *and consequently,* $\kappa_j = (-1)^{n-j} det(A_{nj}) = (-1)^{n+j} det(A_{nj}) = C_{nj}$.

Exercises

1. Use properties of determinants to prove that one can compute the determinant of a matrix using a cofactor expansion in any row:

$$det(A) = a_{i1}C_{i1} + a_{i2}C_{i2} + \cdots + a_{in}C_{in}.$$

2. Prove that one can compute the determinant of a matrix using a cofactor expansion in any column:

$$det(A) = a_{1j}C_{1j} + a_{2j}C_{2j} + \cdots + a_{nj}C_{nj}.$$

3. Let T be an operator on a finite-dimensional inner product space $(V, \langle\ ,\ \rangle)$. Prove that $det(T^*) = \overline{det(T)}$.

4. Let J_n denote the $n \times n$ matrix, all of whose entries are 1. Let j_n denote the

$n \times 1$ matrix, all of whose entries are 1. And, for $1 \leq i < n$, set $\boldsymbol{v}_i = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \\ 0 \\ \vdots \\ -1 \end{pmatrix}$,

where the 1 occurs in the i^{th} position. Prove the following:

i) j_n is an eigenvector of J_n with eigenvalue n.

ii) $(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_{n-1})$ is a basis for $null(J_n)$.

iii) $(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_{n-1}, j_n)$ is a basis for $\mathbb{R}^n$.

5. Let a and b be scalars and set $A = aI_n + bJ_n$. Prove that A is similar to the diagonal matrix $diag\{a, a, \dots, a, a + bn\}$ and conclude that

$$det(A) = a^{n-1}(a + bn).$$

6. Let $\alpha_1, \dots, \alpha_n$ be distinct scalars (in an arbitrary field). We previously proved that there is a basis $\mathcal{B} = (f_1, f_2, \dots, f_n)$ of $\mathbb{F}_{(n-1)}[x]$ such that $f_i(\alpha_j) = 0$ if $j \neq i$ and $f_i(\alpha_i) = 1$. Moreover, for a polynomial $f \in \mathbb{F}_{(n-1)}[x]$, the coordinate vector of f with respect to $\mathcal{B}$ is given by

$$[f]_{\mathcal{B}} = \begin{pmatrix} f(\alpha_1) \\ f(\alpha_2) \\ \vdots \\ f(\alpha_n) \end{pmatrix}.$$

As a consequence the change of basis matrix from the standard basis $\mathcal{S} = (1, x, x^2, \dots, x^n)$ to $\mathcal{B}$ is

$$\mathcal{M}_{I_V}(\mathcal{S}, \mathcal{B}) = \begin{pmatrix} 1 & 1 & \dots & 1 & \\ \alpha_1 & \alpha_2 & \dots & \alpha_n & \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 & \\ \vdots & \vdots & \vdots & \dots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} & \end{pmatrix}.$$

Such a matrix is called a Vandermonde matrix. A previous exercise asked you to prove this matrix is invertible. Now prove that its determinant is

$$\prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i).$$

7. Let A be an $n \times n$ matrix with entries a_{ij} and cofactors C_{ij}. Use the fact that a matrix which has two identical rows has zero determinant to prove that, for any $i \neq j$,

$$a_{j1}C_{i1} + a_{j2}C_{i2} + \cdots + a_{jn}C_{in} = 0.$$

8. Define the ***adjoint***, $Adj(A)$, of the matrix A to be the matrix whose (i, j)-entry is the (j, i)-cofactor, C_{ji} of A. Prove that $A(Adj(A)) = det(A)I_n$.

9. Let A be an invertible $n \times n$ matrix and assume that the entries of both A and A^{-1} are integers. Prove that $det(A) = \pm 1$.

10. Assume A is an $n \times n$ matrix with entries in $\mathbb{Z}$ and $det(A) = \pm 1$. Prove that A^{-1} is an integer matrix.

11. Let T be a Hermitian operator on a finite-dimensional complex inner product space $(V, \langle\ ,\ \rangle)$. Prove that $det(A) \in \mathbb{R}$.

12. Assume T is an operator on a finite dimension inner product space $(V, \langle\ ,\ \rangle)$. Prove $det(T^*T)$ is a non-negative real number and is greater than zero if and only if T is invertible.

13. Let T be an orthogonal operator on a finite-dimensional real Euclidean space V. Prove that $det(T) = \pm 1$.

14. Let T be a unitary operator on a finite-dimensional complex inner product space. Prove that $|det(T)| = 1$.

15. Let T be a skew-symmetric operator on a real inner product space of odd dimension. Prove that $det(T) = 0$.

16. Let A be a $(2k + 1) \times (2k + 1)$ matrix with columns $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{2k+1}$. Assume

$$\boldsymbol{v}_1 + \boldsymbol{v}_3 + \cdots + \boldsymbol{v}_{2k+1} = \boldsymbol{v}_2 + \cdots + \boldsymbol{v}_{2k}.$$

Prove that $det(A) = 0$.

17. Let A be an $n \times n$ rational matrix such that every entry is ± 1. Prove that $det(A)$ is an integer divisible by 2^{n-1}.

18. Let A be an invertible $n \times n$ matrix all of whose entries are either 0 or 1. Determine with a proof the minimum number of 0's in A.

19. In the determinant game, two players alternate placing a real number in an $n \times n$ matrix. Player 1 wins if the determinant of the final matrix is non-zero and player two wins if the determinant is zero. Show that if n is even, then player two has a winning strategy.

20. Assume A, B are $(2k + 1) \times (2k + 1)$ real matrices and $AB = -BA$. Prove that not both A and B are invertible.

7.3 Uniqueness of the Determinant of a Linear Operator

In this section we introduce the concepts of a multilinear map, multilinear form, as well as an alternating multilinear form. We then show how the determinant can be used to define an alternating n-linear form on an n-dimensional vector space and subsequently prove that this form is unique.

What You Need to Know

To make sense of the material in this section, you will need to have a mastery of the following concepts: linear operator on a vector space, and the determinant of a linear operator on finite-dimensional vector space.

Let V be an n-dimensional vector space with a basis $\mathcal{B} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$. Recall, there is a one-to-one correspondence between operators T on V and sequences $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n)$ of length n from V. Specifically, if $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n)$ is such a sequence then the corresponding operator is given by

$$T(c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n) = c_1\boldsymbol{u}_1 + \cdots + c_n\boldsymbol{u}_n.$$

Making use of this correspondence we may interpret the determinant as a function from V^n to $\mathbb{F}$. We use the results of Section (7.2) to record some properties of this function.

Theorem 7.9 *The function $det : V^n \to \mathbb{F}$ satisfies the following:*

*i) $det(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{j-1}, \boldsymbol{u}_j + \boldsymbol{u}_j', \boldsymbol{u}_{j+1}, \ldots, \boldsymbol{u}_n)$
$= det(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{j-1}, \boldsymbol{u}_j, \boldsymbol{u}_{j+1}, \ldots, \boldsymbol{u}_n) + det(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{j-1}, \boldsymbol{u}_j', \boldsymbol{u}_{j+1}, \ldots, \boldsymbol{u}_n)$.*

ii) $det(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{j-1}, c\boldsymbol{u}_j, \ldots, \boldsymbol{u}_n) = c\ det(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{j-1}, \boldsymbol{u}_j, \boldsymbol{u}_{j+1}, \ldots, \boldsymbol{u}_n)$.

iii) $det(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n) = 0$ if $\boldsymbol{u}_i = \boldsymbol{u}_j$ for some $i \neq j$.

iv) $det(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n) = 1$.

Proof *i) Let S be the operator associated with $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n)$ and S' the operator with $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{j-1}, \boldsymbol{u}_j', \boldsymbol{u}_{j+1}, \ldots, \boldsymbol{u}_n)$. We need to show that $det(S + S') = det(S) + det(S')$.*

Let A be the matrix of S with respect to $\mathcal{B}$ and A' the matrix of S' with respect to $\mathcal{B}$. Since $det(S) = det(A), det(S') = det(A')$ and $det(S+S') = det(A+A')$, we need to prove that $det(A + A') = det(A) + det(A')$.

Since also $det(A) = det(A^{tr}), det(A') = det((A')^{tr})$ and $det(A + A') = det((A+A')^{tr})$, it suffices to prove that $det((A+A')^{tr}) = det(A^{tr})+det((A')^{tr})$. However, this now follows from Lemma (7.7).

ii) The proof of this is similar to part i) making use of Lemma (7.6).

iii) This follows from Lemma (7.6).

iv) The operator that corresponds to $\mathcal{B}$ is the identity operator I_V and $det(I_V) = 1$.

The main purpose of the remainder of this section is to prove that the determinant is the only function from V^n to $\mathbb{F}$ which satisfies the conclusions of Theorem (7.9). Before we embark on that task, we first make a few definitions that will put the conclusions of the theorem into a broader perspective.

Definition 7.7 *Let $m \geq 2$, $V_1, \dots, V_m$ and W be vector spaces over a field $\mathbb{F}$. A function $f : V_1 \times \cdots \times V_m \to W$ is said to be an* **m-multilinear map** *if for each j and vectors $\boldsymbol{u}_1 \in V_1 \dots, \boldsymbol{u}_{j-1} \in V_{j-1}, \boldsymbol{u}_{j+1} \in V_{j+1}, \dots, \boldsymbol{u}_m \in V_m$, the map defined by $f(\boldsymbol{u}_1, \dots, \boldsymbol{u}_{j-1}, \boldsymbol{v}, \boldsymbol{u}_{j+1}, \dots, \boldsymbol{u}_m)$ is a linear transformation from V_j to W.*

If $W = \mathbb{F}$, the underlying field, then f is referred to as an **m-multilinear form***. If $m = 2$, we refer to f as a* **bilinear map***. Finally, if $m = 2$ and $W = \mathbb{F}$, then f is a* **bilinear form***.*

With the introduction of this terminology, we can say that when we interpret the determinant as a function from V^n to $\mathbb{F}$ that it is an n-multilinear form.

Definition 7.8 *Let V and W be vector spaces. An m-multilinear map from V^m to W is said to be* **alternating** *if $f(\boldsymbol{u}_1, \dots, \boldsymbol{u}_m) = 0$ whenever $\boldsymbol{u}_i = \boldsymbol{u}_{i+1}$ for some $i, 1 \leq i \leq m-1$. When $W = \mathbb{F}$, we say that f is an* **alternating form***.*

Remark 7.5 *As a consequence of Theorem (7.9), we can say that the determinant is an alternating n-multilinear form on the space V which takes the value 1 on the basis $\mathcal{B}$.*

Before reformulating our uniqueness statement, we prove some lemmas about alternating maps.

Lemma 7.10 *Assume $f : V^m \to W$ is an alternating m-multilinear map. Then*

$$f(\boldsymbol{u}_1, \dots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_i, \boldsymbol{u}_{i+1}, \dots, \boldsymbol{u}_m) = -f(\boldsymbol{u}_1, \dots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_{i+1}, \boldsymbol{u}_i, \dots, \boldsymbol{u}_m).$$

In words, the result of reversing two consecutive arguments is to multiply by -1.

Proof *By the definition of an alternating multilinear map, we have*

$$f(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_i + \boldsymbol{u}_{i+1}, \boldsymbol{u}_i + \boldsymbol{u}_{i+1}, \ldots, \boldsymbol{u}_m) = 0.$$

On the other hand, since f is m-multilinear, we have

$$f(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_i + \boldsymbol{u}_{i+1}, \boldsymbol{u}_i + \boldsymbol{u}_{i+1}, \ldots, \boldsymbol{u}_m)$$

$$= f(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_i, \boldsymbol{u}_i, \ldots, \boldsymbol{u}_m) + f(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_{i+1}, \boldsymbol{u}_{i+1}, \ldots, \boldsymbol{u}_m)$$

$$+ f(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_i, \boldsymbol{u}_{i+1}, \ldots, \boldsymbol{u}_m) + f(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_{i+1}, \boldsymbol{u}_i, \ldots, \boldsymbol{u}_m).$$

Since f is alternating,

$$f(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_i, \boldsymbol{u}_i, \ldots, \boldsymbol{u}_m) = f(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_{i+1}, \boldsymbol{u}_{i+1}, \ldots, \boldsymbol{u}_m) = 0.$$

Consequently, we have

$$f(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_i, \boldsymbol{u}_{i+1}, \ldots, \boldsymbol{u}_m) + f(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_{i+1}, \boldsymbol{u}_i, \ldots, \boldsymbol{u}_m) = 0$$

from which it follows that

$$f(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_i, \boldsymbol{u}_{i+1}, \ldots, \boldsymbol{u}_m) = -f(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_{i+1}, \boldsymbol{u}_i, \ldots, \boldsymbol{u}_m).$$

We can use Lemma (7.10) to prove that an alternating map takes the value zero whenever two arguments are equal:

Corollary 7.18 *Assume $f : V^m \to W$ is an alternating m-multilinear map. Then $f(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m) = 0$ whenever $\boldsymbol{u}_i = \boldsymbol{u}_j$ for some $i < j$.*

This is left as an exercise.

The proof of the following corollary is proved in exactly the same way as Lemma (7.10). It is left as an exercise.

Corollary 7.19 *Assume $f : V^m \to W$ is an alternating map. Then*

$$f(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m) = -f(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, \boldsymbol{v}_j, \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_{j-1}, \boldsymbol{v}_i, \boldsymbol{v}_{j+1}, \ldots, \boldsymbol{v}_m).$$

In words, if two arguments are exchanged, the result is to multiply the original image by -1.

Finally, we will require the following result, which tells us the value of an alternating map on a linearly dependent sequence:

Lemma 7.11 *Let $f : V^m \to W$ be an alternating m-multilinear map. Assume $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m)$ is linearly dependent. Then $f(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m) = \mathbf{0}_W$.*

Proof *If $\boldsymbol{u}_1 = \mathbf{0}_V$ then by multilinearity, $f(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m) = \mathbf{0}_W$, so we may assume $\boldsymbol{u}_1 \neq 0$. Since $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m)$ is linearly dependent, there is a $j > 1$ such that $\boldsymbol{u}_j$ is a linear combination of $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{j-1}$. So assume*

$$\boldsymbol{u}_j = \sum_{i=1}^{j-1} c_i \boldsymbol{u}_i.$$

By the multilinearity of f, we have

$$\begin{aligned} f(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_j, \ldots, \boldsymbol{u}_m) &= f(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{j-1}, \sum_{i=1}^{j-1} c_i \boldsymbol{u}_i, \boldsymbol{u}_{j+1}, \ldots, \boldsymbol{u}_m) \\ &= \sum_{i=1}^{j-1} c_i f(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{j-1}, \boldsymbol{u}_i, \boldsymbol{u}_{j+1}, \ldots, \boldsymbol{u}_m). \end{aligned}$$

However, each $f(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{j-1}, \boldsymbol{u}_i, \boldsymbol{u}_{j+1}, \ldots, \boldsymbol{u}_m) = \mathbf{0}_W$ since two of its arguments are identical ($i < j$). Thus, each term of the sum is $\mathbf{0}_W$ and hence the sum is $\mathbf{0}_W$.

Theorem 7.10 *Let V be an n-dimensional vector space over the field $\mathbb{F}$ and fix a basis $\mathcal{B} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$. Then there exists a unique alternating n-multilinear form Δ such that $\Delta(\mathcal{B}) = 1$.*

We will prove the theorem in a series of lemmas. The main strategy will be to use the correspondence between V^n and $\mathcal{L}(V, V)$, which allows us to interpret Δ as a function on $\mathcal{L}(V, V)$ and use the hypotheses to draw conclusions about this map. In particular, we will show that it is a multiplicative map, that is, $\Delta(ST) = \Delta(S)\Delta(T)$, and that it is zero on any non-invertible operator. Certain operators, elementary operators, play an important role in the proof, and so we begin by introducing these at this point.

Definition 7.9 *We denote the operator associated with the sequence $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, \boldsymbol{v}_j, \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_{j-1}, \boldsymbol{v}_i, \boldsymbol{v}_{j+1}, \ldots, \boldsymbol{v}_n)$, which exchanges $\boldsymbol{v}_i$ and $\boldsymbol{v}_j$ for $i < j$ by $\widehat{P}_{ij}$. We refer to this as an* **exchange operator**.

Definition 7.10 *We denote the operator associated with the sequence* $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_{j-1}, c\boldsymbol{v}_j, \boldsymbol{v}_{j+1}, \dots, \boldsymbol{v}_n,)$ *which fixes all* $\boldsymbol{v}_i, i \neq j$ *and multiplies* $\boldsymbol{v}_j$ *by the scalar* c *by* $\widehat{D}_j(c)$. *We refer to this as a* **scaling operator**.

Definition 7.11 *We denote the operator associated with the sequence* $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_{j-1}, c\boldsymbol{v}_i + \boldsymbol{v}_j, \boldsymbol{v}_{j+1}, \dots, \boldsymbol{v}_n)$, *which fixes each* $\boldsymbol{v}_k, k \neq j$ *and adds* $c\boldsymbol{v}_i$ *to* $\boldsymbol{v}_j$ *by* $\widehat{T}_{ij}(c)$ *and refer to this as an* **elimination operator**.

Remark 7.6 *The matrix of an elementary operator with respect to* $\mathcal{B}$ *is an elementary matrix of the corresponding type.*

Our first lemma is an immediate consequence of Lemma (7.11):

Lemma 7.12 *Let* T *be a non-invertible operator on* V. *Then* $\Delta(T) = 0$.

Proof *Set* $\boldsymbol{u}_j = T(\boldsymbol{v}_j)$. *Since* T *is non-invertible,* $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ *is linearly dependent. Then* $\Delta(T) = \Delta(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n) = 0$ *by Lemma (7.11).*

In our next lemma, we show that $\Delta(E) = det(E)$ when E is an elementary operator.

Lemma 7.13 *The following hold:*

i) $\Delta(\widehat{P}_{ij}) = -1 = det(\widehat{P}_{ij})$.

ii) $\Delta(\widehat{D}_j(c)) = c = det(\widehat{D}_j(c))$.

iii) $\Delta(\widehat{T}_{ij}(c)) = 1 = det(\widehat{T}_{ij}(c))$.

Proof *i) Set* $\boldsymbol{u}_k = \widehat{P}_{ij}(\boldsymbol{v}_k)$. *We then have*

$$(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n) = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_{i-1}, \boldsymbol{v}_j, \boldsymbol{v}_{i+1}, \dots, \boldsymbol{v}_{j-1}, \boldsymbol{v}_i, \boldsymbol{v}_{j+1}, \dots, \boldsymbol{v}_n).$$

By Corollary (7.19), $\Delta(\widehat{P}_{ij}) = -1$ *as asserted.*

ii) This follows from the multilinearity of Δ.

iii) Set $\boldsymbol{u}_k = \widehat{T}_{ij}(c)(\boldsymbol{v}_k)$. *We then have*

$$(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n) = \boldsymbol{v}_1, \dots, \boldsymbol{v}_{j-1}, c\boldsymbol{v}_i + \boldsymbol{v}_j, \boldsymbol{v}_{j+1}, \dots, \boldsymbol{v}_n).$$

Whence $\Delta(\widehat{T}_{ij}(c)) = \Delta(\boldsymbol{v}_1, \dots, \boldsymbol{v}_{j-1}, c\boldsymbol{v}_i + \boldsymbol{v}_j, \boldsymbol{v}_{j+1}, \dots, \boldsymbol{v}_n)$. *By the n-multilinearity of* Δ *we have*

$$\begin{aligned}&\Delta(\boldsymbol{v}_1, \dots, \boldsymbol{v}_{j-1}, c\boldsymbol{v}_i + \boldsymbol{v}_j, \boldsymbol{v}_{j+1}, \dots, \boldsymbol{v}_n)\\ &= c\Delta(\boldsymbol{v}_1, \dots, \boldsymbol{v}_{j-1}, \boldsymbol{v}_i, \boldsymbol{v}_{j+1}, \dots, \boldsymbol{v}_n) + \Delta(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n).\end{aligned}$$

Since two of the arguments in $\Delta(\boldsymbol{v}_1, \dots, \boldsymbol{v}_{j-1}, \boldsymbol{v}_i, \boldsymbol{v}_{j+1}, \dots, \boldsymbol{v}_n)$ *are equal, we can conclude that it is zero. It therefore follows that* $\Delta(\widehat{T}_{ij}(c)) = 1$ *as required.*

The next result is similar to Theorem (7.3) in both its content and proof.

Lemma 7.14 *Let T be an operator on V and E an elementary operator. Then* $\Delta(TE) = \Delta(T)\Delta(E)$.

Proof *We treat the three types of elementary operators separately. Set* $T(\boldsymbol{v}_k) = \boldsymbol{u}_k$. *Then* $\Delta(T) = \Delta(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$.

Assume $E = \widehat{P}_{ij}$ *and set* $\boldsymbol{w}_k = (T\widehat{P}_{ij})(\boldsymbol{v}_k)$. *Then* $(\boldsymbol{w}_1, \dots, \boldsymbol{w}_n) = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_j, \boldsymbol{u}_{i+1}, \dots, \boldsymbol{u}_{j-1}, \boldsymbol{u}_i, \boldsymbol{u}_{j+1}, \dots, \boldsymbol{u}_n)$. *Then*

$$\begin{aligned}\Delta(T\widehat{P}_{ij}) &= \Delta(\boldsymbol{w}_1, \dots, \boldsymbol{w}_n)\\ &= (\boldsymbol{u}_1, \dots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_j, \boldsymbol{u}_{i+1}, \dots, \boldsymbol{u}_{j-1}, \boldsymbol{u}_i, \boldsymbol{u}_{j+1}, \dots, \boldsymbol{u}_n)\\ &= -\Delta(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n) = \Delta(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)\Delta(\widehat{P}_{ij}).\end{aligned}$$

Now assume that $E = \widehat{D}_i(c)$ *and set* $\boldsymbol{w}_k = (T\widehat{D}_i(c))(\boldsymbol{v}_k)$. *Then* $(\boldsymbol{w}_1, \dots, \boldsymbol{w}_n) = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_{i-1}, c\boldsymbol{u}_i, \boldsymbol{u}_{i+1}, \dots, \boldsymbol{u}_n)$. *We then have*

$$\Delta(T\widehat{D}_i(c)) = \Delta(\boldsymbol{u}_1, \dots, \boldsymbol{u}_{i-1}, c\boldsymbol{u}_i, \boldsymbol{u}_{i+1}, \dots, \boldsymbol{u}_n).$$

By the n-multilinearity of Δ, *this is equal to*

$$c\Delta(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n) = \Delta(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)\Delta(\widehat{D}_i(c)) = \Delta(T)\Delta(\widehat{D}_i(c)).$$

Finally, assume that $E = \widehat{T}_{ij}(c)$ *and set* $\boldsymbol{w}_k = \widehat{T}_{ij}(c)(\boldsymbol{v}_k)$. *Then* $(\boldsymbol{w}_1, \dots, \boldsymbol{w}_n) = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_{j-1}, c\boldsymbol{u}_i + \boldsymbol{u}_j, \boldsymbol{u}_{j+1}, \dots, \boldsymbol{u}_n)$. *It then follows that* $\Delta(T\widehat{T}_{ij}(c)) = \Delta(\boldsymbol{u}_1, \dots, \boldsymbol{u}_{j-1}, c\boldsymbol{u}_i + \boldsymbol{u}_j, \boldsymbol{u}_{j+1}, \dots, \boldsymbol{u}_n)$. *In turn, this is equal to*

$$\Delta(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n) + c\Delta(\boldsymbol{u}_1, \dots, \boldsymbol{u}_{j-1}, \boldsymbol{u}_i, \boldsymbol{u}_{j+1}, \dots, \boldsymbol{u}_n) = \Delta(\boldsymbol{u}_1, \dots \boldsymbol{u}_n).$$

The latter holds since $\Delta(\boldsymbol{u}_1, \dots, \boldsymbol{u}_{j-1}, \boldsymbol{u}_i, \boldsymbol{u}_{j+1}, \dots, \boldsymbol{u}_n) = 0$ *because two of its arguments are equal. Thus,*

$$\Delta(T\widehat{T}_{ij}(c)) = \Delta(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n) = \Delta(T) = \Delta(T)\Delta(\widehat{T}_{ij}(c)).$$

As a corollary of Lemma (7.14), we have:

Corollary 7.20 *Assume an operator T is the product $E_1E_2\dots E_t$ of elementary operators. Then $\Delta(T) = \Delta(E_1)\Delta(E_2)\dots\Delta(E_t)$.*

Proof *Write $T = E_1E_2\dots E_t$. From Lemma (7.14), we can repeatedly write*

$$\Delta(E_1E_2) = \Delta(E_1)\Delta(E_2).$$

$$\Delta([E_1E_1]E_3) = \Delta(E_1E_2)\Delta(E_3) = \Delta(E_1)\Delta(E_2)\Delta(E_3.)$$

By continuing this way the result follows.

We can now prove that $\Delta(T) = det(T)$ for an operator T on V. If T is non-vertible, then we have seen that $\Delta(T) = 0 = det(T)$. So assume T is invertible. Then T is a product of elementary operators (exercise). So write $T = E_1E_2\dots E_t$ where the E_i are elementary operators. From Lemma (7.20), we have $\Delta(T) = \Delta(E_1)\dots\Delta(E_t)$. By Lemma (7.13), we have $\Delta(E_1)\dots\Delta(E_t) = det(E_1)\dots det(E_t)$. Finally, by the multiplicative property of the determinant, we have $det(E_1)\dots det(E_t) = det(E_1\dots E_t) = det(T)$.

Exercises

1. Prove Corollary (7.18).

2. Prove that every invertible operator is a product of elementary operators.

3. Let V and W be vector spaces over the field $\mathbb{F}$ and m a natural number. Denote by $\mathcal{L}(V^m, W)$ the collection of all m-multilinear maps from V to W. This is clearly a subset of the vector space $\mathcal{M}(V^m, W)$ of all maps from V^m to W. Prove that it is a subspace.

4. Let V and W be vector spaces over the field $\mathbb{F}$ and m a natural number. Let $Alt(V^m, W)$ be the collection of all alternating m-multilinear maps from V to W. Prove that this is a subspace of $\mathcal{L}(V^m, W)$.

5. Assume V is an n-dimensional vector space over $\mathbb{F}$, W is a vector space over $\mathbb{F}$, and $m > n$. Prove that $Alt(V^m, W)$ consists of only the zero map.

6. Let $\mathbb{F}$ be a field and set $V = \mathbb{F}^4$. For $1 \le i < j \le 4$, define the map f_{ij} from V^2 to $\mathbb{F}$ as follows:

$$f_{ij}\left(\begin{pmatrix} a_{11} \\ a_{21} \\ a_{31} \\ a_{41} \end{pmatrix}, \begin{pmatrix} a_{12} \\ a_{22} \\ a_{32} \\ a_{42} \end{pmatrix}\right) = det\left(\begin{pmatrix} a_{i1} & a_{i2} \\ a_{j1} & a_{j2} \end{pmatrix}\right) = a_{i1}a_{j2} - a_{j1}a_{i2}.$$

Prove that each f_{ij} is an alternating bilinear map.

7. Prove that the sequence of maps $(f_{11}, f_{12}, f_{13}, f_{23}, f_{24}, f_{34})$ is a basis for $Alt(V^2, \mathbb{F})$.

8. Let A be a 4×3 matrix. For a natural number $i, 1 \leq i \leq 4$, let A_i be the 3×3 matrix obtained by deleting the i^{th} row of A. If $\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3 \in \mathbb{F}^4$, identify the sequence $(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3)$ with the matrix whose columns are these vectors. Define a map $g_i : V^3 \to \mathbb{F}$ by $g_i(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3) = det((\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3)_i)$.

Prove that g_i is an alternating 3-linear form.

9. Prove that (g_1, g_2, g_3, g_4) is a basis for $Alt(V^3, \mathbb{F})$.

This page intentionally left blank

8

Bilinear Forms

CONTENTS

This chapter is devoted to bilinear forms. We previously defined the concept of an m-multilinear map from vector spaces $V_1, \dots, V_m$ to the vector space W. A particularly important special case is when $m = 2$. Such functions were referred to as bilinear maps. Bilinear maps are important because of their role in the definition of the tensor product of two spaces, which is the subject of chapter ten. Bilinear forms (bilinear maps to $\mathbb{F}$, the underlying field) arise throughout mathematics, in fields ranging from differential geometry and mathematical physics on the one hand, to group theory and number theory on the other. In the introductory section of this chapter we develop some basic properties of bilinear maps and forms, introduce the notion of a reflexive form, and prove that any reflexive form is either alternating or symmetric. The second section is devoted to the structure of symplectic space, a vector space equipped with an alternating form. In the third section, we define the notion of a quadratic form and develop the general theory of an orthogonal space. In particular, we prove Witt's theorem for an orthogonal space when the characteristic of the field is not two. The fourth section deals with orthogonal space over a perfect field of characteristic two. Finally, section five is concerned with real orthogonal spaces.

8.1 Basic Properties of Bilinear Maps

In this section we develop some basic properties of bilinear maps and forms, introduce the notion of a reflexive form, and prove that any reflexive form is either alternating or symmetric.

What You Need to Know

To be successful in understanding the new material of this section, it is essential that you have already mastered the following concepts: vector space, basis of a vector space, dimension of a vector space, finite-dimensional vector space, linear transformation, coordinate vector with respect to a basis, matrix of a linear transformation, an algebra, determinant of a matrix or operator, multilinear map, multilinear form, bilinear map, and bilinear form.

We begin by recalling the definition of a bilinear map:

Definition (7.7)

Assume V, W, X are vector spaces over a field $\mathbb{F}$. A function $f : V \times W \to X$ is a **bilinear map** *if the following hold:*

1) For $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V, c_1, c_2 \in \mathbb{F}$ and $\boldsymbol{w}$ in W we have $f(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2, \boldsymbol{w}) = c_1 f(\boldsymbol{v}_1, \boldsymbol{w}) + c_2 f(\boldsymbol{v}_2, \boldsymbol{w})$.

2) For $\boldsymbol{v} \in V, \boldsymbol{w}_1, \boldsymbol{w}_2 \in W, c_1, c_2 \in \mathbb{F}$ we have $f(\boldsymbol{v}, c_1\boldsymbol{w}_1+c_2\boldsymbol{w}_2) = c_1 f(\boldsymbol{v}, \boldsymbol{w}_1)+ c_2 f(\boldsymbol{v}, \boldsymbol{w}_2)$.

In other words, when one of the arguments is fixed, the resulting function is a linear transformation.

When $X = \mathbb{F}$ a bilinear map is referred to as a **bilinear form***.*

We will denote by $B(V, W; X)$ the collection of all bilinear maps from $V \times W$ to X. When $V = W$ we will write $B(V^2; X)$.

Example 8.1 *Assume A is an algebra over the field $\mathbb{F}$ (for example, $\mathcal{L}(V, V)$ or $\mathbb{F}[x]$). Then the multiplication of A is a bilinear map from $A \times A$ to A.*

Example 8.2 *If $(V, \langle\ ,\ \rangle)$ is a real inner product space, then $\langle\ ,\ \rangle$ is a bilinear form on V.*

Example 8.3 *For $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in M_{22}(\mathbb{F})$ set*

$$f(A, B) = det(A + B) - det(A) - det(B) = a_{11}b_{22} + a_{22}b_{11} - a_{12}b_{21} - a_{21}b_{12}.$$

Then f defines a bilinear form on $M_{22}(\mathbb{F})$.

Example 8.4 *Assume X is an n-dimensional space and $\mathcal{B}_X = (\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n)$ is a basis for X. Assume $f_1, \ldots, f_s$ are bilinear forms on $V \times W$. Define $F : V \times W \to X$ by $F(\boldsymbol{v}, \boldsymbol{w}) = \sum_{i=1}^{n} f_i(\boldsymbol{v}, \boldsymbol{w})\boldsymbol{x}_i$. Then F is bilinear map.*

Example 8.5 *Let $V = \mathbb{F}^m, W = \mathbb{F}^n$, and $A \in M_{mn}(\mathbb{F})$. For $\boldsymbol{v} \in V, \boldsymbol{w} \in W$ set $f(\boldsymbol{v}, \boldsymbol{w}) = \boldsymbol{v}^{tr} A\boldsymbol{w}$. Then f is a bilinear form.*

Theorem 8.1 *Let V, W, X be vector spaces over the field $\mathbb{F}$. Then $B(V, W; X)$ is a vector space over $\mathbb{F}$.*

Proof *Since $B(V, W; X)$ is a subset of $\mathcal{M}(V \times W, X)$ we need to prove i) if $f, g \in B(V, W; X)$, then $f + g \in B(V, W; X)$; and ii) if $f \in B(V, W; X)$ and $c \in \mathbb{F}$, then $cf \in B(V, W; X)$.*

i) Let $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V, \boldsymbol{w} \in W$, and $c_1, c_2 \in \mathbb{F}$. Then, by the definition of the sum $f + g$,

$$(f + g)(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2, \boldsymbol{w}) = f(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2, \boldsymbol{w}) + g(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2, \boldsymbol{w}).$$

Since both f, g are bilinear, we have

$$f(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2, \boldsymbol{w}) + g(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2, \boldsymbol{w})$$

$$= [c_1 f(\boldsymbol{v}_1, \boldsymbol{w}) + c_2 f(\boldsymbol{v}_2, \boldsymbol{w})] + [c_1 g(\boldsymbol{v}_1, \boldsymbol{w}) + c_2 g(\boldsymbol{v}_2, \boldsymbol{w})]. \tag{8.1}$$

After rearranging and regrouping terms in (8.1) we get

$$c_1[f(\boldsymbol{v}_1, \boldsymbol{w}) + g(\boldsymbol{v}_1, \boldsymbol{w})] + c_2[f(\boldsymbol{v}_2, \boldsymbol{w}) + g(\boldsymbol{v}_2, \boldsymbol{w})]$$

$$= c_1(f + g)(\boldsymbol{v}_1, \boldsymbol{w}) + c_2(f + g)(\boldsymbol{v}_2, \boldsymbol{w}).$$

This shows that $f + g$ is linear in the first argument. In exactly the same way, we can show that $f + g$ is linear in the second argument.

ii) Let $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V, \boldsymbol{w} \in W$ and $c_1, c_2 \in \mathbb{F}$. Then, by the definition of cf, we have ,

$$(cf)(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2, \boldsymbol{w}) = c[f(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2, \boldsymbol{w})].$$

Since f is bilinear, this is equal to

$$c[c_1 f(\boldsymbol{v}_1, \boldsymbol{w}) + c_2 f(\boldsymbol{v}_2, \boldsymbol{w})]$$

$$= (cc_1)f(\boldsymbol{v}_1, \boldsymbol{w}) + (cc_2)f(\boldsymbol{v}_2, \boldsymbol{w}) = c_1(cf)(\boldsymbol{v}_1, \boldsymbol{w}) + c_2(cf)(\boldsymbol{v}_2, \boldsymbol{w}).$$

which is what we needed to show. In exactly the same way, we can show that cf is linear in the second argument.

The following lemma is useful toward characterizing the space of bilinear maps from a pair of spaces V and W to a space X.

Lemma 8.1 *Let f be a bilinear map from $V \times W$ to a space X and ϕ be a linear transformation from X to $\mathbb{F}$. Then $\phi \circ f$ is a bilinear form.*

Proof *Assume $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V, c_1, c_2 \in \mathbb{F}$ and $\boldsymbol{w} \in W$. Then*

$$(\phi \circ f)(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2, \boldsymbol{w}) = \phi(f(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2, \boldsymbol{w})) = \phi(c_1 f(\boldsymbol{v}_1, \boldsymbol{w}) + c_2 f(\boldsymbol{v}_2, \boldsymbol{w}))$$

since f is bilinear. Since ϕ is linear

$$\phi(c_1 f(\boldsymbol{v}_1, \boldsymbol{w}) + c_2 f(\boldsymbol{v}_2, \boldsymbol{w})) = c_1\phi(f(\boldsymbol{v}_1, \boldsymbol{w})) + c_2\phi(f(\boldsymbol{v}_2, \boldsymbol{w}))$$

$$= c_1(\phi \circ f)(\boldsymbol{v}_1, \boldsymbol{w}) + c_2(\phi \circ f)(\boldsymbol{v}_2, \boldsymbol{w}).$$

In exactly the same way, it follows for $\boldsymbol{v} \in V, \boldsymbol{w}_1, \boldsymbol{w}_2 \in W$ and $c_1, c_2 \in \mathbb{F}$ that

$$(\phi \circ f)(\boldsymbol{v}, c_1\boldsymbol{w}_1 + c_2\boldsymbol{w}_2) = c_1(\phi \circ f)(\boldsymbol{v}, \boldsymbol{w}_1) + c_2(\phi \circ f)(\boldsymbol{v}, \boldsymbol{w}_2).$$

Making use of Lemma (8.1) we now show that when X is a finite-dimensional vector space then every bilinear map from $V \times W$ to X can be constructed as in Example (**??**).

Theorem 8.2 *Assume that X is a finite-dimensional vector space with basis $\mathcal{B}_X = (\boldsymbol{x}_1, \dots, \boldsymbol{x}_q)$ and assume f is a map from $V \times W$ to X. For $\boldsymbol{v} \in V, \boldsymbol{w} \in W$ let $f(\boldsymbol{v}, \boldsymbol{w}) = \sum_{i=1}^{q} f_i(\boldsymbol{v}, \boldsymbol{w})\boldsymbol{x}_i$. Then f is a bilinear map if and only if each f_i is a bilinear form.*

Proof *If each f_i is bilinear, it follows from Example (8.4) that the map f is bilinear. Set $X_i = Span(\boldsymbol{x}_i), 1 \leq i \leq q$ and $Y_i = \sum_{j \neq i} X_i$ so that $V = X_i \oplus Y_i$. Let $\pi_i = Proj_{(X_I, Y_i)}$. Then $f_i = \pi_i \circ f$, and then by Lemma (8.1) each f_i is a bilinear form.*

In our next result, we prove if V and W are finite-dimensional, then every bilinear form arises as in Example (8.5).

Theorem 8.3 *Let V be an m-dimensional vector space with basis $\mathcal{B}_V = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_m)$ and W an n-dimensional vector space with basis $\mathcal{B}_W = (\boldsymbol{w}_1, \dots, \boldsymbol{w}_n)$. Assume $f : V \times W \to \mathbb{F}$ is bilinear. Set $a_{ij} = f(\boldsymbol{v}_i, \boldsymbol{w}_j)$ for $1 \leq i \leq m, 1 \leq j \leq n$, and $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$. If $\boldsymbol{v} = \sum_{i=1}^m c_i \boldsymbol{v}_i$ and $\boldsymbol{w} = \sum_{j=1}^n d_j \boldsymbol{w}_j$, then*

$$f(\boldsymbol{v}, \boldsymbol{w}) = \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix}^{tr} A \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix}.$$

This is left as an exercise.

Corollary 8.1 *Assume that V, W, and X are finite-dimensional vector spaces over the field $\mathbb{F}$. Then $dim(B(V, W; X)) = (dim(V))(dim(W))(dim(X))$.*

This is left as an exercise.

Definition 8.1 *Let V be a vector space with basis $\mathcal{B}_V = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_m)$, W a vector space with basis $\mathcal{B}_W = (\boldsymbol{w}_1, \dots, \boldsymbol{w}_n)$, and $f \in B(V, W; \mathbb{F})$, a bilinear form. The* **matrix** *of f with respect to $(\mathcal{B}_V, \mathcal{B}_W)$ is the $m \times n$ matrix whose (i, j)-entry is $f(\boldsymbol{v}_i, \boldsymbol{w}_j)$. This matrix is denoted by $\mathcal{M}_f(\mathcal{B}_V, \mathcal{B}_W)$. When $V = W$, it is customary to take $\mathcal{B}_W = \mathcal{B}_V = \mathcal{B}$, and then $\mathcal{M}_f(\mathcal{B}, \mathcal{B})$ is the* **matrix** *of f with respect to $\mathcal{B}$.*

It is instructive to look at what the effect of changing bases has on the matrix of a form. The next lemma does so.

Lemma 8.2 *Let V be an m-dimensional vector space over the field $\mathbb{F}$ with bases $\mathcal{B}_V = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_m)$ and $\mathcal{B}'_V = (\boldsymbol{v}'_1, \dots, \boldsymbol{v}'_m)$. Let W be an n-dimensional vector space over $\mathbb{F}$ with bases $\mathcal{B}_W = (\boldsymbol{w}_1, \dots, \boldsymbol{w}_n)$ and $\mathcal{B}'_W = (\boldsymbol{w}'_1, \dots, \boldsymbol{w}'_n)$. Assume $f \in B(V, W; \mathbb{F})$. Set $A = \mathcal{M}_f(\mathcal{B}_V, \mathcal{B}_W)$, $A' = \mathcal{M}_f(\mathcal{B}'_V, \mathcal{B}'_W), P = \mathcal{M}_{I_V}(\mathcal{B}'_V, \mathcal{B}_V)$, and $Q = \mathcal{M}_{I_W}(\mathcal{B}'_W, \mathcal{B}_W)$. Then*

$$A' = P^{tr} A Q.$$

Proof *Let $1 \leq i \leq m, 1 \leq j \leq n$. Denote the (i, j)-entry of A by a_{ij} and that* *of A' by a'_{ij}. We need to compute $a'_{ij} = f(\boldsymbol{v}'_i, \boldsymbol{w}'_j)$. Suppose $[\boldsymbol{v}'_i]_{\mathcal{B}_V} = \begin{pmatrix} p_{1i} \\ p_{2i} \\ \vdots \\ p_{ni} \end{pmatrix}$ and $[\boldsymbol{w}'_j]_{\mathcal{B}_W} = \begin{pmatrix} q_{1j} \\ q_{2j} \\ \vdots \\ q_{mj} \end{pmatrix}$. Then*

$$\begin{aligned} f(\boldsymbol{v}'_i, \boldsymbol{w}'_j) &= f(\sum_{k=1}^{n} p_{ki}\boldsymbol{v}_k, \sum_{l=1}^{m} q_{lj}\boldsymbol{w}_l) \\ &= \sum_{k=1}^{n}\sum_{l=1}^{m} p_{ki}a_{kl}q_{lj}. \qquad (8.2) \end{aligned}$$

The expression in (8.2) is just the (i,j)-entry of the matrix $P^{tr}AQ$.

Lemma (8.2) motivates the following definitions:

Definition 8.2 *Two $m \times n$ matrices A and A' are said to be* **equivalent** *if there is an invertible $m \times m$ matrix R and an invertible $n \times n$ matrix Q such that $A' = RAQ$.*

Two $n \times n$ matrices A and A' are **congruent** *if there is an invertible $n \times n$ matrix P such that $A' = P^{tr}AP$.*

It is a consequence of Lemma (8.2) that two $m \times n$ matrices A and A' are matrices of the same form (with respect to different pairs of bases) if and only if the matrices are equivalent. It is also a consequence of the lemma that two $n \times n$ matrices are matrices of the same bilinear form defined on an n-dimensional vector space V if and only if the matrices are congruent.

Remark 8.1 *Assume f, g are bilinear forms on $V \times W$. It is then the case that $\mathcal{M}_{f+g}(\mathcal{B}_V, \mathcal{B}_W) = \mathcal{M}_f(\mathcal{B}_V, \mathcal{B}_W) + \mathcal{M}_g(\mathcal{B}_V, \mathcal{B}_W)$ and for a scalar c that $\mathcal{M}_{cf}(\mathcal{B}_V, \mathcal{B}_W) = c\mathcal{M}_f(\mathcal{B}_V, \mathcal{B}_W)$.*

It is a consequence of Remark (8.1) that $B(V, W; \mathbb{F})$ and $M_{mn}(\mathbb{F})$ are isomorphic as vector spaces. The next theorem allows us to see this in a more elegant and abstract way.

Theorem 8.4 *Let V and W be vector spaces. Let W' denote the dual space of $W, \mathcal{L}(W, \mathbb{F})$. Then $B(V, W; \mathbb{F})$ is isomorphic as a vector space to $\mathcal{L}(V, W')$.*

Proof *Assume $f \in B(V, W; \mathbb{F})$. For $\boldsymbol{v} \in V$, denote by $f_{\boldsymbol{v}}$ the function from W to $\mathbb{F}$ given by $f_{\boldsymbol{v}}(\boldsymbol{w}) = f(\boldsymbol{v}, \boldsymbol{w})$. By the definition of bilinear form, $f_{\boldsymbol{v}} \in W'$. Now define $\epsilon : B(V, W; \mathbb{F}) \to W'$ by $\epsilon(f)(\boldsymbol{v}) = f_{\boldsymbol{v}}$. Since f is linear in its first argument ϵ is a linear map.*

On the other hand, suppose $F \in \mathcal{L}(V, W')$. Let $\widehat{F}$ be the map from $V \times W$ to $\mathbb{F}$ given by $\widehat{F}(\boldsymbol{v}, \boldsymbol{w}) = (F(\boldsymbol{v}))(\boldsymbol{w})$. Then $\widehat{F} \in B(V, W; \mathbb{F})$. Denote by δ the map from $\mathcal{L}(V, W')$ such that $\delta(F) = \widehat{F}$. Then δ is a linear map. The maps δ and ϵ are inverses of each other.

Suppose now that V is an m-dimensional vector space with basis $\mathcal{B}_V, W$ is an n-dimensional vector space with basis $\mathcal{B}_W, f \in B(V, W; \mathbb{F})$, and A is the matrix of f with respect to $(\mathcal{B}_V, \mathcal{B}_W)$. Suppose $\boldsymbol{v} \in V$ and $[\boldsymbol{v}]_{\mathcal{B}_V}$ is in the null space of A^{tr}. Then for all $\boldsymbol{w} \in W, f(\boldsymbol{v}, \boldsymbol{w}) = 0$. Similarly, if $\boldsymbol{w} \in W$ and $[\boldsymbol{w}]_{\mathcal{B}_W} \in null(A)$ then $f(\boldsymbol{v}, \boldsymbol{w}) = 0$ for all $\boldsymbol{v} \in V$. This motivates the following definitions:

Definition 8.3 *Let V, W be vector spaces and $f \in B(V, W; \mathbb{F})$. The* **left radical** *of f consists of those $\boldsymbol{v} \in V$ such that $f(\boldsymbol{v}, \boldsymbol{w}) = 0$ for all $\boldsymbol{w} \in W$. This is denoted by $Rad_L(f)$.*

The **right radical** *of f consists of those $\boldsymbol{w} \in W$ such that $f(\boldsymbol{v}, \boldsymbol{w}) = 0$ for all $\boldsymbol{v} \in W$. This is denoted by $Rad_R(f)$.*

Theorem 8.5 *Let V, W be vector spaces and $f \in B(V, W; \mathbb{F})$. Then $Rad_L(f)$ is a subspace of V and $Rad_R(f)$ is a subspace of W.*

Proof *Assume $\boldsymbol{v}_1, \boldsymbol{v}_2 \in Rad_L(f)$ and $\boldsymbol{w} \in W$. Then $f(\boldsymbol{v}_1 + \boldsymbol{v}_2, \boldsymbol{w}) = f(\boldsymbol{v}_1, \boldsymbol{w}) + f(\boldsymbol{v}_2, \boldsymbol{w}) = 0 + 0 = 0$ since $\boldsymbol{v}_1, \boldsymbol{v}_2 \in Rad_L(f)$. Therefore, $\boldsymbol{v}_1 + \boldsymbol{v}_2 \in Rad_L(f)$.*

Assume $\boldsymbol{v} \in Rad_L(f), c \in \mathbb{F}$ is a scalar, and $\boldsymbol{w} \in W$. Then $f(c\boldsymbol{v}, \boldsymbol{w}) = cf(\boldsymbol{v}, \boldsymbol{w}) = c \cdot 0 = 0$. Thus, $c\boldsymbol{v} \in Rad_L(f)$. This proves that $Rad_L(f)$ is a subspace of V. That $Rad_R(f)$ is a subspace of W is proved in exactly the same way.

Let V and W be finite-dimensional vector spaces, and f a bilinear form on $V \times W$. It is not difficult to see that if $Rad_L(f) = \{\boldsymbol{0}_V\}$ and $Rad_R(f) = \{\boldsymbol{0}_W\}$, then it must be the case that $dim(V) = dim(W)$. We leave this as an exercise. Of course, this is possible if $V = W$. This situation motivates the following definition:

Definition 8.4 *A bilinear form on a finite-dimensional vector space V is* **non-degenerate** *if $Rad_L(f) = Rad_R(f) = \{\boldsymbol{0}\}$.*

Lemma 8.3 *Assume V is a finite-dimensional vector space and f is a non-degenerate bilinear form on V. For $\boldsymbol{v} \in V$, denote by $f_L(\boldsymbol{v})$ the function from V to $\mathbb{F}$ given by $f_L(\boldsymbol{v})(\boldsymbol{w}) = f(\boldsymbol{v}, \boldsymbol{w})$ and by $f_R(\boldsymbol{v})$ the function given by $f_R(\boldsymbol{v})(\boldsymbol{w}) = f(\boldsymbol{w}, \boldsymbol{v})$. Then both $f_L$and f_R are isomorphisms of V with $V' = \mathcal{L}(V, \mathbb{F})$.*

Proof *Because f is linear in its first argument, the map f_L is a transformation from V to V'. Since $dim(V) = dim(V')$, to prove this is an isomorphism it suffices to prove that $Ker(f_L) = \{\mathbf{0}\}$ by Theorem (2.12). However, if $\boldsymbol{v} \in Ker(f_L)$, then $\boldsymbol{v} \in Rad_L(f) = \{\mathbf{0}\}$. That f_R is also an isomorphism is proved in exactly the same way.*

The next result gives a practical way of computing the left and right radicals of a bilinear form f on V.

Lemma 8.4 *Let V be a vector space with basis $\mathcal{B} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ and f a bilinear form. Then $Rad_L(f) = \cap_{i=1}^n Ker(f_R(\boldsymbol{v}_i))$ and $Rad_R(f) = \cap_{i=1}^n Ker(f_L(\boldsymbol{v}_i))$.*

Proof *Assume $\boldsymbol{u} \in Rad_L(f)$. Then $f(\boldsymbol{u}, \boldsymbol{v}) = 0$ for all $\boldsymbol{v} \in V$. In particular, $f(\boldsymbol{u}, \boldsymbol{v}_i) = 0$ for all $i, 1 \leq i \leq n$ and $\boldsymbol{u} \in Ker(f_R(\boldsymbol{v}_i))$ for all i. This proves that $Rad_L(f) \subset \cap_{i=1}^n Ker(f_R(\boldsymbol{v}_i))$.*

On the other hand, suppose $\boldsymbol{u} \in \cap_{i=1}^n Ker(f_R(\boldsymbol{v}_i))$ and $\boldsymbol{v} \in V$. We need to prove that $f(\boldsymbol{u}, \boldsymbol{v}) = 0$. Write $\boldsymbol{v} = c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n$. Then $f(\boldsymbol{u}, \boldsymbol{w}) = f(\boldsymbol{u}, c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n) = c_1 f(\boldsymbol{u}, \boldsymbol{v}_1) + \cdots + c_n f(\boldsymbol{u}, \boldsymbol{v}_n) = 0$. Thus, $\boldsymbol{u} \in Rad_L(f)$ and $\cap_{i=1}^n Ker(f_R(f(\boldsymbol{v}_i) \subset Rad_L(f)$. Consequently, we have equality. The second statement is proved in exactly the same way.

Imitating our treatment of inner products we make the following definition:

Definition 8.5 *Let f be a bilinear form on a vector space V. We will say that vectors $\boldsymbol{u}, \boldsymbol{v}$ are* **orthogonal with respect to** *f if $f(\boldsymbol{u}, \boldsymbol{v}) = 0$ and write $\boldsymbol{u} \perp_f \boldsymbol{v}$.*

Remark 8.2 *When f is an inner product the relation of orthogonality is symmetric, but this is not necessarily the case for an arbitrary bilinear form. However, it is precisely those bilinear forms for which orthogonality is a symmetric relation which will be the object of our interest in the remainder of this section.*

Definition 8.6 *Let f be a bilinear form on a vector space V. We say that f is* **reflexive** *provided that the relation $\perp_f$ is a symmetric relation, that is, for two vectors $\boldsymbol{u}$ and $\boldsymbol{v}$, $f(\boldsymbol{u},\boldsymbol{v}) = 0$ if and only if $f(\boldsymbol{v},\boldsymbol{u}) = 0$.*

The following is a consequence of the definition of a reflexive form:

Lemma 8.5 *Let f be a reflexive form on the space V. Then $Rad_L(f) = Rad_R(f)$.*

Proof *Suppose $\boldsymbol{u} \in Rad_L(f)$ and $\boldsymbol{v} \in V$. Then $f(\boldsymbol{v},\boldsymbol{u}) = f(\boldsymbol{u},\boldsymbol{v}) = 0$ and hence $\boldsymbol{u} \in Rad_R(f)$. This proves $Rad_L(f) \subset Rad_R(f)$. In exactly the same way we can prove the reverse inclusion and therefore we have equality.*

When f is reflexive, we will write *Rad*(f) for $Rad_L(f) = Rad_R(f)$.

The next two definitions introduce two types of reflexive forms.

Definition 8.7 *A bilinear form $f : V^2 \to \mathbb{F}$ is said to be* **alternating** *if $f(\boldsymbol{v},\boldsymbol{v}) = 0$ for all $\boldsymbol{v} \in V$.*

The following is not difficult to prove, and we leave it as an exercise:

Lemma 8.6 *Assume $f : V^2 \to \mathbb{F}$ is an alternating bilinear form. Then $f(\boldsymbol{w},\boldsymbol{v}) = -f(\boldsymbol{v},\boldsymbol{w})$ for all $\boldsymbol{v},\boldsymbol{w} \in V$.*

Remark 8.3 *If the field $\mathbb{F}$ does not have characteristic two, then the assumption that $f(\boldsymbol{w},\boldsymbol{v}) = -f(\boldsymbol{v},\boldsymbol{w})$ (along with bilinearity) implies that $f$is alternating. However, this is not true when $1 + 1 = 0$.*

The following lemma describes the matrix of an alternating form.

Lemma 8.7 *Let V be a finite-dimensional vector space with basis $\mathcal{B} = (\boldsymbol{v}_1,\ldots,\boldsymbol{v}_n)$ and $f : V^2 \to \mathbb{F}$ an alternating form. Then the matrix $\mathcal{M}_f(\mathcal{B},\mathcal{B})$ is skew symmetric, $\mathcal{M}_f(\mathcal{B},\mathcal{B})^{tr} = -\mathcal{M}_f(\mathcal{B},\mathcal{B})$, and has zeros on the diagonal.*

Proof *Let $a_{ij} = f(\boldsymbol{v}_i,\boldsymbol{v}_j)$. By Lemma (8.6) $a_{ji} = f(\boldsymbol{v}_j,\boldsymbol{v}_i) = -f(\boldsymbol{v}_i,\boldsymbol{v}_j) = -a_{ij}$.*

The diagonal entry $a_{ii} = f(\boldsymbol{v}_i,\boldsymbol{v}_i) = 0$.

We now come to a second type of reflexive form.

Definition 8.8 *A bilinear form $f : V^2 \to \mathbb{F}$ is said to be* **symmetric** *if $f(\boldsymbol{v}, \boldsymbol{w}) = f(\boldsymbol{w}, \boldsymbol{v})$ for all $\boldsymbol{v}, \boldsymbol{w} \in V$.*

The following lemma describes the matrix of a symmetric form. Its proof is similar to that of Lemma (8.7).

Lemma 8.8 *Let V be a finite-dimensional vector space with basis $\mathcal{B} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ and $f : V^2 \to \mathbb{F}$ a symmetric form. Then the matrix $\mathcal{M}_f(\mathcal{B}, \mathcal{B})$ is symmetric, $\mathcal{M}_f(\mathcal{B}, \mathcal{B})^{tr} = \mathcal{M}_f(\mathcal{B}, \mathcal{B})$. Conversely, if $\mathcal{M}_f(\mathcal{B}, \mathcal{B})$ is symmetric then the form f is symmetric.*

Clearly, symmetric and alternating forms are reflexive. In the next theorem we prove the converse.

Theorem 8.6 *Assume $f : V^2 \to \mathbb{F}$ is a reflexive bilinear form. Then f is either alternating or symmetric.*

Proof *Let $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in V$ and consider $f(\boldsymbol{x}, f(\boldsymbol{x}, \boldsymbol{y})\boldsymbol{z} - f(\boldsymbol{x}, \boldsymbol{z})\boldsymbol{y})$. Using bilinearity we get*

$$\begin{aligned} f(\boldsymbol{x}, f(\boldsymbol{x}, \boldsymbol{y})\boldsymbol{z} - f(\boldsymbol{x}, \boldsymbol{z})\boldsymbol{y}) &= f(\boldsymbol{x}, f(\boldsymbol{x}, \boldsymbol{y})\boldsymbol{z}) - f(\boldsymbol{x}, f(\boldsymbol{x}, \boldsymbol{z})\boldsymbol{y}) \\ &= f(\boldsymbol{x}, \boldsymbol{y})f(\boldsymbol{x}, \boldsymbol{z}) - f(\boldsymbol{x}, \boldsymbol{z})f(\boldsymbol{x}, \boldsymbol{y}) \\ &= 0. \end{aligned}$$

Since f is reflexive, we get $f(f(\boldsymbol{x}, \boldsymbol{y})\boldsymbol{z} - f(\boldsymbol{x}, \boldsymbol{z})\boldsymbol{y}, \boldsymbol{x}) = 0$.

Using bilinearity we get

$$f(\boldsymbol{x}, \boldsymbol{y})f(\boldsymbol{z}, \boldsymbol{x}) - f(\boldsymbol{x}, \boldsymbol{z})f(\boldsymbol{y}, \boldsymbol{x}) = 0. \tag{8.3}$$

Setting $\boldsymbol{z} = \boldsymbol{x}$ we obtain the relation

$$[f(\boldsymbol{x}, \boldsymbol{y}) - f(\boldsymbol{y}, \boldsymbol{x})]f(\boldsymbol{x}, \boldsymbol{x}) = 0. \tag{8.4}$$

Assume now that f is not symmetric. We will show that it is alternating. Thus, suppose that $f(\boldsymbol{u}, \boldsymbol{v}) \neq f(\boldsymbol{v}, \boldsymbol{u})$ for some pair $\boldsymbol{u}$ and $\boldsymbol{v}$. Now in Equation (8.4) set $\boldsymbol{x} = \boldsymbol{u}$ and $\boldsymbol{y} = \boldsymbol{v}$ to get that $f(\boldsymbol{u}, \boldsymbol{u}) = 0$. On the other hand, setting $\boldsymbol{x} = \boldsymbol{v}$ and $\boldsymbol{y} = \boldsymbol{u}$ we get $f(\boldsymbol{v}, \boldsymbol{v}) = 0$. We have thus shown that if $f(\boldsymbol{u}, \boldsymbol{v}) \neq f(\boldsymbol{v}, \boldsymbol{u})$ then $f(\boldsymbol{u}, \boldsymbol{u}) = f(\boldsymbol{v}, \boldsymbol{v}) = 0$.

Now let $\boldsymbol{w} \in V$ be an arbitrary vector. We want to show that $f(\boldsymbol{w}, \boldsymbol{w}) = 0$. If $f(\boldsymbol{u}, \boldsymbol{w}) \neq f(\boldsymbol{w}, \boldsymbol{u})$ or $f(\boldsymbol{v}, \boldsymbol{w}) \neq f(\boldsymbol{w}, \boldsymbol{u})$, then by what we have just shown $f(\boldsymbol{w}, \boldsymbol{w}) = 0$ as desired so we may assume that

$$f(\boldsymbol{u}, \boldsymbol{w}) = f(\boldsymbol{w}, \boldsymbol{u}) \text{ and } f(\boldsymbol{v}, \boldsymbol{w}) = f(\boldsymbol{w}, \boldsymbol{v}).$$

Setting $\boldsymbol{x} = \boldsymbol{u}, \boldsymbol{y} = \boldsymbol{v}$ and $\boldsymbol{z} = \boldsymbol{w}$ in (8.3) and using the fact that $f(\boldsymbol{u}, \boldsymbol{w}) = f(\boldsymbol{w}, \boldsymbol{u})$ we get

$$f(\boldsymbol{u}, \boldsymbol{w})[f(\boldsymbol{u}, \boldsymbol{v}) - f(\boldsymbol{v}, \boldsymbol{u})] = 0. \tag{8.5}$$

Since $f(\boldsymbol{u}, \boldsymbol{v}) \neq f(\boldsymbol{v}, \boldsymbol{u})$, we conclude from (8.5) that $f(\boldsymbol{u}, \boldsymbol{w}) = 0$. Similarly, setting $\boldsymbol{x} = \boldsymbol{v}, \boldsymbol{y} = \boldsymbol{u}, \boldsymbol{z} = \boldsymbol{w}$ we get that $f(\boldsymbol{v}, \boldsymbol{w}) = 0$.

Now we have

$$\begin{aligned} f(\boldsymbol{u} + \boldsymbol{w}, \boldsymbol{v}) &= f(\boldsymbol{u}, \boldsymbol{v}) + f(\boldsymbol{w}, \boldsymbol{v}) \\ &= f(\boldsymbol{u}, \boldsymbol{v}) \end{aligned}$$

and

$$\begin{aligned} f(\boldsymbol{v}, \boldsymbol{u} + \boldsymbol{w}) &= f(\boldsymbol{v}, \boldsymbol{u}) + f(\boldsymbol{v}, \boldsymbol{w}) \\ &= f(\boldsymbol{v}, \boldsymbol{u}). \end{aligned}$$

Since $f(\boldsymbol{u}, \boldsymbol{v}) \neq f(\boldsymbol{v}, \boldsymbol{u})$ we can conclude that $f(\boldsymbol{u} + \boldsymbol{w}, \boldsymbol{v}) \neq f(\boldsymbol{v}, \boldsymbol{u} + \boldsymbol{w})$. It follows that $f(\boldsymbol{u} + \boldsymbol{w}, \boldsymbol{u} + \boldsymbol{w}) = 0$. Since $f(\boldsymbol{u}, \boldsymbol{u}) = f(\boldsymbol{u}, \boldsymbol{w}) = 0$ we finally conclude that $f(\boldsymbol{w}, \boldsymbol{w}) = 0$. Since $\boldsymbol{w}$ is arbitrary, f is alternating.

The next definition introduces a concept that is closely related to symmetric forms.

Definition 8.9 *A bilinear form f on a finite-dimensional vector space V is* **diagonalizable** *if there is a basis $\mathcal{B}$ such that the matrix of f with respect to $\mathcal{B}$ is a diagonal matrix.*

It follows from Lemma (8.8) that a diagonalizable form is symmetric. There is a partial converse that we will prove in a later section.

Exercises.

1. Prove the assertion of Example (8.4).

2. Prove the assertion of Example (8.5).

3. Prove Theorem (8.3).

4. Prove Corollary (8.1)

5. Assume $dim(V) = m$ and $dim(W) = n$ with $m < n$ and $f \in B(V, W; \mathbb{F})$. Prove that $dim(Rad_R(f)) \geq n - m$.

6. Give an example of a bilinear form on a vector space V such that $Rad_L(f) \neq Rad_R(f)$.

7. Give an example of a degenerate bilinear form on a vector space V such that $Rad_L(f) = Rad_R(f)$ but f is not reflexive.

8. Give an example of a non-degenerate form which is not reflexive.

9. Let $f : V^2 \rightarrow \mathbb{F}$ be a bilinear form and assume the characteristic of $\mathbb{F}$ is not two. Prove that f can be expressed in a unique way as the sum of a symmetric and alternating form.

10. Prove that the relation of equivalence on $n \times m$ matrices is an equivalence relation.

11. Prove that two $n \times m$ matrices have the same rank if and only if they are equivalent.

12. Prove that the relation of congruence on $n \times n$ matrices is an equivalence relation.

13. Let $f \in B(V, W; \mathbb{F})$ be a bilinear form where V is an n-dimensional space and W is an $m-$dimensional space. Show that $dim(V/Rad_L(f)) = dim(W/Rad_R(f))$.

14. Let $f \in B(V, W; \mathbb{F})$ where V and W are finite-dimensional vectors spaces over $\mathbb{F}$. Assume $Rad_L(f) = \{\mathbf{0}_V\}$ and $Rad_R(f) = \{\mathbf{0}_W\}$. Prove $dim(V) = dim(W)$.

15. Prove Lemma (8.6).

16. Let V be a finite-dimensional vector space, $f : V \times W \rightarrow \mathbb{F}$ a non-degenerate bilinear form, and $\mathcal{B}_V = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ a basis for V. Prove that there exists a basis $\mathcal{B}_W = (\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n)$ for W such that $f(\boldsymbol{v}_i, \boldsymbol{w}_j) = 0$ if $i \neq j$ and 1 if $i = j$.

8.2 Symplectic Spaces

This section is devoted to the structure of symplectic space, that is, a vector space equipped with an alternating form. We introduce the notion of an isometry of a symplectic space. We quickly specialize to the case that the alternating form is non-degenerate. We show the existence of a certain type of basis, referred to as a hyperbolic basis. We conclude the section by proving Witt's theorem for non-degenerate symplectic spaces.

What You Need to Know

To make sense of the new material of this section, it is essential that you have already mastered the following concepts: vector space, basis of a vector space, dimension of a vector space, finite-dimensional vector space, linear transformation, coordinate vector with respect to a basis, matrix of a linear transformation, bilinear form, reflexive bilinear form, and an alternating bilinear form. Finally, you should be familiar with the notion of a group, which can be found in Appendix B.

We begin with a definition:

Definition 8.10 *A* **symplectic space** *is a pair* $(V, \langle \ , \ \rangle)$ *consisting of a vector space* V *and a bilinear alternating form* $\langle \ , \ \rangle$*. The space is* **non-degenerate** *if the form* $\langle \ , \ \rangle$ *is non-degenerate, that is,* $Rad(\langle \ , \ \rangle) = \{\mathbf{0}\}$*. The dimension of a symplectic space* $(V, \langle \ , \ \rangle)$ *is the dimension of* V*.*

One of the major goals in this section will be to show that any two non-degenerate symplectic spaces over the same field with the same dimension are essentially the same. We need to make precise what we might mean when we say that two symplectic spaces are the same and we do so in the next definition.

Definition 8.11 *Assume* $(V, \langle \ , \ \rangle_V)$ *and* $(W, \langle \ , \ \rangle_W)$ *are symplectic spaces. By an* **isometry** *from* V *to* W *we shall mean a vector space isomorphism* $T : V \to W$ *such that for all* $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V, \langle T(\boldsymbol{v}_1), T(\boldsymbol{v}_2)\rangle_W = \langle \boldsymbol{v}_1, \boldsymbol{v}_2\rangle_V$*. When there exists an isometry* T *from* V *to* W *we will say that* $(V, \langle \ , \ \rangle_V)$ *and* $(W, \langle \ , \ \rangle_W)$ *are* **isometric**.

The next lemma is not difficult to prove and we leave it as an exercise.

Lemma 8.9 *Assume $(V, \langle\ ,\ \rangle_V), (W, \langle\ ,\ \rangle_W)$, and $(X, \langle\ ,\ \rangle_X)$ are symplectic spaces and that $S : V \to W$ and $T : W \to X$ are isometries. Then the following hold:*

i) The inverse map $S^{-1} : W \to V$ is an isometry.

ii) The composition $T \circ S : V \to X$ is an isometry.

Remark 8.4 *1) It follows from Lemma (8.9) that the relation that two symplectic spaces are isometric is an equivalence relation.*

2) If $(V, \langle\ ,\ \rangle)$ is a symplectic space then the subset of $GL(V)$ consisting of all isometries of V is a group.

In light of the second part of Remark (8.4), we make the following definition:

Definition 8.12 *Let $(V, \langle\ ,\ \rangle)$ be a symplectic space. The collection of all isometries $T : V \to V$ is the* **symplectic group** *of $(V, \langle\ ,\ \rangle)$. It is denoted by $Sp(V)$.*

If $(V, \langle\ ,\ \rangle)$ is a symplectic space and U is a vector subspace of V, then it is natural to consider the symplectic space obtained by equipping U with the form $\langle\ ,\ \rangle$ restricted to $U \times U$. We formalize this in the following definition.

Definition 8.13 *Let $(V, \langle\ ,\ \rangle)$ be a symplectic space. By a subspace of $(V, \langle\ ,\ \rangle)$, we shall mean a pair $(U, \langle\ ,\ \rangle_U)$ consisting of a vector subspace U of V together with the alternating form obtained by restricting $\langle\ ,\ \rangle$ to $U \times U$. By the* **radical** *of the subspace $U, Rad(U)$, we will mean $\{\boldsymbol{v} \in U | \langle \boldsymbol{v}, \boldsymbol{u} \rangle = 0, \forall \boldsymbol{u} \in U\}$. The subspace U is* **non-degenerate** *if $Rad(U) = \{\mathbf{0}\}$.*

Definition 8.14 *If U is a subspace such that $U = Rad(U)$, then for every pair of vectors $\boldsymbol{u}, \boldsymbol{v} \in U, \langle \boldsymbol{u}, \boldsymbol{v} \rangle = 0$. Such subspaces are said to be* **totally isotropic***.*

Definition 8.15 *Recall, if $(V, \langle\ ,\ \rangle)$ is a symplectic space and $\boldsymbol{u}, \boldsymbol{v}$ vectors in V then $\boldsymbol{u}$ and $\boldsymbol{v}$ are* **orthogonal** *if $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = 0$ and we write $\boldsymbol{u} \perp \boldsymbol{v}$.*

Now assume that U is a subspace of V. The **orthogonal complement** *to U, denoted by $U^\perp$, is the collection of all vectors, which are orthogonal to every vector in U:*

$$U^\perp = \{\boldsymbol{v} \in V | \langle \boldsymbol{v}, \boldsymbol{u} \rangle = 0, \forall \boldsymbol{u} \in U\}.$$

As an immediate consequence of the bilinearity of $\langle\ ,\ \rangle$, we have:

Lemma 8.10 *Assume U is a subspace of the symplectic space $(V, \langle\ ,\ \rangle)$. Then $U^\perp$ is a subspace.*

The following lemma is also an easy consequence of the definitions.

Lemma 8.11 *Let U be a subspace of a symplectic space $(V, \langle\ ,\ \rangle)$. Then $U \cap U^\perp = Rad(U)$.*

Proof *Assume that $\boldsymbol{v} \in Rad(U)$. Then $\boldsymbol{v} \in U$ and $\langle \boldsymbol{v}, \boldsymbol{u}\rangle = 0$ for all $\boldsymbol{u} \in U$, in which case also $\boldsymbol{v} \in U^\perp$. Thus, $\boldsymbol{v} \in U \cap U^\perp$ and we have $Rad(U) \subset U \cap U^\perp$.*

Conversely, assume $\boldsymbol{v} \in U \cap U^\perp$. Then $\langle \boldsymbol{v}, \boldsymbol{u}\rangle = 0$ for all $\boldsymbol{u} \in U$. Since $\boldsymbol{v} \in U$ we can conclude that $\boldsymbol{v} \in Rad(U)$. Therefore $U \cap U^\perp \subset Rad(U)$ and we have equality.

An important consequence of Lemma (8.11) is:

Corollary 8.2 *Assume U is a non-degenerate subspace of a symplectic space $(V, \langle\ ,\ \rangle)$. Then $U \cap U^\perp = \{\boldsymbol{0}\}$.*

Recall when we studied finite-dimensional inner product spaces we proved that the space was always a direct sum of a subspace and its orthogonal complement. The corresponding statement is not in general true for symplectic spaces. However, it is true if we restrict ourselves to non-degenerate subspaces. This will depend on the following result which states that $dim(U) + dim(U^\perp) = dim(V)$.

Lemma 8.12 *i) Let $(V, \langle\ ,\ \rangle)$ be a non-degenerate finite-dimensional symplectic space and U a subspace. Then $dim(U) + dim(U^\perp) = dim(V)$.*

ii) If U is a non-degenerate subspace of V, then $V = U \oplus U^\perp$.

iii) If U is a non-degenerate subspace of V, then $U^\perp$ is non-degenerate.

Proof *i) Set $n = dim(V)$ and $k = dim(U)$. Let $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$ be a basis for U and extend this to a basis $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n)$ for V. By Exercise 9 of Section (8.1), there is a basis $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n)$ of V such that $\langle \boldsymbol{u}_i, \boldsymbol{w}_j\rangle = 0$ if $i \neq j$ and 1 if $i = j$. Suppose $\boldsymbol{w} = \sum_{l=1}^n c_l \boldsymbol{w}_l \in U^\perp$, and $i \leq k$. Then*

$$0 = \langle \boldsymbol{u}_i, \boldsymbol{w}\rangle = \langle \boldsymbol{u}_i, \sum_{l=1}^n c_l \boldsymbol{w}_l\rangle = \sum_{l=1}^n c_l \langle \boldsymbol{u}_i, \boldsymbol{w}_l\rangle = c_i.$$

This implies that $U^{\perp} \subset Span(\boldsymbol{w}_{k+1}, \dots, \boldsymbol{w}_n)$. On the other hand, if $i \leq k$ and $l > k$, then $\langle \boldsymbol{u}_i, \boldsymbol{w}_l \rangle = 0$. Therefore $Span(\boldsymbol{w}_{k+1}, \dots, \boldsymbol{w}_n) \subset U^{\perp}$. Consequently, $U^{\perp} = Span(\boldsymbol{w}_{k+1}, \dots, \boldsymbol{w}_n)$. Since $(\boldsymbol{w}_{k+1}, \dots, \boldsymbol{w}_n)$ is linearly independent we have $dim(U^{\perp}) = n - k$.

ii) If U is non-degenerate, then $U \cap U^{\perp} = \{\mathbf{0}\}$ by Corollary (8.2). Then $U + U^{\perp} = U \oplus U^{\perp}$ and $dim(U + U^{\perp}) = dim(U) + dim(U^{\perp}) = dim(V)$ by part i). It follows that $U \oplus U^{\perp} = V$.

iii) We leave this as an exercise.

Corollary 8.3 *Let $(V, \langle\ ,\ \rangle)$ be a finite-dimensional non-degenerate symplectic space and U a subspace of V. Then $(U^{\perp})^{\perp} = U$.*

We leave this as an exercise.

We can now prove that the dimension of a finite-dimensional non-degenerate symplectic space is even and also show the existence of a very special basis for V.

Theorem 8.7 *Let $(V, \langle\ ,\ \rangle)$ be a finite-dimensional non-degenerate symplectic space. Then the following hold:*

i) The dimension of V is even.

ii) There exists a basis $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ for V such that

a. $\langle \boldsymbol{u}_i, \boldsymbol{u}_j \rangle = \langle \boldsymbol{v}_i, \boldsymbol{v}_j \rangle = 0$ for all $1 \leq i, j \leq n$;

b. $\langle \boldsymbol{u}_i, \boldsymbol{v}_j \rangle = 0$ for $i \neq j$; and

c. $\langle \boldsymbol{u}_i, \boldsymbol{v}_i \rangle = 1$.

Proof *i) The proof is by induction on $dim(V)$. Let $\boldsymbol{u} \in V$. Since V is non-degenerate it has a trivial radical. In particular, $\boldsymbol{u}$ is not in the radical of $\langle\ ,\ \rangle$ and therefore there must exist $\boldsymbol{v} \in V$ such that $\langle \boldsymbol{u}, \boldsymbol{v} \rangle \neq 0$. Note if $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = c$ then $\langle \boldsymbol{u}, \frac{1}{c}\boldsymbol{v} \rangle = 1$, so without loss of generality we may assume that $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = 1$.*

Set $U = Span(\boldsymbol{u}, \boldsymbol{v})$. If $\boldsymbol{x} \in Span(\boldsymbol{v})$ then $\langle \boldsymbol{u}, \boldsymbol{x} \rangle \neq 0$. If $\boldsymbol{x} \notin Span(\boldsymbol{v})$, then $\boldsymbol{x} = a\boldsymbol{u} + b\boldsymbol{v}$ with $a \neq 0$. Then $\langle \boldsymbol{x}, \boldsymbol{v} \rangle = b \neq 0$. This proves that U is non-degenerate. By Lemma (8.12), $U^{\perp}$ is non-degenerate. Since $dim(U^{\perp}) = dim(V) - dim(U) = dim(V) - 2$, in particular, $dim(U^{\perp}) < dim(U)$. Now we can invoke the inductive hypothesis and conclude that $dim(U^{\perp})$ is even. Since $dim(V) = dim(U^{\perp}) + 2$ this implies that $dim(V)$ is even.

ii) We may now assume that $dim(V) = 2n$ for some natural number n. We proceed by induction on n. If $n = 1$, then we are done by the proof of the first part. Suppose then that $n > 1$. Let $U = Span(\boldsymbol{u}, \boldsymbol{v})$ as in part 1). As *shown there, $U^{\perp}$ is non-degenerate and has dimension $2n-2=2(n-1)$. We can therefore invoke the inductive hypothesis and say that there exists a basis $(\boldsymbol{u}_1,\dots,\boldsymbol{u}_{n-1},\boldsymbol{v}_1,\dots,\boldsymbol{v}_{n-1})$ such that*

a. $\langle \boldsymbol{u}_i,\boldsymbol{u}_j\rangle=\langle \boldsymbol{v}_i,\boldsymbol{v}_j\rangle=0$ for all $1\le i,j\le n-1$;

b. $\langle \boldsymbol{u}_i,\boldsymbol{v}_j\rangle=0$ for $i\ne j$; and

c. $\langle \boldsymbol{u}_i,\boldsymbol{v}_i\rangle=1$.

Now set $\boldsymbol{u}_n=\boldsymbol{u},\boldsymbol{v}_n=\boldsymbol{v}$. It is now the case that $(\boldsymbol{u}_1,\dots,\boldsymbol{u}_n,\boldsymbol{v}_1,\dots,\boldsymbol{v}_n)$ is a basis of V with the required properties.

Definition 8.16 *Let $(V,\langle\ ,\ \rangle)$ be a non-degenerate symplectic space of dimension $2n$. A basis $(\boldsymbol{u}_1,\dots,\boldsymbol{u}_n,\boldsymbol{v}_1,\dots,\boldsymbol{v}_n)$ that satisfies the conclusions of part ii) of Theorem (8.7) is said to be a* **hyperbolic basis**.

Lemma 8.13 *Assume $(V,\langle\ ,\ \rangle)$ is a non-degenerate symplectic space of dimension $2n$ and U is a totally isotropic subspace. Then the following hold:*

i) dim$(U)\le n$; and

ii) U is the radical of $U^{\perp}$.

We leave these as exercises.

We will use the next lemma in proving the major result of this section. It says that any linearly independent sequence of mutually orthogonal vectors can be embedded into a hyperbolic basis.

Lemma 8.14 *Let $(V,\langle\ ,\ \rangle)$ be a non-degenerate symplectic space of dimension $2n$ and assume $\mathcal{S}=(\boldsymbol{u}_1,\dots,\boldsymbol{u}_k)$ is an independent sequence of vectors satisfying $\langle \boldsymbol{u}_i,\boldsymbol{u}_j\rangle=0$ for all i,j. Then $\mathcal{S}$ can extended to a hyperbolic basis.*

Proof *The proof is by induction on n. We first treat the case that $k=n$. Extend $\mathcal{S}$ to a basis $\mathcal{B}=(\boldsymbol{u}_1,\dots,\boldsymbol{u}_{2n})$. By Exercise 9 of Section (8.1), there exists a basis $(\boldsymbol{x}_1,\dots,\boldsymbol{x}_{2n})$ such that $\langle \boldsymbol{u}_i,\boldsymbol{x}_j\rangle=0$ if $i\ne j$ and 1 if $i=j$. Set $\boldsymbol{v}_1=\boldsymbol{x}_1$ and $U=Span(\boldsymbol{u}_1,\boldsymbol{v}_1)$, a non-degenerate subspace of dimension 2. By Lemmas (8.12), $U^{\perp}$ is a non-degenerate subspace of dimension $2n-2$. Note that $\boldsymbol{u}_i\in U^{\perp}$ for $2\le i\le n$. We can now invoke the induction hypothesis and conclude that there are vectors $\boldsymbol{v}_2,\dots,\boldsymbol{v}_n\in U^{\perp}$ such that $(\boldsymbol{u}_2,\dots,\boldsymbol{u}_n,\boldsymbol{v}_2,\dots,\boldsymbol{v}_n)$ is a hyperbolic basis of $U^{\perp}$. It then follows that $(\boldsymbol{u}_1,\dots,\boldsymbol{u}_n,\boldsymbol{v}_1,\dots,\boldsymbol{v}_n)$ is a hyperbolic basis of V.*

Suppose now that $k<n$ and set $U=Span(\boldsymbol{u}_1,\dots,\boldsymbol{u}_k)$. By Lemma (8.12),

the dimension of $U^\perp$ is $2n-k>k$ and by part ii) of Lemma (8.13) U is the radical of $U^\perp$. Let W be a complement to U in $U^\perp$. Then W is non-degenerate of dimension $2n-2k$ and $W^\perp$ is non-degenerate of dimension $2k$ and contains U. By induction, we can extend $(\boldsymbol{u}_1,\dots,\boldsymbol{u}_k)$ to a hyperbolic basis $(\boldsymbol{u}_1,\dots,\boldsymbol{u}_k,\boldsymbol{v}_1,\dots,\boldsymbol{v}_k)$ of $W^\perp$. If $(\boldsymbol{u}_{k+1},\dots,\boldsymbol{u}_n,\boldsymbol{v}_{k+1},\dots,\boldsymbol{v}_n)$ is a hyperbolic basis of W then $(\boldsymbol{u}_1,\dots,\boldsymbol{u}_n,\boldsymbol{v}_1,\dots,\boldsymbol{v}_n)$ is a hyperbolic basis of V.

Remark 8.5 *From the proof of Lemma (8.14), it follows that if W is a non-degenerate subspace then any hyperbolic basis $\mathcal{H}_W$ can be extended to a hyperbolic basis $\mathcal{H}$ of V.*

Given a hyperbolic basis $\mathcal{H}=(\boldsymbol{u}_1,\dots,\boldsymbol{u}_n,\boldsymbol{v}_1,\dots,\boldsymbol{v}_n)$ and two vectors $\boldsymbol{x},\boldsymbol{y}$ expressed as a linear combination of the vectors in $\mathcal{H}$, it is easy to compute $\langle\boldsymbol{x},\boldsymbol{y}\rangle$: Say $\boldsymbol{x}=\sum_{i=1}^n(a_i\boldsymbol{u}_i+b_i\boldsymbol{v}_i)$ and $\boldsymbol{y}=\sum_{i=1}^n(c_i\boldsymbol{u}+d_i\boldsymbol{v}_i)$. Then

$$\langle\boldsymbol{x},\boldsymbol{y}\rangle=\sum_{i=1}^n(a_id_i-b_ic_i). \tag{8.6}$$

We can use this to prove the following characterization of the isometries of a symplectic space.

Theorem 8.8 *Let $(V,\langle\ ,\ \rangle_V)$ and $(W,\langle\ ,\ \rangle_W)$ be $2n$-dimensional non-degenerate symplectic spaces over the field $\mathbb{F}$. Let $\mathcal{H}_V=(\boldsymbol{u}_1,\dots,\boldsymbol{u}_n,\boldsymbol{v}_1,\dots,\boldsymbol{v}_n)$ be a hyperbolic basis for V and assume T is a linear transformation from V to W. Set $\boldsymbol{w}_i=T(\boldsymbol{u}_i)$ and $\boldsymbol{x}_i=T(\boldsymbol{v}_i)$. Then T is an isometry if and only if $(\boldsymbol{w}_1,\dots,\boldsymbol{w}_n,\boldsymbol{x}_1,\dots,\boldsymbol{x}_n)$ is a hyperbolic basis of W.*

Proof *Assume $(\boldsymbol{w}_1,\dots,\boldsymbol{w}_n,\boldsymbol{x}_1,\dots,\boldsymbol{x}_n)$ is a hyperbolic basis for W. Let $\boldsymbol{y},\boldsymbol{z}\in V$. We need to show that $\langle T(\boldsymbol{y}),T(\boldsymbol{z})\rangle_W=\langle\boldsymbol{y},\boldsymbol{z}\rangle_V$.*

Assume $\boldsymbol{y}=\sum_{i=1}^n(a_i\boldsymbol{u}_i+b_i\boldsymbol{v}_i)$ and $\boldsymbol{z}=\sum_{i=1}^n(c_i\boldsymbol{u}_i+d_i\boldsymbol{v}_i)$. By (8.6), we have

$$\langle\boldsymbol{y},\boldsymbol{z}\rangle_V=\sum_{i=1}^n(a_id_i-b_ic_i).$$

On the other hand, $T(\boldsymbol{y})=T(\sum_{i=1}^n(a_i\boldsymbol{u}_i+b_i\boldsymbol{v}_i))=\sum_{i=1}^n(a_iT(\boldsymbol{u}_i)+b_iT(\boldsymbol{v}_i))=\sum_{i=1}^n(a_i\boldsymbol{w}_i+b_i\boldsymbol{x}_i)$. Similarly, $T(\boldsymbol{z})=\sum_{i=1}^n(c_i\boldsymbol{w}_i+d_i\boldsymbol{x}_i)$. We can apply (8.6) and conclude that

$$\langle T(\boldsymbol{w}),T(\boldsymbol{x})\rangle_W=\sum_{i=1}^n(a_id_i-b_ic_i).$$

Thus, T is an isometry.

Conversely, assume that T is an isometry. Then

$$\langle \boldsymbol{w}_i, \boldsymbol{w}_j \rangle_W = \langle T(\boldsymbol{u}_i), T(\boldsymbol{u}_j) \rangle_W = \langle \boldsymbol{u}_i, \boldsymbol{u}_j \rangle_V = 0.$$

$$\langle \boldsymbol{x}_i, \boldsymbol{x}_i \rangle_W = \langle T(\boldsymbol{v}_i), T(\boldsymbol{v}_j) \rangle_W = \langle \boldsymbol{v}_i, \boldsymbol{v}_j \rangle_V = 0.$$

$\langle \boldsymbol{w}_i, \boldsymbol{x}_j \rangle_W = \langle T(\boldsymbol{u}_i), T(\boldsymbol{v}_j) \rangle_W = \langle \boldsymbol{u}_i, \boldsymbol{v}_j \rangle_V = 0$ *if* $i \neq j$ *and 1 if* $i = j$. *Thus,* $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ *is a hyperbolic basis as claimed.*

As a consequence of Theorem (8.8), we have the following:

Theorem 8.9 *Let* $(V, \langle\ ,\ \rangle_V)$ *and* $(W, \langle\ ,\ \rangle_W)$ *be two finite-dimensional non-degenerate symplectic spaces over the same field* $\mathbb{F}$. *Then* V *and* W *are isometric if and only if dim*$(V) =$ *dim*(W).

One of our ultimate goals is to show that if $(V_1, \langle\ ,\ \rangle_1)$ and $(V_2, \langle\ ,\ \rangle_2)$ are non-degenerate symplectic spaces of dimension $2n$, U_i is a subspace of $V_i, i = 1, 2$, and U_1, U_2 are isometric by a transformation σ, then there is an isometry $S : V_1 \to V_2$ such that $S_{|_{U_1}} = \sigma$. We will prove several lemmas leading up to this result. We begin with a result about extending isometries of non-degenerate subspaces.

Lemma 8.15 *Let* $(V, \langle\ ,\ \rangle)$ *be a non-degenerate finite-dimensional symplectic space,* U *a non-degenerate subspace, and* σ *an isometry of* U. *Define* $S : V \to V$ *as follows: For* $\boldsymbol{x} = \boldsymbol{u} + \boldsymbol{v}$ *with* $\boldsymbol{u} \in U, \boldsymbol{v} \in U^{\perp}$, $S(\boldsymbol{x}) = \sigma(\boldsymbol{u}) + \boldsymbol{v}$. *Then* S *is an isometry of* V.

Proof *Suppose* $\boldsymbol{x}_1 = \boldsymbol{u}_1 + \boldsymbol{v}_1, \boldsymbol{x}_2 = \boldsymbol{u}_2 + \boldsymbol{v}_2$ *where* $\boldsymbol{u}_i \in U, \boldsymbol{v}_i \in U^{\perp}$. *We need to show that* $\langle \boldsymbol{x}_1, \boldsymbol{x}_2 \rangle = \langle S(\boldsymbol{x}_1), S(\boldsymbol{x}_2) \rangle$.

$$\langle \boldsymbol{x}_1, \boldsymbol{x}_2 \rangle = \langle \boldsymbol{u}_1 + \boldsymbol{v}_1, \boldsymbol{u}_2 + \boldsymbol{v}_2 \rangle = \langle \boldsymbol{u}_1, \boldsymbol{u}_2 \rangle + \langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle$$

since $\langle \boldsymbol{u}_i, \boldsymbol{v}_j \rangle = 0$. *On the other hand,*

$$\begin{aligned} \langle S(\boldsymbol{x}_1), S(\boldsymbol{x}_2) \rangle &= \langle S(\boldsymbol{u}_1 + \boldsymbol{v}_1), S(\boldsymbol{u}_2 + \boldsymbol{v}_2) \rangle \\ &= \langle \sigma(\boldsymbol{u}_1) + \boldsymbol{v}_1, \sigma(\boldsymbol{u}_2) + \boldsymbol{v}_2 \rangle \\ &= \langle \sigma(\boldsymbol{u}_1), \sigma(\boldsymbol{u}_2) \rangle + \langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle \end{aligned}$$

by the definition of S *and the fact that* $\sigma(\boldsymbol{u}_i) \in U$ *and therefore orthogonal to* $\boldsymbol{v}_j$. *However,* $\langle \sigma(\boldsymbol{u}_1), \sigma(\boldsymbol{u}_2) \rangle = \langle \boldsymbol{u}_1, \boldsymbol{u}_2 \rangle$ *by hypothesis and therefore we have the desired equality.*

We now prove a lemma that gives a "transitivity" result for non-zero vectors of a non-degenerate symplectic space. This is a precursor to the more general Witt theorem, which we will prove below.

Lemma 8.16 *Let $(V, \langle\ ,\ \rangle)$ be a finite-dimensional non-degenerate symplectic space and $\boldsymbol{u}, \boldsymbol{v}$ non-zero vectors. Then there exists an isometry T such that $T(\boldsymbol{u}) = \boldsymbol{v}$.*

Proof *First assume that $\langle \boldsymbol{u}, \boldsymbol{v}\rangle = c \neq 0$. Then $(\boldsymbol{u}, \frac{1}{c}\boldsymbol{v})$ is a hyperbolic basis of Span$(\boldsymbol{u}, \boldsymbol{v})$. Likewise, $(\boldsymbol{v}, -\frac{1}{c}\boldsymbol{u})$ is a hyperbolic basis of Span$(\boldsymbol{u}, \boldsymbol{v})$. Therefore, there exists an isometry σ of Span$(\boldsymbol{u}, \boldsymbol{v})$ such that $\sigma(\boldsymbol{u}) = \boldsymbol{v}, \sigma(\boldsymbol{v}) = -\boldsymbol{u}$. By Lemma (8.15), this extends to an isometry of V.*

Now suppose $\langle \boldsymbol{u}, \boldsymbol{v}\rangle = 0$. Since V is non-degenerate, there exists a vector $\boldsymbol{w}$ such that $\langle \boldsymbol{u}, \boldsymbol{w}\rangle \neq 0$. Suppose also that $\langle \boldsymbol{v}, \boldsymbol{w}\rangle \neq 0$. Then by what we have shown there are isometries S, T such that $S(\boldsymbol{u}) = \boldsymbol{w}, T(\boldsymbol{w}) = \boldsymbol{v}$ and then $(T \circ S)(\boldsymbol{u}) = \boldsymbol{v}$. Thus, we may assume that $\langle \boldsymbol{v}, \boldsymbol{w}\rangle = 0$.

Since V is non-degenerate, there is a vector $\boldsymbol{x}$ such that $\langle \boldsymbol{v}, \boldsymbol{x}\rangle \neq 0$. As in the previous paragraph, if $\langle \boldsymbol{u}, \boldsymbol{x}\rangle \neq 0$, we are done, and therefore we may assume that $\langle \boldsymbol{u}, \boldsymbol{x}\rangle = 0$. Now set $\boldsymbol{z} = \boldsymbol{w} + \boldsymbol{x}$. Then $\langle \boldsymbol{u}, \boldsymbol{z}\rangle = \langle \boldsymbol{u}, \boldsymbol{w}\rangle \neq 0$ and $\langle \boldsymbol{v}, \boldsymbol{z}\rangle = \langle \boldsymbol{v}, \boldsymbol{x}\rangle \neq 0$, and we are done by the paragraph above.

The next theorem may be considered a generalization of Lemma (8.16). Basically, it means that if two subspaces of a finite-dimensional non-degenerate symplectic space $(V, \langle\ ,\ \rangle)$ are isometric, then there is an isometry of V taking one to the other. It is known as the *Witt Extension Theorem for Symplectic Space.*

Theorem 8.10 *Let $(V, \langle\ ,\ \rangle)$ be a finite-dimensional non-degenerate symplectic space, U and W subspaces of V, and assume that σ is an isometry of U onto W. Then there exists an isometry S of V such that S restricted to U is σ.*

Proof *Suppose first that U is totally isotropic. Let $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$ be a basis of U and set $\boldsymbol{w}_i = \sigma(\boldsymbol{u}_i)$. Then $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k)$ is linearly independent and $\boldsymbol{w}_i \perp \boldsymbol{w}_j$ for all i, j. By Lemma (8.14), we can extend $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$ to a hyperbolic basis $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$, and we can extend $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k)$ to a hyperbolic basis $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$. There is a unique linear operator on V such that $S(\boldsymbol{u}_i) = \boldsymbol{w}_i$ and $S(\boldsymbol{v}_i) = \boldsymbol{x}_i$ for $1 \leq i \leq n$. By Lemma (8.8), S is an isometry. Since $S(\boldsymbol{u}_i) = \boldsymbol{w}_i = \sigma(\boldsymbol{u}_i)$, S restricted to U is σ.*

Next suppose U is non-degenerate. Then dim$(U) = 2k$, and we may assume $k < n$ (otherwise, we are done). Choose a hyperbolic basis $\mathcal{H}_U =$

$(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)$ of U and set $\boldsymbol{w}_i = \sigma(\boldsymbol{u}_i)$ and $\boldsymbol{x}_i = \sigma(\boldsymbol{v}_i)$. Then $\mathcal{H}_W = (\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_k)$ is a hyperbolic basis of W. By Remark (8.5), $\mathcal{H}_U$ can be extended to a hyperbolic basis $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ of V and, likewise, $\mathcal{H}_W$ can be extended to a hyperbolic basis $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ of V. As in the previous paragraph, there is a unique linear operator on V such that $S(\boldsymbol{u}_i) = \boldsymbol{w}_i$ and $S(\boldsymbol{v}_i) = \boldsymbol{x}_i$ for $1 \le i \le n$. S is an isometry Tby heorem (8.8) and S restricted to U is σ.

It remains to consider the case that U is neither totally isotropic nor non-degenerate. Let $R_U = Rad(U)$ and C_U be a complement to R_U in U. Then C_U is non-degenerate. Let $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ be a basis of R_U and set $\boldsymbol{w}_i = \sigma(\boldsymbol{u}_i)$. Also, let $(\boldsymbol{p}_1, \ldots, \boldsymbol{p}_l, \boldsymbol{q}_1, \ldots, \boldsymbol{q}_l)$ be a hyperbolic basis for C_U. Set $\boldsymbol{y}_i = \sigma(\boldsymbol{p}_i), \boldsymbol{z}_i = \sigma(\boldsymbol{q}_i)$. It must now be the case that $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k)$ is a basis for R_W, the radical of W, and that $Span(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_l, \boldsymbol{z}_1, \ldots, \boldsymbol{z}_l)$ is a complement to R_W in W. Set $U' = C_U^{\perp}$ and $W' = C_W^{\perp}$. Then U' is non-degenerate and contains R_U. Likewise W' is non-degenerate and contains R_W. Extend $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$ to a hyperbolic basis $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)$ for U' and extend $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k)$ to a hyperbolic basis $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_m)$ for W'. Now set $S(\boldsymbol{u}_i) = \boldsymbol{w}_i, 1 \le i \le m, S(\boldsymbol{v}_i) = \boldsymbol{x}_i, 1 \le i \le m, S(\boldsymbol{p}_j) = \boldsymbol{y}_j, 1 \le j \le l$ and $S(\boldsymbol{q}_j) = \boldsymbol{z}_j, 1 \le j \le l$. Then S is an isometry of V by Theorem (8.8), and S restricted to U is the map σ.

Exercises

1. Prove Lemma (8.9).

2. Prove Lemma (8.10).

3. Let U be a subspace of a non-degenerate finite-dimensional symplectic space. Prove that $(U^{\perp})^{\perp} = U$.

4. Prove part iii) of Lemma (8.12).

5. Let U be a totally isotropic subspace of a non-degenerate symplectic space of dimension $2n$. Prove that $dim(U) \le n$.

6. Let U be a totally isotropic subspace of a non-degenerate symplectic space of dimension $2n$. Prove that $U = Rad(U^{\perp})$.

7. Let $(V, \langle\ ,\ \rangle)$ be a non-degenerate finite-dimensional symplectic space, $\boldsymbol{v}$ a non-zero vector in V, and $c \in \mathbb{F}$. Define a linear operator $T_{(\boldsymbol{v},c)}$ on V by $T_{(\boldsymbol{v},c)}(\boldsymbol{u}) = \boldsymbol{u} + c\langle \boldsymbol{u}, \boldsymbol{v}\rangle \boldsymbol{v}$. Prove that $T_{\boldsymbol{v},c}$ is an isometry of V.

8. Let $\boldsymbol{v}, \boldsymbol{w} \in V$ and c, d non-zero scalars. Prove that $T_{\boldsymbol{v},c}$ and $T_{\boldsymbol{w},d}$ commute if and only $\boldsymbol{u} \perp \boldsymbol{w}$.

9. Let $(V, \langle\ ,\ \rangle)$ be a non-degenerate $2n$-dimensional symplectic space over the finite field $\mathbb{F}_q$. Determine how many pairs there are of vectors $(\boldsymbol{u}, \boldsymbol{v})$ with $\langle \boldsymbol{u}, \boldsymbol{v}\rangle = 1$.

10. Let $(V, \langle\ ,\ \rangle)$ be a non-degenerate $2n$-dimensional symplectic space over the finite field $\mathbb{F}_q$. Use induction and Exercise 9 to show that there are

$q^{n^2}\prod_{i=1}^{n}(q^{2i}-1)$ hyperbolic bases and then conclude that this is the order of the group $Sp(V)$.

11. Prove Corollary (8.3).

8.3 Quadratic Forms and Orthogonal Space

In this section we define the notion of a quadratic form and develop the general theory of an orthogonal space. In particular, we prove Witt's theorem for an orthogonal space when the characteristic of the field is not two.

What You Need to Know

To make sense of the new material of this section, it is essential that you have already mastered the following concepts: vector space, basis of a vector space, dimension of a vector space, finite-dimensional vector space, linear transformation, coordinate vector with respect to a basis, matrix of a linear transformation, bilinear form, reflexive bilinear form, symmetric bilinear form, and the matrix of a bilinear form.

We begin with a definition:

Definition 8.17 *Let V be a vector space over a field $\mathbb{F}$. By a* **quadratic form***, we mean a function $\phi : V \to \mathbb{F}$ that satisfies the following:*

1) For $c \in \mathbb{F}$ and $\boldsymbol{v} \in V, \phi(c\boldsymbol{v}) = c^2\phi(\boldsymbol{v})$.

2) For $\boldsymbol{v}, \boldsymbol{w} \in V$, the function $\langle \boldsymbol{v}, \boldsymbol{w} \rangle_\phi = \phi(\boldsymbol{v}+\boldsymbol{w})-\phi(\boldsymbol{v})-\phi(\boldsymbol{w})$ is a symmetric bilinear form, referred to as the **symmetric form** *associated with ϕ.*

Let V be a finite-dimensional vector space over a field $\mathbb{F}, \phi$ is a quadratic form on V with associated symmetric form $\langle\ ,\ \rangle_\phi$ and $\mathcal{B}$ a basis of V. Then, by the matrix of ϕ with respect to $\mathcal{B}$, we will mean the matrix of $\langle\ ,\ \rangle_\phi$ with respect to $\mathcal{B}$. This is a symmetric matrix.

Remark 8.6 *When the field $\mathbb{F}$ has characteristic two the symmetric form associated with a quadratic form on a vector space V is alternating.*

Example 8.6 *Assume that the characteristic of$\mathbb{F}$ is not two and $f : V \times V \to \mathbb{F}$ is a symmetric form. Set $\phi(\boldsymbol{v}) = f(\boldsymbol{v}, \boldsymbol{v})$. Then ϕ is a quadratic form and the associated form $\langle\ ,\ \rangle_\phi = 2f$.*

Example 8.7 *Define $\phi : \mathbb{F}^2 \to \mathbb{F}$ by $\phi\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = x_1x_2$. This form is referred to as a two-dimensional* **hyperbolic form**.

Example 8.8 *Assume $x^2 + bx + c$ is an irreducible polynomial over the field $\mathbb{F}$. Define $\phi : \mathbb{F}^2 \to \mathbb{F}$ by $\phi\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = x_1^2 + bx_1x_2 + cx_2^2$. This form is referred to as a two-dimensional* **elliptic form***.*

In analogy with symplectic spaces, we introduce the notion of an orthogonal space.

Definition 8.18 *An* **orthogonal space** *is a pair (V, ϕ) consisting of a vector space V and a quadratic form $\phi : V \to \mathbb{F}$.*

Before we embark on our investigation of orthogonal spaces, we need to introduce some more terminology.

Definition 8.19 *Let (V, ϕ) be an orthogonal space with associated form $\langle\ ,\ \rangle_\phi$. Two vectors $\boldsymbol{v}, \boldsymbol{w}$ are said to be* **orthogonal***, and we write $\boldsymbol{v} \perp \boldsymbol{w}$, if $\langle \boldsymbol{v}, \boldsymbol{w}\rangle_\phi = 0$.*

Definition 8.20 *A vector $\boldsymbol{v}$ is said to be* **singular** *if $\phi(\boldsymbol{v}) = 0$ and* **non-singular** *otherwise.*

Definition 8.21 *Let U be a subspace of V. The* **orthogonal complement** *to U consists of all vectors in V which are orthogonal to all the vectors in U. This is denoted by $U^\perp$. Thus,*

$$U^\perp := \{\boldsymbol{v} \in V | \langle \boldsymbol{u}, \boldsymbol{v}\rangle_\phi = 0, \forall \boldsymbol{u} \in V\}.$$

Definition 8.22 *For U a subspace of V, the* **radical** *of U, denoted by $Rad(U)$, consists of all the vectors in U, which are orthogonal to every vector in U. Thus*

$$Rad(U) = U \cap U^\perp.$$

By the **rank** *of a finite-dimensional orthogonal space (V, ϕ), we will mean $dim(V) - dim(Rad(V))$.*

A subspace U is **non-degenerate** *if $Rad(U) = \{\mathbf{0}\}$. At the other extreme, U is* **totally isotropic** *if $U = Rad(U)$ and* **totally singular** *if $\phi(\boldsymbol{u}) = 0$ for every $\boldsymbol{u} \in U$.*

The orthogonal space (V, ϕ) is **non-singular** *if it is either non-degenerate or $Rad(V)$ has dimension one and for any non-zero vector $\boldsymbol{v}$ in $Rad(V), \phi(\boldsymbol{v}) \neq 0$.*

The following lemma is a simple consequence of the definitions but will prove to be quite useful. We leave the proof as an exercise.

Lemma 8.17 *Let $\boldsymbol{u}, \boldsymbol{v}$ be vectors in an orthogonal space (V, ϕ). Then $\phi(\boldsymbol{v} + \boldsymbol{w}) = \phi(\boldsymbol{v}) + \phi(\boldsymbol{w})$ if and only if $\langle \boldsymbol{v}, \boldsymbol{w} \rangle_\phi = 0$ if and only if $\boldsymbol{v} \perp \boldsymbol{w}$.*

Example 8.9 *For the orthogonal space of Example (8.7), the vectors $\begin{pmatrix} c \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ c \end{pmatrix}$ are singular vectors. All other non-zero vectors are non-singular. This form is non-degenerate.*

Example 8.10 *The orthogonal space of Example (8.8) has no non-zero singular vectors. This form is non-degenerate.*

Example 8.11 *Let $\mathbb{F}$ be a field of characteristic two. Define the form ϕ on $\mathbb{F}^3$ by*

$$\phi\left(\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}\right) = x_1 x_2 + x_3^2.$$

This form is degenerate but non-singular. The radical is the span of the vector $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$. Note that $\phi\left(\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\right) = 1$.

Remark 8.7 *Assume that the characteristic of $\mathbb{F}$ is not two. Then an orthogonal space (V, ϕ) is non-degenerate if and only if it is non-singular. This follows since $\phi(\boldsymbol{v}) = 0$ if and only if $\langle \boldsymbol{v}, \boldsymbol{v} \rangle_\phi = 0$.*

In the following definition we make rigorous the notion that two orthogonal spaces are the "same."

Definition 8.23 *Assume (V_1, ϕ_1) and (V_2, ϕ_2) are orthogonal spaces over the field $\mathbb{F}$. An isometry T from (V_1, ϕ_1) to (V_2, ϕ_2) is a vector space isomorphism $T : V_1 \to V_2$ such that for all vectors $\boldsymbol{v} \in V, \phi_2(T(\boldsymbol{v})) = \phi_1(\boldsymbol{v})$.*

As in the case of symplectic spaces, we have the following lemma about inverses and composition of isometries:

Lemma 8.18 *Assume $(V_1, \phi_1), (V_2, \phi_2)$ and (V_3, ϕ_3) are orthogonal spaces and that $S : V_1 \to V_2$ and $T : V_2 \to V_3$ are isometries. Then the following hold:*

i) The inverse map $S^{-1} : V_2 \to V_1$ is an isometry.

ii) The composition $T \circ S : V_1 \to V_3$ is an isometry.

Remark 8.8 *1) It follows from Lemma (8.9) that the relation that two orthogonal spaces are isometric is an equivalence relation.*

2) If (V, ϕ) is an orthogonal space, then the subset of $GL(V)$ consisting of all isometries of V is a subgroup.

In light of the second part of Remark (8.8), we make the following definition:

Definition 8.24 *Let (V, ϕ) be an orthogonal space. The collection of all isometries $T : V \to V$ is the* **orthogonal group** *of (V, ϕ). It is denoted by $O(V, \phi)$.*

Remark 8.9 *Let $f : V \times V \to \mathbb{F}$ be a symmetric bilinear form. By an isometry of f, we mean a bijective linear map $T : V \to V$ such that $f(T(\boldsymbol{v}), T(\boldsymbol{w})) = f(\boldsymbol{v}, \boldsymbol{w})$ for all $\boldsymbol{v}, \boldsymbol{w} \in V$. When (V, ϕ) is an orthogonal space with associated form $\langle\ ,\ \rangle_\phi$ and the characteristic of $\mathbb{F}$ is not two, the isometries of ϕ and the isometries of $\langle\ ,\ \rangle_\phi$ are the same. However, when the characteristic is two, the group of isometries of $\langle\ ,\ \rangle_\phi$ properly contains the group of isometries of ϕ.*

For the remainder of this section, we will confine ourselves to non-degenerate orthogonal spaces over fields of characteristic not two.

We state a number of lemmas that are analogues of results from the section on symplectic spaces. In most cases, we omit the proofs because of the similarity to the symplectic case.

Lemma 8.19 *i) Let (V, ϕ) be a non-degenerate finite-dimensional orthogonal space and U a subspace. Then $dim(U) + dim(U^\perp) = dim(V)$.*

ii) If U is a non-degenerate subspace of V, then $V = U \oplus U^\perp$.

iii) If U is a non-degenerate subspace of V, then $U^\perp$ is non-degenerate.

Definition 8.25 *Let (V, ϕ) be a non-degenerate finite-dimensional orthogonal space with associated form $\langle \ , \ \rangle_\phi$. A basis $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ for V is* **orthogonal** *if $\langle \boldsymbol{u}_i, \boldsymbol{u}_j \rangle_\phi = 0$ for all $i \neq j$.*

The following is a consequence of Lemma (8.17) and mathematical induction.

Lemma 8.20 *Assume $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ is an orthogonal basis for the orthogonal space (V, ϕ) with associated form $\langle \ , \ \rangle_\phi$. Set $d_i = \phi(\boldsymbol{u}_i)$. If $\boldsymbol{v} = \sum_{i=1}^n a_i \boldsymbol{u}_i$, then $\phi(\boldsymbol{v}) = \sum_{i=1}^n d_i a_i^2$.*

In our next lemma, we prove orthogonal bases always exists. It will be a consequence of this that a symmetric matrix over a field $\mathbb{F}$ of characteristic not two is congruent to a diagonal matrix.

Lemma 8.21 *Assume (V, ϕ) is a finite-dimensional orthogonal space. Then there exists an orthogonal basis for V.*

Proof *We do induction on $dim(V/Rad(V))$. Of course, if ϕ is trivial then any basis of V is an orthogonal basis and, therefore, we may assume $V \neq Rad(V)$. Let W be a complement to $Rad(V)$. If we can show that W has an orthogonal basis then we can extend this with any basis for $Rad(V)$, and the sequence obtained will be an orthogonal basis for V. Therefore, we may assume that $Rad(V) = \{\boldsymbol{0}\}$ and that V is non-degenerate.*

Let $\boldsymbol{v} \in V$ such that $\phi(\boldsymbol{v}) \neq 0$. Since the characteristic is not two, $\boldsymbol{v} \notin \boldsymbol{v}^\perp$ and $V = Span(\boldsymbol{v}) \oplus \boldsymbol{v}^\perp$. The subspace $\boldsymbol{v}^\perp$ is non-degenerate and $dim(\boldsymbol{v}^\perp) = n-1$. We can therefore invoke our inductive hypothesis and conclude that there exists an orthogonal basis $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_{n-1})$ for $\boldsymbol{v}^\perp$. Setting $\boldsymbol{v}_n = \boldsymbol{v}$ it is then the case that $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ is an orthogonal basis of V.

Corollary 8.4 *Assume $\mathbb{F}$ does not have characteristic two and A is an $n \times n$ symmetric matrix. Then A is congruent to a diagonal matrix.*

Proof *Let $\mathcal{S}$ be the standard basis of $\mathbb{F}^n$. Define a symmetric bilinear form, $\langle \ , \ \rangle : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}$, by $\langle \boldsymbol{v}, \boldsymbol{w} \rangle = \boldsymbol{v}^{tr} A \boldsymbol{w}$. Then A is the matrix of $\langle \ , \ \rangle$ with respect to $\mathcal{S}$. Since A is symmetric this form is symmetric. This defines a quadratic form ϕ defined by $\phi(\boldsymbol{v}) = \langle \boldsymbol{v}, \boldsymbol{v} \rangle$.*

Let $\mathcal{B} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ be an orthogonal basis for (V, ϕ) and set $\phi(\boldsymbol{v}_i) = d_i$ and set $P = \mathcal{M}_{I_{\mathbb{F}^n}}(\mathcal{B}, \mathcal{S})$. Then the matrix of $\langle \ , \ \rangle$ with respect to $\mathcal{B}$ is $P^{tr} A P =$

$$\begin{pmatrix} 2d_1 & 0 & \dots 0 & \\ 0 & 2d_2 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 2d_n \end{pmatrix}.$$

Our immediate goal is to prove if vectors $\boldsymbol{v}, \boldsymbol{w}$ satisfy $\phi(\boldsymbol{v}) = \phi(\boldsymbol{w})$, then there is an isometry T with $T(\boldsymbol{v}) = \boldsymbol{w}$. Toward that goal, we prove the next lemma which shows the existence of many isometries.

Until otherwise noted, we will henceforth write $\langle \boldsymbol{x}, \boldsymbol{y} \rangle$ for $\langle \boldsymbol{x}, \boldsymbol{y} \rangle_\phi$ when there is no confusion.

Lemma 8.22 *Let $\boldsymbol{x}$ be a non-singular vector. Define the map $\rho_{\boldsymbol{x}} : V \to V$ by*

$$\rho_{\boldsymbol{x}}(\boldsymbol{v}) = \boldsymbol{v} - 2\frac{\langle \boldsymbol{v}, \boldsymbol{x} \rangle}{\langle \boldsymbol{x}, \boldsymbol{x} \rangle}\boldsymbol{x}.$$

Then $\rho_{\boldsymbol{x}}$ is an isometry of V.

Proof *Let $\boldsymbol{v}, \boldsymbol{w} \in V$. We need to prove that $\langle \boldsymbol{v}, \boldsymbol{w} \rangle = \langle \rho_{\boldsymbol{x}}(\boldsymbol{v}), \rho_{\boldsymbol{x}}(\boldsymbol{w}) \rangle$.*

$$\begin{aligned}
\langle \rho_{\boldsymbol{x}}(\boldsymbol{v}), \rho_{\boldsymbol{x}}(\boldsymbol{w}) \rangle &= \langle \boldsymbol{v} - 2\frac{\langle \boldsymbol{v}, \boldsymbol{x} \rangle}{\langle \boldsymbol{x}, \boldsymbol{x} \rangle}\boldsymbol{x}, \boldsymbol{w} - 2\frac{\langle \boldsymbol{w}, \boldsymbol{x} \rangle}{\langle \boldsymbol{x}, \boldsymbol{x} \rangle}\boldsymbol{x} \rangle \\
&= \langle \boldsymbol{v}, \boldsymbol{w} \rangle - \langle \boldsymbol{v}, 2\frac{\langle \boldsymbol{w}, \boldsymbol{x} \rangle}{\langle \boldsymbol{x}, \boldsymbol{x} \rangle}\boldsymbol{x} \rangle - \langle 2\frac{\langle \boldsymbol{v}, \boldsymbol{x} \rangle}{\langle \boldsymbol{x}, \boldsymbol{x} \rangle}\boldsymbol{x}, \boldsymbol{w} \rangle + \langle 2\frac{\langle \boldsymbol{v}, \boldsymbol{x} \rangle}{\langle \boldsymbol{x}, \boldsymbol{x} \rangle}\boldsymbol{x}, 2\frac{\langle \boldsymbol{w}, \boldsymbol{x} \rangle}{\langle \boldsymbol{x}, \boldsymbol{x} \rangle}\boldsymbol{x} \rangle \\
&= \langle \boldsymbol{v}, \boldsymbol{w} \rangle - 2\frac{\langle \boldsymbol{v}, \boldsymbol{x} \rangle \langle \boldsymbol{w}, \boldsymbol{x} \rangle}{\langle \boldsymbol{x}, \boldsymbol{x} \rangle} - 2\frac{\langle \boldsymbol{v}, \boldsymbol{x} \rangle \langle \boldsymbol{x}, \boldsymbol{w} \rangle}{\langle \boldsymbol{x}, \boldsymbol{x} \rangle} + 4\frac{\langle \boldsymbol{v}, \boldsymbol{x} \rangle \langle \boldsymbol{w}, \boldsymbol{x} \rangle}{\langle \boldsymbol{x}, \boldsymbol{x} \rangle^2}\langle \boldsymbol{x}, \boldsymbol{x} \rangle \\
&= \langle \boldsymbol{v}, \boldsymbol{w} \rangle
\end{aligned}$$

Definition 8.26 *Let $\boldsymbol{x}$ be a non-singular vector in the orthogonal space (V, ϕ). The map $\rho_{\boldsymbol{x}}$ is the* **reflection** *through $\boldsymbol{x}$.*

We leave it as an exercise to show that $\rho_{\boldsymbol{x}}$ is the identity when restricted to $\boldsymbol{x}^\perp$ and $\rho_{\boldsymbol{x}}(\boldsymbol{x}) = -\boldsymbol{x}$.

This next lemma shows how an isometry can be built up from isometries on a non-degenerate subspace U and its orthogonal complement.

Lemma 8.23 *Let U be a non-degenerate subspace of the orthogonal space (V, ϕ) and suppose $\sigma_1 : U \to U$ is an isometry and $\sigma_2 : U^\perp \to U^\perp$ is an isometry. Define $S : V \to V$ by $S(\boldsymbol{u} + \boldsymbol{v}) = \sigma_1(\boldsymbol{u}) + \sigma_2(\boldsymbol{v})$, where $\boldsymbol{u} \in U$ and $\boldsymbol{v} \in U^\perp$. Then S is an isometry.*

Proof *Let* $\boldsymbol{u} \in U, \boldsymbol{v} \in U^{\perp}$. *Since* $\boldsymbol{u} \perp \boldsymbol{v}$ *by Lemma (8.17),* $\phi(\boldsymbol{u}+\boldsymbol{v}) = \phi(\boldsymbol{u})+\phi(\boldsymbol{v})$. *On the other hand,* $\sigma_1(\boldsymbol{u}) \in U$ *and* $\sigma_2(\boldsymbol{v}) \in U^{\perp}$ *so* $\sigma_1(\boldsymbol{u}) \perp \sigma_2(\boldsymbol{v})$. *Therefore we also have that*

$$\begin{aligned} \phi(S(\boldsymbol{u}+\boldsymbol{v})) &= \phi(\sigma_1(\boldsymbol{u})+\sigma_2(\boldsymbol{v})) \\ &= \phi(\sigma_1(\boldsymbol{u}))+\phi(\sigma_2(\boldsymbol{v})) \\ &= \phi(\boldsymbol{u})+\phi(\boldsymbol{v}), \end{aligned}$$

the latter equality follows since σ_1 *and* σ_2 *are isometries.*

Theorem 8.11 *Assume* $\boldsymbol{v}, \boldsymbol{w}$ *are vectors and* $\phi(\boldsymbol{v}) = \phi(\boldsymbol{w}) \neq 0$. *Then there exists an isometry* T *such that* $T(\boldsymbol{v}) = \boldsymbol{w}$.

Proof *Suppose first that* $\boldsymbol{v} \perp \boldsymbol{w}$. *Set* $U = Span(\boldsymbol{v}, \boldsymbol{w})$. *Define* $\sigma_1 : U \to U$ *by* $\sigma_1(\boldsymbol{v}) = \boldsymbol{w}, \sigma_1(\boldsymbol{w}) = \boldsymbol{v}$. *Then* σ_1 *is an isometry. Set* $\sigma_2 : U^{\perp} \to U^{\perp}$ *equal to* $1_{U^{\perp}}$, *the identity map. By Lemma (8.23), this defines an isometry* S *such that* $S(\boldsymbol{v}) = \boldsymbol{w}, S(\boldsymbol{w}) = \boldsymbol{v}$ *and* S *restricted to* $U^{\perp}$ *is the identity.*

Assume now that $\boldsymbol{v}$ *and* $\boldsymbol{w}$ *are not orthogonal. Set* $\boldsymbol{x} = \frac{1}{2}(\boldsymbol{v}+\boldsymbol{w})$ *and* $\boldsymbol{y} = \frac{1}{2}(\boldsymbol{x}-\boldsymbol{y})$. *Note that* $\boldsymbol{v} = \boldsymbol{x}+\boldsymbol{y}$ *and* $\boldsymbol{w} = \boldsymbol{x}-\boldsymbol{y}$. *We claim that* $\boldsymbol{x} \perp \boldsymbol{y}$

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \langle \frac{1}{2}(\boldsymbol{v}+\boldsymbol{w}), \frac{1}{2}(\boldsymbol{v}-\boldsymbol{w}) \rangle$$

$$= \frac{1}{4}(\langle \boldsymbol{v}, \boldsymbol{v} \rangle - \langle \boldsymbol{v}, \boldsymbol{w} \rangle + \langle \boldsymbol{w}, \boldsymbol{v} \rangle - \langle \boldsymbol{w}, \boldsymbol{w} \rangle). \tag{8.7}$$

Since $\langle\ ,\ \rangle$ *is symmetric* $-\langle \boldsymbol{v}, \boldsymbol{w} \rangle + \langle \boldsymbol{w}, \boldsymbol{v} \rangle = 0$. *Therefore, the expression in (8.7) is equal to*

$$= \frac{1}{4}(\langle \boldsymbol{v}, \boldsymbol{v} \rangle - \langle \boldsymbol{w}, \boldsymbol{w} \rangle). \tag{8.8}$$

Since $\phi(\boldsymbol{v}) = \phi(\boldsymbol{w})$, *the expression in (8.8) is zero and* $\boldsymbol{x} \perp \boldsymbol{y}$ *as claimed.*

Suppose $\phi(\boldsymbol{x}) \neq 0$. *Then* $\rho_{\boldsymbol{x}}(\boldsymbol{v}) = \rho_{\boldsymbol{x}}(\frac{1}{2}(\boldsymbol{x}+\boldsymbol{y})) = \frac{1}{2}(-\boldsymbol{x}+\boldsymbol{y}) = -\boldsymbol{w}$. *Then* $(\rho_{\boldsymbol{w}} \circ \rho_{\boldsymbol{x}})(\boldsymbol{v}) = \boldsymbol{w}$. *Suppose, on the other hand, that* $\phi(\boldsymbol{x}) = 0$ *but* $\phi(\boldsymbol{y}) \neq 0$. *Then* $\rho_{\boldsymbol{y}}(\boldsymbol{v}) = \rho_{\boldsymbol{y}}(\frac{1}{2}(\boldsymbol{x}+\boldsymbol{y})) = \frac{1}{2}(\boldsymbol{x}-\boldsymbol{y}) = \boldsymbol{w}$. *So, if either* $\phi(\boldsymbol{x}) \neq 0$ *or* $\phi(\boldsymbol{y}) \neq 0$, *then we are done.*

Suppose then that $\phi(\boldsymbol{x}) = \phi(\boldsymbol{y}) = 0$. *Then by Lemma (8.17)* $\phi(\boldsymbol{v}) = \phi(\frac{1}{2}(\boldsymbol{x}+\boldsymbol{y})) = \frac{1}{4}(\phi(\boldsymbol{x})+\phi(\boldsymbol{y})) = 0$, *a contradiction.*

We will need a similar result for singular vectors (if they exist). Before proving this we show that if an orthogonal space (V, ϕ) has a singular vector then it must contain a pair $(\boldsymbol{u}, \boldsymbol{v})$ of singular vectors such that $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = 1$.

Lemma 8.24 *Assume (V, ϕ) is a non-degenerate orthogonal space and that $\boldsymbol{u}$ is a singular vector. Then there exists a singular vector $\boldsymbol{v}$ such that $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = 1$.*

Proof *Since V is non-degenerate, there must exist a vector $\boldsymbol{x}$ such that $\langle \boldsymbol{u}, \boldsymbol{x} \rangle = c \neq 0$. If $\boldsymbol{x}$ is singular, set $\boldsymbol{v} = \frac{1}{c}\boldsymbol{x}$.*

We may therefore assume that $\phi(\boldsymbol{x}) \neq 0$. Since $\boldsymbol{u}$ is not orthogonal to $\boldsymbol{x}, \rho_{\boldsymbol{x}}(\boldsymbol{u}) = \boldsymbol{y} \neq \boldsymbol{u}$. Also, Span$(\boldsymbol{u}, \boldsymbol{x})$ = Span$(\boldsymbol{y}, \boldsymbol{w})$ and therefore $\boldsymbol{u}$ is not orthogonal to $\boldsymbol{y}$. Since $\rho_{\boldsymbol{x}}$ is an isometry, $\phi(\boldsymbol{u}) = \phi(\rho_{\boldsymbol{x}}(\boldsymbol{v})) = \phi(\boldsymbol{y})$ and therefore $\boldsymbol{y}$ is a singular vector not orthogonal to $\boldsymbol{v}$. As in the first paragraph, set $c = \langle \boldsymbol{u}, \boldsymbol{y} \rangle$ and $\boldsymbol{v} = \frac{1}{c}\boldsymbol{y}$.

Definition 8.27 *A pair of singular vectors $(\boldsymbol{v}, \boldsymbol{w})$ in an orthogonal space (V, ϕ) such that $\langle \boldsymbol{v}, \boldsymbol{w} \rangle = 1$ is called a* **hyperbolic pair**.

Lemma 8.25 *Assume (V, ϕ) is a non-degenerate orthogonal space and $\boldsymbol{u}, \boldsymbol{v}$ are singular vectors. Then there exists an isometry T of V such that $T(\boldsymbol{u}) = \boldsymbol{v}$.*

Proof *We first show that if $\boldsymbol{u}$ is a singular vector and $c \neq 0$ is a scalar then there is an isometry T of V such that $T(\boldsymbol{u}) = c\boldsymbol{u}$. By Lemma (8.24), there exists a singular vector $\boldsymbol{w}$ such that $\langle \boldsymbol{u}, \boldsymbol{w} \rangle = 1$. Set $U =$ Span$(\boldsymbol{u}, \boldsymbol{w})$. The map $\tau : U \to U$ such that $\tau(\boldsymbol{u}) = c\boldsymbol{u}, \tau(\boldsymbol{w}) = \frac{1}{c}\boldsymbol{w}$ is an isometry of U. The subspace U is non-degenerate. By Lemma (8.23), there is an isometry T of V such that T restricted to U is τ and T restricted to $U^{\perp}$ is the identity on $U^{\perp}$. Then $T(\boldsymbol{u}) = c\boldsymbol{u}$.*

Now assume that $\boldsymbol{u}$ and $\boldsymbol{v}$ are singular vectors and $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = c \neq 0$. Then $U =$ Span$(\boldsymbol{u}, \boldsymbol{v})$ is non-degenerate. The map $\tau : U \to U$ such that $\tau(\boldsymbol{u}) = \boldsymbol{v}$ and $\tau(\boldsymbol{v}) = \boldsymbol{u}$ is an isometry, which can be extended to an isometry T of V such that T restricted to $U^{\perp}$ is the identity on $U^{\perp}$.

Suppose finally that $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = 0$. By Lemma (8.24), there is a singular vector $\boldsymbol{w}$ such that $\langle \boldsymbol{u}, \boldsymbol{w} \rangle \neq 0$. Then, by the previous paragraph, there is an isometry T_1 of V such that $T_1(\boldsymbol{u}) = \boldsymbol{w}$. If also $\langle \boldsymbol{v}, \boldsymbol{w} \rangle \neq 0$ then there will exist an isometry T_2 of V such that $T_2(\boldsymbol{w}) = \boldsymbol{v}$. Then $(T_2 \circ T_1)(\boldsymbol{u}) = \boldsymbol{w}$. Therefore, we may assume that $\langle \boldsymbol{v}, \boldsymbol{w} \rangle = 0$.

By Lemma (8.24), there exists a singular vector $\boldsymbol{x}$ such that $\langle \boldsymbol{v}, \boldsymbol{x} \rangle \neq 0$ and there is an isometry $T_2 : V \to V$ such that $T_2(\boldsymbol{x}) = \boldsymbol{v}$. As in the previous paragraph, if $\langle \boldsymbol{u}, \boldsymbol{x} \rangle \neq 0$, then we are done so we may assume that $\langle \boldsymbol{u}, \boldsymbol{x} \rangle = 0$.

Suppose $\langle \boldsymbol{w}, \boldsymbol{x} \rangle \neq 0$. Then there is an isometry T_3 of V such that $T_3(\boldsymbol{w}) = \boldsymbol{x}$. Then $T = T_2 \circ T_3 \circ T_1$ is an isometry such that $T(\boldsymbol{u}) = \boldsymbol{v}$. Consequently, we may assume that $\langle \boldsymbol{w}, \boldsymbol{x} \rangle = 0$. However, it is then the case that $\boldsymbol{y} = \boldsymbol{w} + \boldsymbol{x}$ is a singular vector and $\langle \boldsymbol{u}, \boldsymbol{y} \rangle = \langle \boldsymbol{u}, \boldsymbol{w} + \boldsymbol{x} \rangle = \langle \boldsymbol{u}, \boldsymbol{w} \rangle \neq 0$ and $\langle \boldsymbol{v}, \boldsymbol{y} \rangle = \langle \boldsymbol{v}, \boldsymbol{w} + \boldsymbol{x} \rangle = \langle \boldsymbol{v}, \boldsymbol{x} \rangle \neq 0$ and we are done by the argument of the third paragraph above.

We need to extend Lemma (8.25), and this is the point of the next lemma.

Lemma 8.26 *Let (V, ϕ) be a non-degenerate orthogonal space and $\boldsymbol{u}, \boldsymbol{v}_1, \boldsymbol{v}_2$ be singular vectors such that $\langle \boldsymbol{u}, \boldsymbol{v}_1\rangle = 1 = \langle \boldsymbol{u}, \boldsymbol{v}_2\rangle$. Then there is an isometry T of V such that $T(\boldsymbol{u}) = \boldsymbol{u}, T(\boldsymbol{v}_1) = \boldsymbol{v}_2$.*

Proof *Suppose first that $\langle \boldsymbol{v}_1, \boldsymbol{v}_2\rangle \neq 0$. Set $\boldsymbol{x} = \boldsymbol{v}_1 - \boldsymbol{v}_2$. Then $\langle \boldsymbol{u}, \boldsymbol{x}\rangle = \langle \boldsymbol{u}, \boldsymbol{v}_1 - \boldsymbol{v}_2\rangle = \langle \boldsymbol{u}, \boldsymbol{v}_1\rangle - \langle \boldsymbol{u}, \boldsymbol{v}_2\rangle = 1 - 1 = 0$. Thus, $\boldsymbol{u} \perp \boldsymbol{x}$. We claim that $\phi(\boldsymbol{x}) \neq 0$:*

$$\phi(\boldsymbol{x}) = \phi(\boldsymbol{v}_1 - \boldsymbol{v}_2) = \phi(\boldsymbol{v}_1) + \phi(\boldsymbol{v}_2) + \langle \boldsymbol{v}_1, -\boldsymbol{v}_2\rangle. \tag{8.9}$$

Since $\boldsymbol{v}_1, \boldsymbol{v}_2$ are singular, $\phi(\boldsymbol{v}_1) = \phi(\boldsymbol{v}_2) = 0$ and so the expression in (8.9) is equal to

$$-\langle \boldsymbol{v}_1, \boldsymbol{v}_2\rangle \neq 0.$$

We point out that $\boldsymbol{y} = \boldsymbol{v}_1 + \boldsymbol{v}_2$ is orthogonal to $\boldsymbol{x}$ and $\boldsymbol{v}_1 = \frac{1}{2}(\boldsymbol{x} + \boldsymbol{y})$. Now $\rho_{\boldsymbol{x}}(\boldsymbol{u}) = \boldsymbol{u}$ since $\boldsymbol{u} \perp \boldsymbol{x}$ and

$$\rho_{\boldsymbol{x}}(\boldsymbol{v}_1) = \rho_{\boldsymbol{x}}\left(\frac{1}{2}(\boldsymbol{x} + \boldsymbol{y})\right) = \frac{1}{2}(-\boldsymbol{x} + \boldsymbol{y}) = \boldsymbol{v}_2.$$

We may therefore assume that $\langle \boldsymbol{v}_1, \boldsymbol{v}_2\rangle = 0$. By the previous paragraph, it suffices to show that there exists a singular vector $\boldsymbol{v}_3$ such that $\langle \boldsymbol{u}, \boldsymbol{v}_3\rangle = 1, \langle \boldsymbol{v}_1, \boldsymbol{v}_3\rangle \neq 0$, and $\langle \boldsymbol{v}_2, \boldsymbol{v}_3\rangle \neq 0$. We remark that the only singular vectors in Span$(\boldsymbol{u}, \boldsymbol{v}_1)$ are in Span$(\boldsymbol{u}) \cup$ Span$(\boldsymbol{v}_1)$ and therefore dim$(V) \geq 3$. $U =$ Span$(\boldsymbol{u}, \boldsymbol{v}_1)$ is non-degenerate and therefore $U^{\perp}$ is non-degenerate. In particular, $U^{\perp}$ contains non-singular vectors. Let $\boldsymbol{z} \in U^{\perp}$ such that $\phi(\boldsymbol{z}) = c \neq 0$ and consider the three-dimensional subspace $W =$ Span$(\boldsymbol{u}, \boldsymbol{v}_1, \boldsymbol{z})$. We claim that for every non-zero scalar a the vector $\boldsymbol{w}_a = -a^2c\boldsymbol{u} + \boldsymbol{v}_1 + a\boldsymbol{z}$ is singular and $\langle \boldsymbol{u}, \boldsymbol{w}_a\rangle = 1$.

Since $(-a^2c\boldsymbol{u} + \boldsymbol{v}_1) \perp a\boldsymbol{z}$ by Lemma (8.17), it follows that

$$\phi(\boldsymbol{w}_a) = \phi(-a^2c\boldsymbol{u} + \boldsymbol{v}_1) + \phi(a\boldsymbol{z}).$$

Since $\phi(\boldsymbol{u}) = \phi(\boldsymbol{v}_1) = 0$, we have

$$\phi(-a^2c\boldsymbol{u} + \boldsymbol{v}_1) + \phi(a\boldsymbol{z}) = \langle -a^2c\boldsymbol{u}, \boldsymbol{v}_1\rangle + \phi(a\boldsymbol{z})$$

$$= -a^2c\langle \boldsymbol{u}, \boldsymbol{v}_1\rangle + a^2\phi(\boldsymbol{z}) = -a^2c + a^2c = 0.$$

Moreover,

$$\langle \boldsymbol{u}, \boldsymbol{w}_a\rangle = \langle \boldsymbol{u}, -a^2c\boldsymbol{u} + \boldsymbol{v}_1 + a\boldsymbol{z}\rangle = \langle \boldsymbol{u}, \boldsymbol{v}_1\rangle = 1.$$

Also note that $\langle \boldsymbol{w}_a, \boldsymbol{v}_1\rangle = -a^2c \neq 0$, and therefore, by what we have shown, for every $a \neq 0$ there is an isometry T_a such that $T_a(\boldsymbol{u}) = \boldsymbol{u}, T_a(\boldsymbol{v}_1) = \boldsymbol{w}_a$.

Next note that W is not contained in $\boldsymbol{v}_2^{\perp}$ since $\boldsymbol{u}$ and $\boldsymbol{v}_2$ are not orthogonal. It then follows that dim$(W \cap \boldsymbol{v}_2^{\perp}) = 2$. There are at most two one-dimensional subspaces spanned by singular vectors in $W \cap \boldsymbol{v}_2^{\perp}$, one of which is Span$(\boldsymbol{v}_2)$. Since we are assuming that the field $\mathbb{F}$ does not have characteristic two, in particular, $\mathbb{F} \neq \mathbb{F}_2$. Therefore, there are at least two distinct one-dimensional spaces Span$(\boldsymbol{w}_a)$, and consequently, there is a scalar a such that $\langle \boldsymbol{w}_a, \boldsymbol{v}_2\rangle \neq 0$. Set $\boldsymbol{v}_3 = \boldsymbol{w}_a$ for this choice of a. By the first paragraph, there are isometries T_1, T_2 such that $T_1(\boldsymbol{u}) = T_2(\boldsymbol{u}) = \boldsymbol{u}, T_1(\boldsymbol{v}_1) = \boldsymbol{v}_3, T_2(\boldsymbol{v}_3) = \boldsymbol{v}_2$. Then $T = (T_2 \circ T_1)$ is an isometry satisfying $T(\boldsymbol{u}) = \boldsymbol{u}$ and $T(\boldsymbol{v}_1) = \boldsymbol{v}_2$.

As a corollary, we have the following result about pairs $(\boldsymbol{u}_1, \boldsymbol{v}_1), (\boldsymbol{u}_2, \boldsymbol{v}_2)$ of singular vectors such that $\langle \boldsymbol{u}_1, \boldsymbol{v}_1\rangle = \langle \boldsymbol{u}_2, \boldsymbol{v}_2\rangle = 1$. We leave the proof as an exercise.

Corollary 8.5 *Let (V, ϕ) be a non-degenerate orthogonal space. Assume $\boldsymbol{u}_1$, $\boldsymbol{u}_2$, $\boldsymbol{v}_1$, $\boldsymbol{v}_2$ are singular vectors and $\langle \boldsymbol{u}_1, \boldsymbol{v}_1\rangle = \langle \boldsymbol{u}_2, \boldsymbol{v}_2\rangle = 1$. Then there exists an isometry T of V such that $T(\boldsymbol{u}_1) = \boldsymbol{u}_2$ and $T(\boldsymbol{v}_1) = \boldsymbol{v}_2$.*

We need a couple more preparatory lemmas before we can prove our main result:

Lemma 8.27 *Assume (V, ϕ) is a non-degenerate orthogonal space over a field $\mathbb{F}$ of characteristic not two and that U is a totally singular subspace of dimension k. Then there exists a non-degenerate subspace W of dimension $2k$ containing U.*

Proof *We do induction on k. If $k = 1$, the result follows from Lemma (8.24). Assume the result has been proved for all totally singular subspaces of dimension k and U is a totally singular subspace of dimension $k+1$. Let $\boldsymbol{u} \in U$ be a non-zero vector. By Lemma (8.24) there exists a singular vector $\boldsymbol{v}$ such that $\langle \boldsymbol{u}, \boldsymbol{v}\rangle = 1$. Set $X =$ Span$(\boldsymbol{u}, \boldsymbol{v})$. Then X is a non-degenerate subspace of dimension 2. Then $X^{\perp}$ is a non-degenerate subspace of V. Set $Y = U \cap \boldsymbol{v}^{\perp}$. Then Y is a totally singular subspace of dimension k contained in $X^{\perp}$. By the inductive hypothesis there exists a non-degenerate subspace Z of $X^{\perp}$ containing Y with dim$(Z) = 2k$. The spaces X and Z are mutually orthogonal. Since each is non-degenerate it follows that $X + Z = X \oplus Z$ is non-degenerate. Set $W = X \oplus Z$. Then $U \subset W$, W is non-degenerate, and dim$(W) = 2k + 2 = 2(k+1)$.*

Lemma 8.28 *Assume (V, ϕ) is a non-degenerate orthogonal space over a field $\mathbb{F}$ of characteristic not two. Assume $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$ is a linearly independent sequence of singular vectors such that for all i, j $\boldsymbol{u}_i \perp \boldsymbol{u}_j$. Then there are singular vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$ such that $\langle \boldsymbol{u}_i, \boldsymbol{v}_j \rangle = 0$ if $i \neq j$ and 1 if $i = j$.*

Proof *By Lemma (8.27), we may assume dim$(V) = 2k$. We proceed by induction on k. When $k = 1$, the result is a consequence of Lemma (8.24). Assume that the result is true for k and that dim$(U) = k + 1$, dim$(V) = 2k + 2$. Set $W =$ Span$(\boldsymbol{u}_2, \ldots, \boldsymbol{u}_{k+1})$. Then W is a totally singular subspace of dimension k. It then follows that dim$(W^\perp) = k + 2$. Since Rad$(W^\perp) = W$, in particular, $\boldsymbol{u}_1$ is not in Rad$(W^\perp)$. Let $\boldsymbol{x} \in W^\perp$ be chosen so that $\langle \boldsymbol{u}_1, \boldsymbol{x} \rangle \neq 0$. Then Span$(\boldsymbol{u}_1, \boldsymbol{x})$ is non-degenerate and contained in $W^\perp$. As in the proof of Lemma (8.24), there exists a singular vector $\boldsymbol{v}_1 \in$ Span$(\boldsymbol{u}_1, \boldsymbol{x})$ such that $\langle \boldsymbol{u}_1, \boldsymbol{v}_1 \rangle = 1$. Now set $U_1 =$ Span$(\boldsymbol{u}_1, \boldsymbol{v}_1)$. $U_1^\perp$ has dimension $2k$ and $W =$ Span$(\boldsymbol{u}_2, \ldots, \boldsymbol{u}_{k+1}) \subset U_1^\perp$. We can invoke the inductive hypothesis and conclude that there are singular vectors $\boldsymbol{v}_2, \ldots, \boldsymbol{v}_{k+1}$ in $U_1^\perp$ such that $\langle \boldsymbol{u}_i, \boldsymbol{v}_j \rangle = 0$ if $2 \leq i, j \leq k+1$ and $i \neq j$ and is 1 if $i = j$. Since $\boldsymbol{u}_i, \boldsymbol{v}_i \perp \boldsymbol{u}_1, \boldsymbol{v}_1$ for $2 \leq i \leq k + 1$, $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{k+1})$ is the sequence of desired vectors.*

We now have everything necessary to prove *Witt's Theorem for non-degenerate finite-dimensional orthogonal spaces over fields of characteristic not two.*

Theorem 8.12 *Let (V, ϕ) be a non-degenerate finite-dimensional orthogonal space over a field $\mathbb{F}$ with characteristic not two. Assume U_1, U_2 are subspaces of V and that $\tau : U_1 \to U_2$ is an isometry. Then there exists an isometry T of V such that T restricted to U_1 is τ.*

Proof *The proof is by the second principle of induction on $n =$ dim(V). If $n = 1$, there is nothing to prove. So assume the result is true for non-degenerate orthogonal spaces of dimension less than n and dim$(V) = n$.*

Assume first that there exists a non-singular vector $\boldsymbol{x}$ in U_1. Set $\boldsymbol{y} = \tau(\boldsymbol{x})$. Then $\phi(\boldsymbol{y}) = \phi(\boldsymbol{x})$, so by Lemma (8.11) there is an isometry T_1 of V such that $T_1(\boldsymbol{x}) = \boldsymbol{y}$. Set $U_3 = T_1^{-1}(U_2)$ and $\sigma = T_1^{-1} \circ \tau$. Suppose we can find an isometry S of V such that S restricted to U_1 is σ. Then set $T = T_1 \circ S$, an isometry. Moreover, for $\boldsymbol{u} \in U_1$ we have

$$\begin{aligned} T(\boldsymbol{u}) &= (T_1 \circ S)(\boldsymbol{u}) \\ &= T_1(S(\boldsymbol{u})) \\ &= T_1(\sigma(\boldsymbol{u})) \\ &= T_1(T_1^{-1} \circ \tau)(\boldsymbol{u}) \\ &= (T_1 \circ T_1^{-1})(\tau(\boldsymbol{u})) \\ &= \tau(\boldsymbol{u}), \end{aligned}$$

and so T will be the required isometry.

Note that $\sigma(\boldsymbol{x}) = \boldsymbol{x}$. Set $V' = \boldsymbol{x}^\perp, U_1' = U_1 \cap \boldsymbol{x}^\perp$, $U_3' = U_3 \cap \boldsymbol{x}^\perp$, and σ' the restriction of σ to U_1'. V' is a non-degenerate orthogonal space of dimension $n-1 < n$ and σ' is an isometry of U_1' to U_3'. By the inductive hypothesis, there is a isometry S' of V' such that S' restricted to U_1 is σ'. Extend S' to an isometry of V by defining $S(\boldsymbol{x}) = \boldsymbol{x}$. S is the desired isometry.

We may therefore assume that U_1 is totally singular. Let $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$ be a basis for U_1 and set $\boldsymbol{w}_i = \tau(\boldsymbol{u}_i), 1 \le i \le k$. Then $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k)$ is a basis for U_2. We remark that since τ is an isometry, the vectors $\boldsymbol{w}_i$ are singular and mutually orthogonal.

As a consequence of Lemma (8.28), there is a singular vector $\boldsymbol{v}_1$ such that $\langle \boldsymbol{u}_1, \boldsymbol{v}_1\rangle = 1, \langle \boldsymbol{u}_i, \boldsymbol{v}_1\rangle = 0$ for $2 \le i \le k$. Likewise, there is a vector $\boldsymbol{x}_1$ such that $\langle \boldsymbol{w}_1, \boldsymbol{x}_1\rangle = 1, \langle \boldsymbol{w}_i, \boldsymbol{x}_1\rangle = 0$ for $2 \le i \le k$. By Lemma (8.5), there is an isometry T_1 of V such that $T_1(\boldsymbol{u}_1) = \boldsymbol{w}_1, T_1(\boldsymbol{v}_1) = \boldsymbol{x}_1$. Set $U_3 = T_1^{-1}(U_2)$ and $\sigma = T_1^{-1} \circ \tau$, which is an isometry from U_1 to U_3. Note that $\sigma(\boldsymbol{u}_1) = \boldsymbol{u}_1$ and $\sigma(\boldsymbol{v}_1) = \boldsymbol{v}_1$ and so $W = Span(\boldsymbol{u}_1, \boldsymbol{v}_1)$ is contained in $U_1 \cap U_3$. If we can find an isometry S of V such that S restricted to U_1 is σ, then we can proceed as in the previous case and define $T = T_1 \circ S$, and this will fulfill the requirements of the theorem.

Set $X = W^\perp$ so that X is non-degenerate of dimension $n-2$. Let $Y_1 = U_1 \cap W^\perp, Y_3 = U_3 \cap W^\perp$, and γ be the restriction of σ to Y_1. Then γ is an isometry of Y_1 to Y_3, subspaces of the non-degenerate space X of dimension $n-2$. By the inductive hypothesis, there is an isometry R of C such that R restricted to Y_1 is γ. Extend R a linear map S on V by defining $S(\boldsymbol{u}_1) = \boldsymbol{u}_1, S(\boldsymbol{v}_1) = \boldsymbol{v}_1$. Then S is an isometry and S restricted to U_1 is σ. This completes the proof.

Definition 8.28 *Let (V, ϕ) be a non-degenerate finite-dimensional orthogonal space over a field $\mathbb{F}$ of characteristic not two. A totally singular subspace U is said to be* **maximal** *if it is not properly contained in a totally singular subspace.*

As we shall see momentarily, any two maximal totally singular subspaces must have the same dimension, in fact, there must be an isometry taking one to the other. This is the subject of the following result.

Theorem 8.13 *Let (V, ϕ) be a non-degenerate finite-dimensional orthogonal space over a field $\mathbb{F}$ of characteristic not two. Let U and W be two maximal totally singular subspaces. Then there exists an isometry τ of V such that $\tau(U) = W$. In particular, $dim(U) = dim(W)$.*

This is left as an exercise.

Definition 8.29 *Let (V, ϕ) be a non-degenerate finite-dimensional orthogonal space over a field $\mathbb{F}$ of characteristic not two and U be a maximal totally singular subspace. Then $dim(W)$ is referred to as the* **Witt index**.

Exercises

1. Prove Lemma (8.18).

2. Let (V, ϕ) be a finite-dimensional orthogonal space with associated form $\langle\ ,\ \rangle, \mathcal{B}$ a basis of V, and let A be the matrix of $\langle\ ,\ \rangle_\phi$ with respect to $\mathcal{B}$. Prove that the rank of the matrix A is the rank of the space (V, ϕ).

3. Let (V, ϕ) be a finite-dimensional orthogonal space. Assume $\phi(\boldsymbol{x}) \neq 0$. i) Prove that $\rho_{\boldsymbol{x}}(\boldsymbol{x}) = -\boldsymbol{x}$. ii) Assume $\boldsymbol{y} \perp \boldsymbol{x}$. Prove $\rho_{\boldsymbol{x}}(\boldsymbol{y}) = \boldsymbol{y}$.

4. Let $\mathbb{F}$ be a field and ∞ a symbol, which does not represent an element of $\mathbb{F}$ and set $\widehat{\mathbb{F}} = \mathbb{F} \cup \{\infty\}$. Assume that (V, ϕ) is a non-degenerate three-dimensional orthogonal space and contains singular vectors. Set $\mathbb{P}(V) = \{Span(\boldsymbol{v}) | \boldsymbol{v} \neq \boldsymbol{0}, \phi(\boldsymbol{v}) = 0\}$. Prove that there is a one-to-one correspondence between $\mathbb{P}(V)$ and $\widehat{\mathbb{F}}$.

5. Prove Corollary (8.5).

6. Let (V, ϕ) be a non-degenerate finite-dimensional orthogonal space over a field $\mathbb{F}$ of characteristic not two. Prove that all maximal totally singular subspaces have the same dimension.

7. Let (V, ϕ) be a non-degenerate finite-dimensional orthogonal space over a field $\mathbb{F}$ of characteristic not two and T an isometry. Prove that T is a product of reflections.

8. Let (V, ϕ) be a non-degenerate finite-dimensional orthogonal space over a field $\mathbb{F}$ and $T : V \to V$ an isometry. Prove that $det(T) = \pm 1$.

9. Let (V, ϕ) be a non-degenerate finite-dimensional orthogonal space with index at least two. Assume $\boldsymbol{u}, \boldsymbol{v}$ are singular vectors with $\boldsymbol{u} \perp \boldsymbol{v}$. Define a map $T_{(\boldsymbol{u},\boldsymbol{v})}$ as follows:

$$T_{(\boldsymbol{u},\boldsymbol{v})}(\boldsymbol{z}) = \boldsymbol{z} + \langle \boldsymbol{z}, \boldsymbol{v} \rangle \boldsymbol{u} - \langle \boldsymbol{z}, \boldsymbol{u} \rangle \boldsymbol{v}.$$

a) Prove that $T_{(\boldsymbol{u},\boldsymbol{v})}$ is an isometry of V.

b) Prove that $T_{(\boldsymbol{u},\boldsymbol{v})}$ restricted to $Span(\boldsymbol{u}, \boldsymbol{v})^\perp$ is the identity.

c) Prove that $Range(T_{(\boldsymbol{u},\boldsymbol{v})} - I_V) = Span(\boldsymbol{u}, \boldsymbol{v})$.

10. Let $l = Span(\boldsymbol{u}, \boldsymbol{v})$, where $\boldsymbol{u}, \boldsymbol{v}$ are independent singular vectors and $\boldsymbol{u} \perp \boldsymbol{v}$. Set $\chi(l) = \{T_{(\boldsymbol{u},c\boldsymbol{v})} | c \in \mathbb{F} \setminus \{0\}\} \cup \{I_V\}$.

a) Prove that $T_{(\boldsymbol{u},c\boldsymbol{v})} \circ T_{(\boldsymbol{u},-c\boldsymbol{v})} = I_V$.

b) Assume $d \neq -c$. Prove that $T_{(\boldsymbol{u},c\boldsymbol{v})} \circ T_{(\boldsymbol{u},d\boldsymbol{v})} = T_{(\boldsymbol{u},(c+d)\boldsymbol{v})}$.

11. Assume $\boldsymbol{x} = a\boldsymbol{u} + b\boldsymbol{v}, \boldsymbol{y} = c\boldsymbol{u} + d\boldsymbol{v}$ is a basis for $l = Span(\boldsymbol{u}, \boldsymbol{v})$. Prove that $T_{(\boldsymbol{x},\boldsymbol{y})} = T_{(\boldsymbol{u},(ad-bc)\boldsymbol{v})}$.

12. Assume that $\boldsymbol{v} \perp \boldsymbol{u} \perp \boldsymbol{w}$ and $\langle \boldsymbol{v}, \boldsymbol{w} \rangle = 1$. Set $l = Span(\boldsymbol{u}, \boldsymbol{v})$. Prove for every $c \in \mathbb{F}$ there is a unique $T \in \chi(l)$ such that $T(\boldsymbol{w}) = c\boldsymbol{u} + \boldsymbol{w}$.

13. Let (V, ϕ) be a non-degenerate finite-dimensional orthogonal space with positive Witt index. Assume $\boldsymbol{u}, \boldsymbol{v}$ are orthogonal vectors with $\boldsymbol{u}$ singular. For $\boldsymbol{x} \in \boldsymbol{u}^\perp$, define $\delta_{\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{x}) = \boldsymbol{x} + \langle \boldsymbol{x}, \boldsymbol{v} \rangle_\phi \boldsymbol{u}$. Prove that $\delta_{\boldsymbol{u},\boldsymbol{v}}$ is an isometry of $\boldsymbol{u}^\perp$.

14. By Witt's extension theorem the isometry $\delta_{\boldsymbol{u},\boldsymbol{v}}$ is induced by an isometry of D of (V, ϕ). Let $\boldsymbol{w}$ be a singular vector in $\boldsymbol{v}^\perp$ such that $\langle \boldsymbol{u}, \boldsymbol{w} \rangle_\phi = 1$. Prove that $D(\boldsymbol{w}) = \boldsymbol{w} - \boldsymbol{v} - \phi(\boldsymbol{v})\boldsymbol{u}$. In particular, D is unique.

Let $T_{\boldsymbol{u},\boldsymbol{v}}$ denote the unique extension of $\delta_{\boldsymbol{u},\boldsymbol{v}}$ to V.

15. If $\boldsymbol{v}, \boldsymbol{w} \in \boldsymbol{u}^\perp$, prove that $D_{\boldsymbol{u},\boldsymbol{v}} D_{\boldsymbol{u},\boldsymbol{w}} = D_{\boldsymbol{u},\boldsymbol{v}+\boldsymbol{w}}$.

16. Assume $\mathbb{F}$ is a field in which every element has a square root (this is true of $\mathbb{C}$). Prove that the isometry class of an n-dimensional orthogonal space (V, ϕ) defined over $\mathbb{F}$ is determined by the rank of (V, ϕ).

17. Let (V, ϕ) be a real orthogonal space. Let $\mathcal{P}$ be the collection of all subspaces of V such that $\phi(\boldsymbol{u}) > 0$ for all $\boldsymbol{u} \in U, \boldsymbol{u} \neq \boldsymbol{0}$. Let M_1, M_2 be maximal elements of $\mathcal{P}$. Prove that there is an isometry S of (V, ϕ) such that $S(M_1) = M_2$.

18. Let (V, ϕ) be a non-degenerate three dimensional orthogonal over a finite field $\mathbb{F}_q$ where q is odd (not characteristic two). Prove that (V, ϕ) is singular.

19. Let (V, ϕ) be a non-degenerate n dimensional orthogonal over a finite field $\mathbb{F}_q$ where q is odd (not characteristic two). Prove that the Witt index is at least $\lfloor \frac{n-1}{2} \rfloor$.

In Exercises 20–22 let (V, ϕ) be a non-degenerate $2m$-dimensional orthogonal over a finite field $\mathbb{F}_q$ where q is odd (not characteristic two) with Witt index m.

20. Use induction on m to prove that the number of singular vectors is $(q^m - 1)(q^{m-1} + 1)$.

21. Assume $\boldsymbol{u}$ is a singular vector. Prove that the number of singular vectors $\boldsymbol{v}$ such that $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = 1$ is q^{2m-2}.

22. Prove that the number of bases $(\boldsymbol{u}_1, \boldsymbol{v}_1, \boldsymbol{u}_2, \boldsymbol{v}_2, \dots, \boldsymbol{u}_m, \boldsymbol{v}_m)$ such that each $\boldsymbol{u}_i, \boldsymbol{v}_i$ is singular and further satisfy $\boldsymbol{u}_i \perp \boldsymbol{u}_j, \boldsymbol{v}_i \perp \boldsymbol{v}_j, \boldsymbol{u}_i \perp \boldsymbol{v}_j$ for $i \neq j$ and $\langle \boldsymbol{u}_i, \boldsymbol{v}_i \rangle = 1$ is $2q^{2\binom{m}{2}}(q^m - 1)\Pi_{i=1}^{m-1}(q^{2i} - 1)$. Then prove that this is the order of $O(V, \phi)$.

23. Let (V, ϕ) be a non-degenerate $2m$-dimensional orthogonal space with Witt index $m - 1$ over the finite field $\mathbb{F}_q$ where q is odd. Prove that the order of $O(V, \phi)$ is $2q^{2\binom{m}{2}}(q^m + 1)\Pi_{i=1}^{m-1}(q^{2i} - 1)$.

8.4 Orthogonal Space, Characteristic Two

In this section we assume that the characteristic of $\mathbb{F}$ is two and that V is a finite-dimensional vector space over $\mathbb{F}$ and $\phi : V \to \mathbb{F}$ is a quadratic form with associated symmetric form $\langle\ ,\ \rangle$. We will assume that the field $\mathbb{F}$ is **perfect** which we define below. Then we will assume that (V, ϕ) is non-singular. The main result of this section is Witt's extension theorem.

What You Need to Know

To understand the material of this section, you must have already mastered the following concepts: vector space, basis of a vector space, dimension of a vector space, finite-dimensional vector space, linear transformation, coordinate vector with respect to a basis, matrix of a linear transformation, and quadratic form, You should also be familiar with the concept of a group, which can be found in Appendix B.

Definition 8.30 *A field $\mathbb{F}$ of characteristic two is said to be* **perfect** *if every element a of $\mathbb{F}$ has a square root in $\mathbb{F}$, that is, there exists $b \in \mathbb{F}$ such that $b^2 = a$.*

Example 8.12 *A finite field of characteristic two is perfect. Also, any algebraic extension of a finite field of characteristic two is perfect. On the other hand, the field $\mathbb{F}_2(t)$ of all rational expressions $\frac{F(t)}{G(t)}$ where $F(t), G(t) \in \mathbb{F}_2[t]$ is not perfect. In particular, t does not have a square root.*

We recall the definition of a non-singular quadratic form:

Definition(8.22) *A finite-dimensional orthogonal space (V, ϕ) with associated symmetric form $\langle\ ,\ \rangle$ over a perfect field of characteristic two is* **non-singular** *if either $(V, \langle\ ,\ \rangle_\phi$ is non-degenerate or for every non-zero vector $\boldsymbol{v}$ in the radical of $\langle\ ,\ \rangle$ we have $\phi(\boldsymbol{v}) \neq 0$.*

Example 8.13 *Let $q = 2^m$ for a natural number m and set $V = \mathbb{F}_q^3$. For $\boldsymbol{v} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ let $\phi(\boldsymbol{v}) = x_1x_2 + x_3^2$. Then (V, ϕ) is degenerate since $\boldsymbol{x} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ is in the radical of the associated symmetric form and $\phi(\boldsymbol{x}) = 1$.However, $\phi(\boldsymbol{x}) = 1$, therefore ϕ is non-singular.*

In our next result we prove that a degenerate, non-singular orthogonal space (over a perfect field of characteristic two) has a radical of dimension one.

Theorem 8.14 *Assume $\mathbb{F}$ is a perfect field of characteristic two, (V, ϕ) is a finite-dimensional non-singular orthogonal space with associated form $\langle\ ,\ \rangle$. Then the radical of $\langle\ ,\ \rangle$ has dimension of at most one.*

Proof *We can assume that $\langle\ ,\ \rangle$ is degenerate and prove its radical has dimension one. Suppose to the contrary that $(\boldsymbol{x}, \boldsymbol{y})$ is a linearly independent sequence contained in the radical. Since $\boldsymbol{x}, \boldsymbol{y}$ are in the radical then for every $\boldsymbol{v} \in V, \langle \boldsymbol{x}, \boldsymbol{v}\rangle = \langle \boldsymbol{v}, \boldsymbol{y}\rangle = 0$. In particular, $\langle \boldsymbol{x}, \boldsymbol{y}\rangle = 0$. Now set $a = \phi(\boldsymbol{x})$ and $b = \phi(\boldsymbol{y})$. Let c be a square root of $\frac{1}{a}$ and d a square root of $\frac{1}{b}$ and set $\boldsymbol{z} = c\boldsymbol{x} + d\boldsymbol{y}$. Then $\boldsymbol{z}$, as a linear combination of $\boldsymbol{x}$ and $\boldsymbol{y}$, belongs to the radical. However, $\phi(\boldsymbol{z}) = \phi(c\boldsymbol{x} + d\boldsymbol{y}) = c^2\phi(\boldsymbol{x}) + cd\langle \boldsymbol{x}, \boldsymbol{y}\rangle + d^2\phi(\boldsymbol{y}) = 1 + 1 = 0$ so that $\boldsymbol{z}$ is a singular vector, a contradiction.*

For the remainder of this section, assume that $\mathbb{F}$ is a perfect field of characteristic two, (V, ϕ) is a finite-dimensional non-singular orthogonal space with associated form $\langle\ ,\ \rangle$.

Lemma 8.29 *Assume that $\boldsymbol{v} \in V$ is a singular vector. Then there exists a singular vector $\boldsymbol{w}$ such that $\langle \boldsymbol{v}, \boldsymbol{w}\rangle = 1$.*

Proof *Since $\boldsymbol{v}$ is not in the radical, there exists a vector $\boldsymbol{x}$ such that $\langle \boldsymbol{v}, \boldsymbol{x}\rangle = a \neq 0$. By replacing $\boldsymbol{x}$ by $\frac{1}{a}\boldsymbol{x}$ we can assume that $\langle \boldsymbol{v}, \boldsymbol{x}\rangle = 1$. Set $\phi(\boldsymbol{x}) = b$. If $b = 0$ then $(\boldsymbol{v}, \boldsymbol{x})$ is a hyperbolic pair and we are done. Otherwise, set $\boldsymbol{w} = b\boldsymbol{v} + \boldsymbol{x}$. Then $\langle \boldsymbol{v}, \boldsymbol{w}\rangle = \langle \boldsymbol{v}, b\boldsymbol{v} + \boldsymbol{x}\rangle = a\langle \boldsymbol{v}, \boldsymbol{v}\rangle + \langle \boldsymbol{v}, \boldsymbol{x}\rangle = 1$. Also, $\phi(\boldsymbol{w}) = \phi(b\boldsymbol{v} + \boldsymbol{x}) = b^2\phi(\boldsymbol{v}) + b\langle \boldsymbol{v}, \boldsymbol{x}\rangle + \phi(\boldsymbol{x}) = b + b = 0$. Thus, $(\boldsymbol{v}, \boldsymbol{w})$ is a hyperbolic pair.*

Corollary 8.6 *Assume (V, ϕ) is two-dimensional, non-singular, and contains singular vectors. Then (V, ϕ) is non-degenerate.*

We leave this as an exercise.

Lemma 8.30 *Assume (V, ϕ) is non-singular of dimensional $n \geq 2$ and every non-zero vector is non-singular. Then $n = 2$ and (V, ϕ) is non-degenerate. Moreover, if $(\boldsymbol{v}, \boldsymbol{w})$ is a basis of V such that $\langle \boldsymbol{v}, \boldsymbol{w}\rangle = 1$, then the quadratic polynomial $x^2 + x + \phi(\boldsymbol{w})$ is irreducible in $\mathbb{F}[x]$.*

Proof *Let $\boldsymbol{v}$ be any non-zero vector not contained in the radical. Set $a = \phi(\boldsymbol{v})$ and let $b \in \mathbb{F}$ such that $b^2 = a$. Replacing $\boldsymbol{v}$ by $\frac{1}{b}\boldsymbol{v}$, if necessary, we can assume that $\phi(\boldsymbol{v}) = 1$. Next choose $\boldsymbol{w}$ a vector in $V \setminus \boldsymbol{v}^{\perp}$. If $\langle \boldsymbol{v}, \boldsymbol{w} \rangle = c$, by replacing $\boldsymbol{w}$ by $\frac{1}{c}\boldsymbol{w}$, if necessary, we may assume that $\langle \boldsymbol{v}, \boldsymbol{w} \rangle = 1$. The two-dimensional subspace Span$(\boldsymbol{v}, \boldsymbol{w})$ is non-degenerate. The orthogonal complement to Span$(\boldsymbol{v}, \boldsymbol{w})$ has dimension $n - 2$, so if $n > 2$, there are non-zero vectors $\boldsymbol{z} \in$ Span$(\boldsymbol{v}, \boldsymbol{w})^{\perp}$. Replacing $\boldsymbol{z}$ by a multiple, if necessary, we can assume that $\phi(\boldsymbol{z}) = 1$. However, the vector $\boldsymbol{x} = \boldsymbol{v} + \boldsymbol{z} \neq \boldsymbol{0}$ and $\phi(\boldsymbol{x}) = 0$, a contradiction. Thus, $n = 2$ and (V, ϕ) is non-degenerate.*

Let $\alpha \in \mathbb{F}$ and set $\boldsymbol{z} = \alpha\boldsymbol{v} + \boldsymbol{w}$. Then $\boldsymbol{z}$ is non-zero and consequently, $\phi(\boldsymbol{z}) \neq 0$. Thus, for no choice of $\alpha \in \mathbb{F}$ is $\phi(\boldsymbol{z}) = \alpha^2 + \alpha + \phi(\boldsymbol{w}) = 0$. Consequently, the polynomial $x^2 + x + \phi(\boldsymbol{w})$ is irreducible in $\mathbb{F}[x]$.

An immediate consequence of the proof of Lemma (8.30) is:

Corollary 8.7 *Assume (V, ϕ) has dimension at least three. Then V contains non-zero singular vectors.*

Corollary 8.8 *Assume $n = dim(V)$ is odd. Then (V, ϕ) is degenerate.*

Proof *The proof is by induction on k where $n = 2k - 1$. If $k = 1$ there is nothing to prove. Assume now that the result is true for $k \geq 1$ and that the dimension of V is $2k + 1 \geq 3$. By Corollary (8.7) there exists a non-zero singular vector $\boldsymbol{v}$ in V and then by Lemma (8.29) there exists a non-zero singular vector $\boldsymbol{w}$ such that $\langle \boldsymbol{v}, \boldsymbol{w} \rangle = 1$. Then Span$(\boldsymbol{v}, \boldsymbol{w})$ is non-degenerate. The dimension of Span$(\boldsymbol{v}, \boldsymbol{w})^{\perp}$ is $2k - 1$ and by the inductive hypothesis the radical of Span$(\boldsymbol{v}, \boldsymbol{w})^{\perp}$ is non-trivial and this is contained in the radical of V.*

We can now classify the finite-dimensional, non-singular orthogonal spaces over a perfect field of characteristic two:

Theorem 8.15 *Assume (V, ϕ) is a finite-dimensional orthogonal space over a perfect field of characteristic two. Then one and only one of the following occurs:*

1a) $n = 2m$ and there is a basis $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_m)$ such that

$$\phi\left(\sum_{i=1}^{m}(a_i\boldsymbol{x}_i + b_i\boldsymbol{y}_i)\right) = \sum_{i=1}^{m} a_i b_i.$$

1b) $n = 2m$ and there is a basis $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{m-1}, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_{m-1}, \boldsymbol{v}, \boldsymbol{w})$ such that

$$\phi\left(\sum_{i=1}^{m-1}(a_i\boldsymbol{x}_i+b_i\boldsymbol{y}_i)+c\boldsymbol{v}+d\boldsymbol{w})\right)=\sum_{i=1}^{m-1}a_ib_i+c^2+cd+d^2\gamma$$

where the polynomial $x^2+x+\gamma$ is irreducible in $\mathbb{F}[x]$.

2) $n=2m+1$ and there is a basis $(\boldsymbol{x}_1,\dots,\boldsymbol{x}_m,\boldsymbol{y}_1,\dots,\boldsymbol{y}_m,\boldsymbol{z})$ such that

$$\phi\left(\sum_{i=1}^{m}(a_i\boldsymbol{x}_i+b_i\boldsymbol{y}_i)+c\boldsymbol{z}\right)=\sum_{i=1}^{m}a_ib_i+c^2.$$

Proof *Suppose first that $n=2m$ is even. The proof is by induction on m. If $m=1$ then the result follows from Lemma (8.29) if there are singular vectors in V and from Lemma (8.30) if there are no singular vectors in V.*

Now assume the result is true for spaces of dimension $2m$ with $m\geq 1$ and that $dim(V)=2(m+1)$. By the proof of Corollary (8.8) it follows that there exists a hyperbolic pair of vectors $(\boldsymbol{x},\boldsymbol{y})$. Set $U=Span(\boldsymbol{x},\boldsymbol{y})$, a non-degenerate subspace of dimension 2. Then $U^\perp$ is non-degenerate of dimension $2m$ and the inductive hypothesis applies. Suppose there is a basis $(\boldsymbol{x}_1,\dots,\boldsymbol{x}_m,\boldsymbol{y}_1,\dots,\boldsymbol{y}_m)$ for $U^\perp$ such that

$$\phi\left(\sum_{i=1}^{m}(a_i\boldsymbol{x}_i+b_i\boldsymbol{y}_i)\right)=\sum_{i=1}^{m}a_ib_i.$$

Set $\boldsymbol{x}_{m+1}=\boldsymbol{x},\boldsymbol{y}_{m+1}=\boldsymbol{y}$. Then 1a) holds.

On the other hand, suppose there is a basis $(\boldsymbol{x}_1,\dots,\boldsymbol{x}_{m-1},\boldsymbol{y}_1,\dots,\boldsymbol{y}_{m-1},\boldsymbol{v},\boldsymbol{w})$ for $U^\perp$ such that

$$\phi\left(\sum_{i=1}^{m-1}(a_i\boldsymbol{x}_i+b_i\boldsymbol{y}_i)+c\boldsymbol{v}+d\boldsymbol{w})\right)=\sum_{i=1}^{m-1}a_ib_i+c^2+cd+d^2\gamma,$$

where the polynomial $x^2+x+\gamma$ is irreducible in $\mathbb{F}[x]$. Set $\boldsymbol{x}_m=\boldsymbol{x}$ and $\boldsymbol{y}_m=\boldsymbol{y}$. Then 1b) holds.

So we may assume that $n=2m+1$ is odd. The proof is by induction on m. If $m=1$, then the result follows from the proof of Corollary (8.8). Assume now that the result is true for spaces of dimension $2m+1$ where $m\geq 1$ and that $dim(V)=2(m+1)+1=2m+3$. It follows from Corollary (8.7) and Lemma (8.29) that there exists a hyperbolic pair $(\boldsymbol{x},\boldsymbol{y})$ in V. Set $U=Span(\boldsymbol{x},\boldsymbol{y})$, a non-degenerate subspace of dimension 2. The orthogonal complement, $U^\perp$, to

U is non-singular of dimension $2m+1$ and therefore the inductive hypothesis applies: there is a basis $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_m, \boldsymbol{z})$ such that

$$\phi\left(\sum_{i=1}^{m}(a_i\boldsymbol{x}_i + b_i\boldsymbol{y}_i) + c\boldsymbol{z}\right) = \sum_{i=1}^{m} a_ib_i + c^2.$$

Set $\boldsymbol{x}_{m+1} = \boldsymbol{x}, \boldsymbol{y}_{m+1} = \boldsymbol{y}$. Now 2) holds.

We now come to Witt's Extension Theorem for finite-dimensional orthogonal spaces over a perfect field of characteristic two:

Theorem 8.16 *Let (V, ϕ) be a non-degenerate finite-dimensional orthogonal space over the perfect field $\mathbb{F}$ of characteristic two, with associated symmetric form $\langle\ ,\ \rangle$. Assume X and Y are subspaces of V and $\sigma : X \to Y$ is an isometry. Then there exists an isometry S of (V, ϕ) such that $S_{|X} = \sigma$.*

Proof *Case 1) First assume $X \cap Y$ is a hyperplane of X (and therefore Y) and that σ restricted to $U = X \cap Y$ is the identity. Set $W = \{\sigma(\boldsymbol{x}) + \boldsymbol{x} | \boldsymbol{x} \in X\}$ so that dim$(W) = 1$ and let $\boldsymbol{x}$ be chosen from X such that $\boldsymbol{w} = \sigma(\boldsymbol{x}) + \boldsymbol{x}$ spans W. We also set $\boldsymbol{y} = \sigma(\boldsymbol{x})$. We treat separately the two subcases: a) X is not contained in $\boldsymbol{w}^\perp$ and b) $X \subset \boldsymbol{w}^\perp$.*

a) Suppose $\boldsymbol{u} \in U$. We claim that $\langle \boldsymbol{u}, \boldsymbol{w}\rangle = 0$:

$$\begin{aligned}
\langle \boldsymbol{u}, \boldsymbol{w}\rangle &= \langle \boldsymbol{u}, \sigma(\boldsymbol{x}) + \boldsymbol{x}\rangle \\
&= \langle \boldsymbol{u}, \sigma(\boldsymbol{x})\rangle + \langle \boldsymbol{u}, \boldsymbol{x}\rangle \\
&= \langle \sigma(\boldsymbol{u}), \sigma(\boldsymbol{x})\rangle + \langle \boldsymbol{u}, \boldsymbol{x}\rangle \\
&= \langle \boldsymbol{u}, \boldsymbol{x}\rangle + \langle \boldsymbol{u}, \boldsymbol{x}\rangle \\
&= 0
\end{aligned}$$

Since U is a hyperplane of X it follows that $X \cap \boldsymbol{w}^\perp = U$. We next show that $\boldsymbol{y} = \sigma(\boldsymbol{x}) \notin \boldsymbol{w}^\perp$. Note that since σ restricted to U is the identity, and $\sigma(\boldsymbol{x}) \neq \boldsymbol{x}$ it follows that $\boldsymbol{x} \notin U$ and $\langle \boldsymbol{w}, \boldsymbol{x}\rangle \neq 0$. We then have:

$$\begin{aligned}
\langle \boldsymbol{y}, \boldsymbol{w}\rangle &= \langle \sigma(\boldsymbol{x}), \boldsymbol{w}\rangle \\
&= \langle \sigma(\boldsymbol{x}), \boldsymbol{w}\rangle \\
&= \langle \sigma(\boldsymbol{x}), \sigma(\boldsymbol{x}) + \boldsymbol{x}\rangle \\
&= \langle \sigma(\boldsymbol{x}), \sigma(\boldsymbol{x})\rangle + \langle \sigma(\boldsymbol{x}), \boldsymbol{x}\rangle \\
&= \langle \boldsymbol{x}, \boldsymbol{x}\rangle + \langle \sigma(\boldsymbol{x}), \boldsymbol{x}\rangle \\
&= \langle \boldsymbol{x} + \sigma(\boldsymbol{x}), \boldsymbol{x}\rangle \\
&= \langle \boldsymbol{w}, \boldsymbol{x}\rangle \\
&\neq 0
\end{aligned}$$

Consequently, $Y = \sigma(X)$ is not contained in $\boldsymbol{w}^{\perp}$. Then $Y \cap \boldsymbol{w}^{\perp}$ is a hyperplane of Y. Since U is a hyperplane of Y contained in $\boldsymbol{w}^{\perp}$ it follows that $Y \cap \boldsymbol{w}^{\perp} = U$. Choose a subspace Z so that $\boldsymbol{w}^{\perp} = U \oplus Z$. Since $U \subset X$, we have $\boldsymbol{w}^{\perp} = U \oplus Z \subset X + Z$. Since $Z \subset \boldsymbol{w}^{\perp}$ we have

$$\begin{array}{rcl} X \cap Z & \subset & (X \cap \boldsymbol{w}^{\perp}) \cap Z \\ & = & U \cap Z = \{\mathbf{0}\}. \end{array}$$

In exactly the same way, $Y \cap Z = \{\mathbf{0}\}$. We now claim that $X \oplus Z = Y \oplus Z = V$. Now $X \oplus Z$ contains $U \oplus Z = \boldsymbol{w}^{\perp}$. However, since X is not contained in $\boldsymbol{w}^{\perp}$ it follows that $\boldsymbol{w}^{\perp}$ is properly contained in $X \oplus Z$. Since $\boldsymbol{w}^{\perp}$ is a hyperplane of V, we can conclude that $X \oplus Z = Y \oplus Z = V$.

Suppose now that $\boldsymbol{x}' \in Z$ and $\boldsymbol{z} \in Z$. Then $\sigma(\boldsymbol{x}') + \boldsymbol{x}' \in W \subset Z^{\perp}$ and therefore, $\langle \sigma(\boldsymbol{x}') + \boldsymbol{x}', \boldsymbol{z} \rangle = 0$. Equivalently, $\langle \sigma(\boldsymbol{x}'), \boldsymbol{z} \rangle = \langle \boldsymbol{x}', \boldsymbol{z} \rangle$. Thus, $\langle \boldsymbol{z}, \boldsymbol{x}' \rangle = \langle \boldsymbol{z}, \sigma(\boldsymbol{x}') \rangle$. Assume now that $\boldsymbol{v}$ is arbitrary in V. We can write $\boldsymbol{v} = \boldsymbol{x}' + \boldsymbol{z}$ for unique vectors $\boldsymbol{x}' \in X$ and $\boldsymbol{z} \in Z$. Now set $S(\boldsymbol{v}) = \sigma(\boldsymbol{x}') + \boldsymbol{z}$. We claim that S is an isometry which extends σ. Thus, suppose $\boldsymbol{v}' = \boldsymbol{x}' + \boldsymbol{z}$ is an arbitrary vector in V for vectors $\boldsymbol{x}' \in X, \boldsymbol{z} \in Z$. Then

$$\begin{array}{rcl} \phi(S(\boldsymbol{v}')) & = & \phi(\sigma(\boldsymbol{x}') + \boldsymbol{z}) \\ & = & \phi(\sigma(\boldsymbol{x}')) + \langle \sigma(\boldsymbol{x}'), \boldsymbol{z} \rangle + \phi(\boldsymbol{z}) \\ & = & \phi(\boldsymbol{x}') + \langle \boldsymbol{x}', \boldsymbol{z} \rangle + \phi(\boldsymbol{z}) \\ & = & \phi(\boldsymbol{x}' + \boldsymbol{z}) \\ & = & \phi(\boldsymbol{v}'). \end{array}$$

Thus, S is an isometry.

b) Now assume that $X \subset \boldsymbol{w}^{\perp}$. Then, of course, $U \subset \boldsymbol{w}^{\perp}$. We claim that $Y \subset \boldsymbol{w}^{\perp}$. Since U is a hyperplane of Y, and U is contained in $\boldsymbol{w}^{\perp}$, it suffices to prove that $\boldsymbol{y} \in \boldsymbol{w}^{\perp}$.

$$\begin{array}{rcl} \langle \boldsymbol{w}, \boldsymbol{y} \rangle & = & \langle \boldsymbol{y} + \boldsymbol{x}, \boldsymbol{y} \rangle \\ & = & \langle \boldsymbol{y}, \boldsymbol{y} \rangle + \langle \boldsymbol{x}, \boldsymbol{y} \rangle \\ & = & \langle \sigma(\boldsymbol{x}), \sigma(\boldsymbol{x}) \rangle + \langle \boldsymbol{x}, \boldsymbol{y} \rangle \\ & = & \langle \boldsymbol{x}, \boldsymbol{x} \rangle + \langle \boldsymbol{x}, \boldsymbol{y} \rangle \\ & = & \langle \boldsymbol{x}, \boldsymbol{x} + \boldsymbol{y} \rangle \\ & = & \langle \boldsymbol{x}, \boldsymbol{w} \rangle \\ & = & 0. \end{array}$$

We now show that $\boldsymbol{w}$ is singular. We first note that since $\boldsymbol{w} = \boldsymbol{y} + \boldsymbol{x}$, $\boldsymbol{y} = \boldsymbol{w} + \boldsymbol{x}$. Therefore,

$$\begin{aligned}\phi(\boldsymbol{y}) &= \phi(\boldsymbol{w})+\langle \boldsymbol{w},\boldsymbol{x}\rangle+\phi(\boldsymbol{x})\\ &= \phi(\boldsymbol{w})+\phi(\boldsymbol{x}).\end{aligned}$$

Since $\phi(\boldsymbol{y})=\phi(\boldsymbol{x})$ we conclude that $\phi(\boldsymbol{w})=0$.

Now by Exercise 14 of Section (1.6), there exists a subspace Z such that $\boldsymbol{w}^{\perp}=X\oplus Z=Y\oplus Z$. Let τ be the operator on $\boldsymbol{w}^{\perp}$ such that $\tau_{|X}=\sigma$ and $\tau_{|Z}$ is the identity map on Z. We claim that this is an isometry of $\boldsymbol{w}^{\perp}$. A typical element of X can be written as $a\boldsymbol{x}+\boldsymbol{v}$ where $\boldsymbol{v}\in U\oplus Z$. For such an element, $\tau(a\boldsymbol{x}+\boldsymbol{v})=a\boldsymbol{y}+\boldsymbol{v}$. Since $\boldsymbol{w}=\boldsymbol{y}+\boldsymbol{x}$ and $\boldsymbol{v}\in Z\subset\boldsymbol{w}^{\perp}$ it follows that $\langle\boldsymbol{y}+\boldsymbol{x},\boldsymbol{v}\rangle=0$. Consequently, $\langle\boldsymbol{y},\boldsymbol{v}\rangle=\langle\boldsymbol{x},\boldsymbol{v}\rangle$. We show that τ is an isometry.

$$\begin{aligned}\phi(\tau(a\boldsymbol{x}+\boldsymbol{v})) &= \phi(a\boldsymbol{y}+\boldsymbol{v})\\ &= \phi(a\boldsymbol{y})+\langle(a\boldsymbol{y},\boldsymbol{v}\rangle+\phi(\boldsymbol{v})\\ &= a^2\phi(\boldsymbol{y})+a\langle(\boldsymbol{y},\boldsymbol{v}\rangle+\phi(\boldsymbol{v})\\ &= a^2\phi(\boldsymbol{x})+a\langle(\boldsymbol{x},\boldsymbol{v}\rangle+\phi(\boldsymbol{v})\\ &= \phi(a\boldsymbol{x})+\langle(a\boldsymbol{x},\boldsymbol{v}\rangle+\phi(\boldsymbol{v})\\ &= \phi(a\boldsymbol{x}+\boldsymbol{v}).\end{aligned}$$

It remains to show that we can extend τ to an isometry of V. We have therefore reduced to the case where $X=Y=\boldsymbol{w}^{\perp}$, σ acts as the identity on a hyperplane U of $\boldsymbol{w}^{\perp}$, for some $\boldsymbol{x}\in X\setminus U, \boldsymbol{w}=\tau(\boldsymbol{x})+\boldsymbol{x}$. If we set $\boldsymbol{y}=\tau(\boldsymbol{x})$ then also $X=Span(\boldsymbol{y})\oplus U$. Now choose any element $\boldsymbol{v}_1\in V,\boldsymbol{v}_1\notin X=\boldsymbol{w}^{\perp}$. Define $F\in\mathcal{L}(V,\mathbb{F})$ such that $F(\boldsymbol{t})=\langle\sigma^{-1}(\boldsymbol{t}),\boldsymbol{v}_1\rangle$ if $\boldsymbol{t}\in\boldsymbol{w}^{\perp}$, and $F(\boldsymbol{v}_1)=0$. Since $\langle\ ,\ \rangle$ is non-degenerate, by Lemma (9.5), there exists a vector $\boldsymbol{v}_2$ such that $F(\boldsymbol{v}')=\langle\boldsymbol{v}',\boldsymbol{v}_2\rangle$ for every vector $\boldsymbol{v}'\in V$. Then, for every vector $\boldsymbol{v}'\in X=\boldsymbol{w}^{\perp},\langle\sigma^{-1}(\boldsymbol{v}'),\boldsymbol{v}_1\rangle=\langle\boldsymbol{v}',\boldsymbol{v}_2\rangle$. Consequently, $\langle\boldsymbol{v}',\boldsymbol{v}_1\rangle=\langle\sigma(\boldsymbol{v}'),\boldsymbol{v}_2\rangle$ for every $\boldsymbol{v}'\in X=\boldsymbol{w}^{\perp}$. If $\phi(\boldsymbol{v}_1)=\phi(\boldsymbol{v}_2)$, then we can extend σ to S by defining $S(\boldsymbol{v}_1)=\boldsymbol{v}_2$. Consider the element $\boldsymbol{v}_3=\boldsymbol{v}_2+a\boldsymbol{w}$. This element is not in $\boldsymbol{w}^{\perp}$ since $\langle\boldsymbol{v}_3,\boldsymbol{w}\rangle=\langle\boldsymbol{v}_2+a\boldsymbol{w},\boldsymbol{w}\rangle=\langle\boldsymbol{v}_2,\boldsymbol{w}\rangle+a\langle\boldsymbol{w},\boldsymbol{w}\rangle=\langle\boldsymbol{v}_2,\boldsymbol{w}\rangle\neq 0$. We now compute $\phi(\boldsymbol{v}_3)$:

$$\begin{aligned}\phi(\boldsymbol{v}_3) &= \phi(\boldsymbol{v}_2+a\boldsymbol{w})\\ &= \phi(\boldsymbol{v}_2)+a\langle\boldsymbol{v}_2,\boldsymbol{w}\rangle+a^2\phi(\boldsymbol{w})\\ &= \phi(\boldsymbol{v}_2)+a\langle\boldsymbol{v}_2,\boldsymbol{w}\rangle.\end{aligned}$$

Set $a=\frac{\phi(\boldsymbol{v}_1)+\phi(\boldsymbol{v}_2)}{\langle\boldsymbol{v}_2,\boldsymbol{w}\rangle}$. Then

$$\begin{aligned}\phi(\boldsymbol{v}_3) &= \phi(\boldsymbol{v}_1)+\frac{\phi(\boldsymbol{v}_1)+\phi(\boldsymbol{v}_2)}{\langle\boldsymbol{v}_2,\boldsymbol{w}\rangle}f\langle\boldsymbol{v}_2,\boldsymbol{w}\rangle\\ &= \phi(\boldsymbol{v}_2)+[\phi(\boldsymbol{v}_1)+\phi(\boldsymbol{v}_2)]\\ &= \phi(\boldsymbol{v}_1).\end{aligned}$$

We can now extend σ to $S : V \to V$ by defining $S(\boldsymbol{v}_1) = \boldsymbol{v}_3$.

Case 2) We now do the general case. We proceed by mathematical induction on $m = dim(X)$. If $m = 1$ then this is contained in case 1. So assume the result holds for all isometries $\sigma : X \to Y$ where $dim(X) = m - 1 \geq 1$ and that $dim(X) = m$. Choose a hyperplane X_0 of X and set $Y_0 = \sigma(X_0)$. By the inductive hypothesis there exists an isometry T of V such that $T_{|X_0} = \sigma_{|X_0}$. Set $\tau = T^{-1}\sigma$. Now τ is an isometry of X and τ restricted to X_0 is the identity. Now by case 1 there is an isometry T' of V such that T' restricted to X is τ. Set $S = TT'$. This is the desired isometry of V.

Definition 8.31 *Let (V, ϕ) be an orthogonal space. A subspace M is a* **totally singular subspace** *if $\phi(\boldsymbol{v}) = 0$ for all $\boldsymbol{v} \in M$. A subspace M is a* **maximal totally singular subspace** *if it is totally singular and not properly contained in a totally singular subspace of V.*

Corollary 8.9 *Let (V, ϕ) be a non-degenerate finite-dimensional orthogonal space over a perfect field of characteristic two with M_1 and M_2 maximal totally singular subspaces. Then $dim(M_1) = dim(M_2)$.*

This is an exercise.

Definition 8.32 *Let (V, ϕ) be a non-degenerate finite-dimensional orthogonal space over a perfect field of characteristic two. The common dimension of every maximal totally singular subspace of V is the* **Witt index** *of (V, ϕ).*

Corollary 8.10 *Let (V, ϕ) be a non-degenerate finite-dimensional orthogonal space over a perfect field of characteristic two and assume X and Y are isometric subspaces of V. Then $X^\perp$ and $Y^\perp$ are isometric.*

This is left as an exercise.

Exercises

1. Prove Corollary (8.6).

2. Prove Corollary (8.9).

3. Prove Corollary (8.10).

4. Let (V, ϕ) be a non-degenerate $2m$-dimensional orthogonal space over a perfect field of characteristic two. Prove that the Witt index of V is either $m - 1$ or m.

5. Let $\mathbb{F}$ be a perfect field of characteristic two and set $V = \mathbb{F}^3$. Define

$\phi\left(\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}\right) = x_1x_2 + x_3^2$. Give an example of isometric subspaces X and Y of V such that there does not exist an isometry S of V with $S(X) = Y$.

6. Let (V, ϕ) be a non-degenerate $2m$-dimensional orthogonal space over a perfect field of characteristic two and Witt index m. Let $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_m)$ be a hyperbolic basis, that is, a basis such that $\phi(\boldsymbol{x}_i) = \phi(\boldsymbol{y}_i) = \langle \boldsymbol{x}_i, \boldsymbol{x}_j \rangle = \langle \boldsymbol{y}_i, \boldsymbol{y}_j \rangle = \langle \boldsymbol{x}_i, \boldsymbol{y}_j \rangle = 0$ for $i \neq j$ and $\langle \boldsymbol{x}_i, \boldsymbol{y}_i \rangle = 1$. Set $X = Span(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m), \mathcal{B}_X = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m), Y = Span(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m), \mathcal{B}_Y = (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m)$. Assume S is an isometry of V such that X and Y are S-invariant. Let S_X be the restriction of S to X and S_Y the restriction of S to Y. Set $M_X = \mathcal{M}_{S_X}(\mathcal{B}_X, \mathcal{B}_X)$ and $M_Y = \mathcal{M}_{S_Y}(\mathcal{B}_Y, \mathcal{B}_Y)$. Prove that $M_Y^{-1} = M_X^{tr}$.

7. Let $O_i(V_i, \phi_i), i = 1, 2$ be two orthogonal spaces with respective associated symmetric forms $\langle\ ,\ \rangle_1$ and $\langle\ ,\ \rangle_2$. Denote by $O_1 \perp O_2$ the pair $(V_1 \oplus V_2, \phi_1 + \phi_2)$ where $(\phi_1 + \phi_2)(\boldsymbol{v}_1 + \boldsymbol{v}_2) = \phi_1(\boldsymbol{v}_1) + \phi_2(\boldsymbol{v}_2)$ for $\boldsymbol{v}_i \in V_i$. Prove that this is a orthogonal space with associated symmetric form defined by $\langle \boldsymbol{v}_1 + \boldsymbol{v}_2, \boldsymbol{w}_1 + \boldsymbol{w}_2 \rangle = \langle \boldsymbol{v}_1, \boldsymbol{w}_1 \rangle_1 + \langle \boldsymbol{v}_2, \boldsymbol{w}_2 \rangle_2$ for $\boldsymbol{v}_1, \boldsymbol{w}_1 \in V_1, \boldsymbol{v}_2, \boldsymbol{w}_2 \in V_2$.

8. Let $\mathbb{F}$ be a perfect field of characteristic two and assume the polynomial $x^2 + x + \delta$ is irreducible in $\mathbb{F}[x]$. Let E_2 denote the orthogonal space $(\mathbb{F}^2, \epsilon)$ with $\epsilon\left(\begin{pmatrix} a \\ b \end{pmatrix}\right) = a^2 + ab + \delta b^2$. Let H_2 denote the orthogonal space $(\mathbb{F}^2, \gamma)$ with $\gamma\left(\begin{pmatrix} a \\ b \end{pmatrix}\right) = ab$. Prove that $E_2 \perp E_2$ is isometric to $H_2 \perp H_2$.

8.5 Real Quadratic Forms

In this section we study finite-dimensional real orthogonal space. In our main theorem we characterize such spaces in terms of three invariants: the rank, the index, and the signature. As a corollary, we determine the number of orbits when the general linear group acts on the space of symmetric real matrices via congruence.

What You Need to Know

To understand the material of this section, you must have already mastered the following concepts: vector space, basis of a vector space, dimension of a vector space, finite-dimensional vector space, linear transformation, coordinate vector with respect to a basis, matrix of a linear transformation, bilinear form, matrix of a bilinear form, symmetric bilinear form, quadratic form, real inner product, orthogonal operator, orthogonal basis, orthogonal matrix, diagonalizable matrix, and congruence of matrices.

Before jumping in, we begin with a word on notation. In this section, V will be a real finite-dimensional vector space with an inner product and a quadratic form ϕ. We will use $\langle\ ,\ \rangle$ to represent the inner product and $\langle\ ,\ \rangle_\phi$ to represent the symmetric form associated with ϕ.

We have previously seen that a quadratic form ϕ (with associated symmetric form $\langle\ ,\ \rangle_\phi$) on a finite-dimensional vector space over a field $\mathbb{F}$ of characteristic not two can be diagonalized; that is, there exists a basis $\mathcal{B} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ for V such that the matrix of $\langle\ ,\ \rangle_\phi$ is a diagonal matrix. Of course, such a basis is an orthogonal basis of (V, ϕ). When the field $\mathbb{F}$ is $\mathbb{R}$, we can use our theory of self-adjoint operators to obtain more.

Theorem 8.17 *Let $(V, \langle\ ,\ \rangle)$ be a finite-dimensional real inner product space and $\langle\ ,\ \rangle_\phi$ a symmetric bilinear form on V. Then there exists an orthonormal basis $\mathcal{B}$ of $(V, \langle\ ,\ \rangle)$ such that the matrix of $\langle\ ,\ \rangle_\phi$ with respect to $\mathcal{B}$ is diagonal.*

Proof *Choose any orthonormal basis $\mathcal{O}$ of $(V, \langle\ ,\ \rangle)$ and let A be the matrix of $\langle\ ,\ \rangle_\phi$ with respect to $\mathcal{O}$. Then A is a symmetric matrix. By Exercise 8 of Section (6.4) there exists an orthogonal matrix Q such that $Q^{tr}AQ$ is a diagonal matrix. Let $\mathcal{B}$ be the basis of $(V, \langle\ ,\ \rangle)$ such that $\mathcal{M}_{I_V}(\mathcal{B}, \mathcal{O}) = Q$. Since Q is an orthogonal matrix and $\mathcal{O}$ is an orthonormal basis it follows that $\mathcal{B}$ is an orthonormal basis. Now the matrix of $\langle\ ,\ \rangle_\phi$ with respect to $\mathcal{B}$ is $Q^{tr}AQ$, which is diagonal as required.*

The following corollary just restates Theorem (8.17):

Corollary 8.11 *Let $(V, \langle\ ,\ \rangle)$ be a finite-dimensional real inner product space and ϕ a quadratic form on V. Then there exists an orthonormal basis $\mathcal{B}$ of $(V, \langle\ ,\ \rangle)$ such that $\mathcal{B}$ is an orthogonal basis of the orthogonal space (V, ϕ).*

In what follows, we shall classify real orthogonal spaces of dimension n by some invariants. One of these invariants has already been introduced, the rank of the space. We recall its definition:

Definition (8.22) *Let (V, ϕ) be a finite-dimensional orthogonal space. The* **rank** *of (V, ϕ) is $dim(V) - dim(Rad(V)) = dim(V/Rad(V))$. As shown in Exercise 2 of Section (8.3), if $\mathcal{B}$ is a basis for V and $\langle\ ,\ \rangle_\phi$ is the associated form, then the rank of (V, ϕ) is the rank of the matrix of $\langle\ ,\ \rangle_\phi$ with respect to $\mathcal{B}$.*

Before introducing the second invariant, we prove a result that goes by the name of *Sylvester's Law of Inertia.*

Theorem 8.18 *Let (V, ϕ) be a real finite-dimensional orthogonal space and $\mathcal{B} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)$ an orthogonal basis for ϕ. Then the following hold:*

i) Let $\pi(\mathcal{B})$ be the number of i such that $\phi(\boldsymbol{v}_i) > 0$. Then $\pi(\mathcal{B})$ is independent of the basis $\mathcal{B}$.

ii) Let $\nu(\mathcal{B})$ be the number of i such that $\phi(\boldsymbol{v}_i) < 0$. Then $\nu(\mathcal{B})$ is independent of the basis $\mathcal{B}$.

Proof *i) Set $\pi = \pi(\mathcal{B})$ and assume $\mathcal{B}$ has been ordered so that $\phi(\boldsymbol{v}_i) > 0$ for $1 \leq i \leq \pi$. Set $U = Span(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\pi)$. Then for every non-zero vector $\boldsymbol{v} \in W, \phi(\boldsymbol{v}) > 0$. Also, set $W = Span(\boldsymbol{v}_{\pi+1}, \ldots, \boldsymbol{v}_n)$. For every vector $\boldsymbol{v} \in W, \phi(\boldsymbol{v}) \leq 0$. Note that $V = U \oplus W$. Suppose U' is a subspace of V which contains U and $dim(U') > \pi$. Then $U' \cap W \neq \{\mathbf{0}\}$. If $\boldsymbol{v}$ is a non-zero vector in $U' \cap W$ then $\phi(\boldsymbol{v}) \leq 0$. Therefore, U is maximal under inclusion amongst all subspaces X such that $\phi(\boldsymbol{x}) > 0$ for all non-zero $\boldsymbol{x} \in X$. By Witt's Theorem for orthogonal spaces, Theorem (8.12), the dimension of such a subspace is an invariant. Thus, π is independent of the basis $\mathcal{B}$.*

ii) This is proved similarly. Alternatively, let $\phi' = -\phi$. Then the number of vectors $\boldsymbol{v}_i$ in the basis $\mathcal{B}$ such that $\phi(\boldsymbol{v}_i) < 0$ is equal to the number of vectors $\boldsymbol{v}_i$ in the basis $\mathcal{B}$ such that $\phi'(\boldsymbol{v}_i) = -\phi(\boldsymbol{v}_i) > 0$.

There are alternative ways to prove the result. One can show that the number π is equal to the number of positive eigenvalues of any symmetric matrix which represents the quadratic form.

There is a matrix version of Theorem (8.18):

Corollary 8.12 *Let A be a real symmetric matrix and D any diagonal matrix which is in the congruence class of A. Then the number of positive diagonal entries and the number of negative diagonal entries are independent of the choice of D.*

Definition 8.33 *Let (V, ϕ) be a real orthogonal space of dimension n. Let $\mathcal{B}$ be an orthogonal basis of (V, ϕ). The invariant $\pi = \pi(\mathcal{B})$ is called the* **index** *of the orthogonal space or of the quadratic form ϕ. The* **signature** *is the number $\sigma = \pi - \nu$, where ν is the invariant $\nu(\mathcal{B})$. The third invariant is the* **rank**, *ρ.*

Remark 8.10 *Given n, the dimension of the orthogonal space, then any two of the invariants π, σ, ρ determine the third: since $\sigma = 2\pi - \rho$. Also, ν can be determined from any two since $\pi + \nu = \rho$.*

The next result is a key step in obtaining a classification of real quadratic forms on a finite-dimensional space.

Lemma 8.31 *Assume (V, ϕ) is a real orthogonal space of dimension n and invariants (π, σ, ρ). Then there exists an orthogonal basis*

$$(\boldsymbol{u}_1, \dots, \boldsymbol{u}_\pi, \boldsymbol{v}_1, \dots, \boldsymbol{v}_{\rho-\pi}, \boldsymbol{w}_1, \dots, \boldsymbol{w}_{n-\rho})$$

where $\phi(\boldsymbol{u}_i) = 1$ for $i = 1, 2, \dots, \pi; \phi(\boldsymbol{v}_j) = -1$, for $j = 1,\ 2,\ \dots \rho - \pi$; and $\phi(\boldsymbol{w}_k) = 0$ for $k = 1, \dots, n - \rho$.

Proof *Let $(\boldsymbol{x}_1, \dots, \boldsymbol{x}_\pi, \boldsymbol{y}_1, \dots, \boldsymbol{y}_{\rho-\pi}, \boldsymbol{z}_1, \dots, \boldsymbol{z}_{n-\rho})$ be an orthogonal basis, where $\phi(\boldsymbol{x}_i) > 0, \phi(\boldsymbol{y}_j) < 0$ and $\phi(\boldsymbol{z}_k) = 0$. Set $\boldsymbol{u}_i = \frac{1}{\sqrt{\phi(\boldsymbol{x}_i)}}\boldsymbol{x}_i, \boldsymbol{v}_j = \frac{1}{\sqrt{-\phi(\boldsymbol{y}_j)}}\boldsymbol{y}_j$ and $\boldsymbol{w}_k = \boldsymbol{z}_k$. This is an orthogonal basis which satisfies the conclusions of the lemma.*

We can now give a classification of quadratic forms on a finite-dimensional real vector space:

Theorem 8.19 *Let (V, ϕ) and (V', ϕ') be real orthogonal spaces of dimension n. Then (V, ϕ) and (V', ϕ') are isometric if and only if they have the same invariants.*

Proof *Suppose (V, ϕ) and (V', ϕ') are isometric via the linear transformation T. Suppose $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\pi, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{\rho-\pi}, \boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n-\rho})$ is an orthogonal basis of V with $\phi(\boldsymbol{u}_i) > 0$ for $1 \le i \le \pi, \phi(\boldsymbol{v}_j) < 0$ for $1 \le j \le \rho - \pi$ and $\phi(\boldsymbol{w}_k) = 0$ for $1 \le k \le n - \rho$. Set $\boldsymbol{u}'_i = T(\boldsymbol{u}_i), \boldsymbol{v}'_j = T(\boldsymbol{v}_j)$ and $\boldsymbol{w}'_k = T(\boldsymbol{w}_k)$. Then $(\boldsymbol{u}'_1, \ldots, \boldsymbol{u}'_\pi, \boldsymbol{v}'_1, \ldots, \boldsymbol{v}'_{\rho-\pi}, \boldsymbol{w}'_1, \ldots, \boldsymbol{w}'_{n-\rho})$ is an orthogonal basis of V' and*

$$\phi'(\boldsymbol{u}'_i) = \phi(\boldsymbol{u}_i) > 0, 1 \le i \le \pi,$$

$$\phi'(\boldsymbol{v}'_j) = \phi(\boldsymbol{v}_j) < 0, 1 \le j \le \rho - \pi,$$

$$\phi'(\boldsymbol{w}'_k) = \phi(\boldsymbol{w}_k) = 0, 1 \le k \le n - \rho.$$

It then follows that the invariants for (V', ϕ') are (π, σ, ρ), the same as (V, ϕ).

Conversely, assume that (V, ϕ) and (V', ϕ') are real orthogonal spaces of dimension n and have the same invariants, (π, σ, ρ).

By Lemma (8.31), there is an orthogonal basis $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\pi, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{\rho-\pi}, \boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n-\rho})$ of V with $\phi(\boldsymbol{u}_i) = 1$ for $1 \le i \le \pi, \phi(\boldsymbol{v}_j) = -1$ for $1 \le j \le \rho - \pi$ and $\phi(\boldsymbol{w}_k) = 0$ for $1 \le k \le n - \rho$.

Likewise, there is an orthogonal basis $(\boldsymbol{u}'_1, \ldots, \boldsymbol{u}'_\pi, \boldsymbol{v}'_1, \ldots, \boldsymbol{v}'_{\rho-\pi}, \boldsymbol{w}'_1, \ldots, \boldsymbol{w}'_{n-\rho})$ of V' with $\phi'(\boldsymbol{u}'_i) = 1$ for $1 \le i \le \pi, \phi'(\boldsymbol{v}'_j) = -1$ for $1 \le j \le \rho - \pi$ and $\phi'(\boldsymbol{w}'_k) = 0$ for $1 \le k \le n - \rho$.

Let $T : V \to V'$ be the linear transformation such that $T(\boldsymbol{u}_i) = \boldsymbol{u}'_i$ for $1 \le i \le \pi$, $T(\boldsymbol{v}_j) = \boldsymbol{v}'_j$ for $1 \le j \le \rho - \pi$ and $T(\boldsymbol{w}_k) = \boldsymbol{w}'_k$ for $1 \le k \le n - \rho$. We claim that T is an isometry.

If $\boldsymbol{x} = \sum_{i=1}^{\pi} a_i \boldsymbol{u}_i + \sum_{j=1}^{\rho-\pi} b_j \boldsymbol{v}_j + \sum_{k=1}^{n-\rho} c_k \boldsymbol{w}_k$, then

$$\phi(\boldsymbol{x}) = \sum_{i=1}^{\pi} a_i^2 - \sum_{j=1}^{\rho-\pi} b_j^2.$$

On the other hand, if $\boldsymbol{x}' = T(\boldsymbol{x})$, then

$$\boldsymbol{x}' = \sum_{i=1}^{\pi} a_i \boldsymbol{u}'_i + \sum_{j=1}^{\rho-\pi} b_j \boldsymbol{v}'_j + \sum_{k=1}^{n-\rho} c_k \boldsymbol{w}'_k,$$

$$\phi'(\boldsymbol{x}') = \sum_{i=1}^{\pi} a_i^2 - \sum_{j=1}^{\rho-\pi} b_j^2 = \phi(\boldsymbol{x}).$$

The matrix version of this theorem follows:

Corollary 8.13 *Two real symmetric $n \times n$ matrices are congruent if and only if they have the same invariants.*

One class of real orthogonal space of dimension n stands out: when the index of the orthogonal space is equal to the rank of the space, is equal to n.

Definition 8.34 *A finite-dimensional real orthogonal space (V, ϕ) is said to be* **positive definite** *if $\phi(\boldsymbol{x}) > 0$ for all non-zero vectors $\boldsymbol{x}$. An $n \times n$ real symmetric matrix is* **positive definite** *if it represents a positive definite quadratic form.*

An example of a positive definite orthogonal space is a real finite-dimensional inner product space. In fact, the converse also holds: a positive definite orthogonal space is a real inner product space.

There is a very nice characterization of positive definite matrices:

Theorem 8.20 *Let A be a real $n \times n$ symmetric matrix. Then the following are equivalent:*

1) A is positive definite.

2) A is congruent to the identity matrix.

3) $A = Q^{tr}Q$ for some invertible matrix Q.

We leave this as an exercise.

Exercises

1. Determine the invariants for the symmetric matrix $\begin{pmatrix} 0 & 2 & 1 \\ 2 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$.

2. Determine the invariants for the symmetric matrix $\begin{pmatrix} 0 & 2 & 0 \\ 2 & 1 & 2 \\ 0 & 2 & 2 \end{pmatrix}$.

3. Let ϕ be the orthogonal form defined on $\mathbb{R}^3$ by $\phi(\boldsymbol{x}) = \boldsymbol{x}^{tr} A \boldsymbol{x}$, where A is the matrix of Exercise 1. Find an orthogonal basis $(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3)$ such that $\phi(\boldsymbol{v}_i) \in \{-1, 0, 1\}$.

4. Let ϕ be the orthogonal form defined on $\mathbb{R}^3$ by $\phi(\boldsymbol{x}) = \boldsymbol{x}^{tr} A \boldsymbol{x}$, where A is the matrix of Exercise 2. Find an orthogonal basis $(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3)$ such that $\phi(\boldsymbol{v}_i) \in \{-1, 0, 1\}$.

5. Determine, with a proof, the number of congruence classes of real $n \times n$ symmetric matrices.

6. Recall for an orthogonal space (V, ϕ) the Witt index is the dimension of a maximal totally singular subspace. Let (V, ϕ) be a real non-degenerate orthogonal space of dimension n with associated form $\langle\ ,\ \rangle_\phi$.

a) Prove that if n is odd then the isometry class of (V, ϕ) is determined by the Witt index and the sign of $det(A)$ where A is any matrix representing $\langle\ ,\ \rangle_\phi$.

b) If n is even and the Witt index is less than $\frac{n}{2}$, then there are two isometry classes of (V, ϕ).

c) If n is even and the Witt index is $\frac{n}{2}$, then there is a unique isometry class.

7. Let $(V, \langle\ ,\ \rangle)$ be a finite-dimensional real inner product space and T a self-adjoint (symmetric) operator. Define a map $[\ ,\ ] : V \times V \to \mathbb{R}$ by $[\boldsymbol{x}, \boldsymbol{y}] = \langle \boldsymbol{x}, T(\boldsymbol{y})\rangle$. Prove that $[\ ,\ ]$ is a symmetric bilinear form on V.

8. Let $(V, \langle\ ,\ \rangle)$ be a finite-dimensional real inner product space and $[\ ,\ ]$ a symmetric bilinear form on V. Prove that there exists a symmetric operator T on V such that $[\boldsymbol{x}, \boldsymbol{y}] = \langle \boldsymbol{x}, T(\boldsymbol{y})\rangle$.

9. Prove Theorem (8.20).

This page intentionally left blank

9

Sesquilinear Forms and Unitary Geometry

CONTENTS

In this chapter we generalize the notion of a bilinear form and introduce the concept of a sesquilinear form. In the first section of this chapter we develop some of the basic properties of sesquilinear forms and, in analogy with bilinear forms, introduce the notion of a reflexive sesquilinear form. Examples are Hermitian and skew Hermitian forms. We then prove that a reflexive sesquilinear form is equivalent to a Hermitian or skew Hermitian form. The second section is devoted to the structure of a unitary space, that is, a vector space equipped with a Hermitian or skew-Hermitian form. In our main result we prove Witt's theorem for a non-degenerate unitary space.

9.1 Basic Properties of Sesquilinear Forms

In this section we introduce the notion of a sesquilinear form. An inner product on a complex vector space is an example. We then go on to develop the properties of sesquilinear forms. We define what is meant by a reflexive sesquilinear form. Examples are Hermitian and skew-Hermitian forms. In our main result prove that a reflexive sesquilinear form is equivalent to a Hermitian or skew-Hermitian form.

What You Need to Know

To be successful in understanding the new material of this section, it is essential that you have already mastered the following concepts: vector space, basis of a vector space, dimension of a vector space, finite-dimensional vector space, linear transformation, coordinate vector with respect to a basis, matrix of a linear transformation, an algebra, determinant of a matrix or operator, multilinear map, multilinear form, bilinear map, and bilinear form.

We begin with a definition:

Definition 9.1 *Let $\mathbb{F}$ be a field, σ an automorphism of $\mathbb{F}$, and V and W vectors spaces over $\mathbb{F}$. A map $T : V \to W$ is σ-semilinear if the following hold:*

1) For $\boldsymbol{u}, \boldsymbol{v} \in V, T(\boldsymbol{u}+\boldsymbol{v}) = T(\boldsymbol{u}) + T(\boldsymbol{v})$; and

2) For $a \in \mathbb{F}, \boldsymbol{v} \in V, T(a\boldsymbol{v}) = \sigma(a)T(\boldsymbol{v})$.

We will denote the collection of all σ-semilinear maps from V to W by $\mathcal{L}_\sigma(V, W)$.

Lemma 9.1 *Let $\mathbb{F}$ be a field and σ an automorphism of $\mathbb{F}$. Let V and W be vectors spaces over $\mathbb{F}$. Then $\mathcal{L}_\sigma(V, W)$ is a vector space over $\mathbb{F}$.*

Proof *Assume $S, T \in \mathcal{L}_\sigma(V, W)$. Clearly $S + T$ is additive so we only need show that for $\boldsymbol{v} \in V$ and $a \in \mathbb{F}$ that $(S+T)(a\boldsymbol{v}) = \sigma(a)(S+T)(\boldsymbol{v})$. By the definition of $S+T, (S+T)(a\boldsymbol{v}) = S(a\boldsymbol{v}) + T(a\boldsymbol{v})$. Since both S and T are σ semilinear, $S(a\boldsymbol{v}) = \sigma(a)S(\boldsymbol{v})$ and $T(a\boldsymbol{v}) = \sigma(a)T(\boldsymbol{v})$. Then*

$$\begin{aligned}(S+T)(a\boldsymbol{v}) &= \sigma(a)S(\boldsymbol{v}) + \sigma(a)T(\boldsymbol{v}) \\ &= \sigma(a)[S(\boldsymbol{v}) + T(\boldsymbol{v})] \\ &= \sigma(a)(S+T)(\boldsymbol{v}).\end{aligned}$$

Next we show if $T \in \mathcal{L}_\sigma(V, W)$ and $b \in \mathbb{F}$ then $bT \in \mathcal{L}_\sigma(V, W)$. Suppose then that $\boldsymbol{v}, \boldsymbol{w} \in V$. Then

$$\begin{aligned}(bT)(\boldsymbol{v}+\boldsymbol{w}) &= b[T(\boldsymbol{v}+\boldsymbol{w})]\\ &= b[T(\boldsymbol{v})+T(\boldsymbol{w})]\\ &= b[T(\boldsymbol{v})]+b[T(\boldsymbol{w})]\\ &= (bT)(\boldsymbol{v})+(bT)(\boldsymbol{w})\end{aligned}$$

and therefore bT is additive.

Now assume $\boldsymbol{v} \in V, a \in \mathbb{F}$. Then

$$\begin{aligned}(bT)(a\boldsymbol{v}) &= b[T(a\boldsymbol{v})]\\ &= b[\sigma(a)T(\boldsymbol{v})]\\ &= [b\sigma(a)]T(\boldsymbol{v})\\ &= [\sigma(a)b]T(\boldsymbol{v})\\ &= \sigma(a)[bT(\boldsymbol{v})]\\ &= \sigma(a)[(bT)(\boldsymbol{v})]\end{aligned}$$

as required.

Lemma 9.2 *Assume σ, τ are automorphisms of the field $\mathbb{F}$ and U, V, W are vector spaces over $\mathbb{F}$. Assume $S : U \to W$ is a σ-semilinear map and $T : V \to W$ is a τ-semilinear map. Then $T \circ S : U \to W$ is a $\tau \circ \sigma$-semilinear map.*

This is left as an exercise.

We now introduce the main object of this section:

Definition 9.2 *Let $\mathbb{F}$ be a field and σ an automorphism of $\mathbb{F}$. Let V be a vector space over $\mathbb{F}$. A map $f : V \times V \to \mathbb{F}$ is said to be* σ-**sesquilinear** *if the following hold:*

1) $f(a\boldsymbol{u} + b\boldsymbol{v}, \boldsymbol{w}) = af(\boldsymbol{u}, \boldsymbol{w}) + bf(\boldsymbol{v}, \boldsymbol{w})$;

2) $f(\boldsymbol{w}, a\boldsymbol{u} + b\boldsymbol{v}) = \sigma(a)f(\boldsymbol{w}, \boldsymbol{u}) + \sigma(b)f(\boldsymbol{w}, \boldsymbol{v})$.

Thus, when we fix the second argument of f and allow the first argument to range over V, we obtain a linear functional. When we fix the first argument and allow the second to range over V, we obtain a σ-semilinear map from V to $\mathbb{F}$.

Example 9.1 *If $\sigma = I_{\mathbb{F}}$, the trivial automorphism, then a σ sesquilinear form is just a bilinear form.*

Example 9.2 *Let $(V, \langle\ ,\ \rangle)$ be a complex inner product space. Then $\langle\ ,\ \rangle : V \times V \to \mathbb{C}$ is a σ sesquilinear form where σ is complex conjugation: $\sigma(a+bi) = a - bi$ for $a, b \in \mathbb{R}$.*

Example 9.3 *Let $V = \mathbb{F}^n$ and $A \in M_{nn}(\mathbb{F})$. For $\boldsymbol{v} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$ denote by $\sigma(\boldsymbol{v})$ the vector in V obtained by applying σ to each entry of $\boldsymbol{v}$:*

$$\sigma(\boldsymbol{v}) = \begin{pmatrix} \sigma(a_1) \\ \sigma(a_2) \\ \vdots \\ \sigma(a_n) \end{pmatrix}.$$

Now define $f : V \times V \to \mathbb{F}$ by

$$f(\boldsymbol{u}, \boldsymbol{v}) = \boldsymbol{u}^{tr} A \sigma(\boldsymbol{v}).$$

Definition 9.3 *Let f, g be sesquilinear forms on V. Then f and g are said to be* **equivalent** *if there exists $\gamma \in \mathbb{F}$ such that $g = \gamma f$. The forms f and g are* **similar** *if there is a linear transformation $T : V \to V$ such that $g(\boldsymbol{v}, \boldsymbol{w}) = f(T(\boldsymbol{v}), T(\boldsymbol{w}))$ for all $\boldsymbol{v}, \boldsymbol{w} \in V$.*

Definition 9.4 *Let $\mathbb{F}$ be a field and σ an automorphism of $\mathbb{F}$. Let V be a vector space over $\mathbb{F}$. We denote by $SEQ_\sigma(V)$ the set of all σ-sesquilinear forms on V.*

Our next result is an immediate consequence of Lemma (9.1.

Lemma 9.3 *Let $\mathbb{F}$ be a field, σ an automorphism of $\mathbb{F}$, and V be a vector space over $\mathbb{F}$. Then $SEQ_\sigma(V)$ is a vector space over $\mathbb{F}$.*

For the remainder of this section assume that $\mathbb{F}$ is a field, σ an automorphism of $\mathbb{F}$, and V is an n-dimensional vector space over $\mathbb{F}$.

Definition 9.5 *Assume $f \in SEQ_\sigma(V)$ and let $\mathcal{B} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ be a basis of V. For $1 \le i, j \le n$ set $a_{ij} = f(\boldsymbol{v}_i, \boldsymbol{v}_j)$. The matrix A whose (i, j)-entry is a_{ij} is the* **matrix** *of f with respect to $\mathcal{B}$ and is denoted by $\mathcal{M}_f(\mathcal{B})$.*

The following should remind the reader of Theorem (8.3). We leave the proof as an exercise.

Theorem 9.1 *Let $f \in SEQ_\sigma(V), \mathcal{B} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ be a basis for V, and $A = \mathcal{M}_f(\mathcal{B})$. Then for any vectors $\boldsymbol{u}, \boldsymbol{v} \in V$ we have*

$$f(\boldsymbol{u}, \boldsymbol{v}) = [\boldsymbol{u}]_{\mathcal{B}}^{tr} A \sigma([\boldsymbol{v}]_{\mathcal{B}}).$$

An immediate consequence of Theorem (9.1) is

Corollary 9.1 *Let $\mathcal{B} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ be a basis of V. For $f \in SEQ_\sigma(V)$ the map $f \to \mathcal{M}_f(\mathcal{B})$ is an isomorphism of vector spaces. Consequently, $dim(SEQ_\sigma(V)) = n^2$.*

Most of the definitions and results of Section (8.1) have analogs for sesquilinear forms. We will focus on the most important ones.

Definition 9.6 *Let f be a σ-sesquilinear form. The* **left radical** *of f, $Rad_L(f)$, consists of all vectors $\boldsymbol{v}$ such that $f(\boldsymbol{v}, \boldsymbol{w}) = 0$ for all $\boldsymbol{w} \in V$. The* **right radical**, *$Rad_R(f)$, is defined similarly: the set of $\boldsymbol{w} \in V$ such that $f(\boldsymbol{v}, \boldsymbol{w}) = 0$ for all $\boldsymbol{v} \in V$. Both the left and right radical are subspaces of V as we prove below, but they may not be equal. However, they do always have the same dimension.*

Lemma 9.4 *Let f be a σ-sesquilinear form. Then $Rad_L(f)$ and $Rad_R(f)$ are subspaces of V. Moreover, $dim(Rad_L(f)) = dim(Rad_R(f))$.*

Proof *Choose a basis $\mathcal{B} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ and set $A = \mathcal{M}_f(\mathcal{B})$. It is straightforward to see that $Rad_L(f)$ consists of all vectors $\boldsymbol{v}$ such that $[\boldsymbol{v}]_{\mathcal{B}}$ is in the null space of the matrix A^{tr} and $Rad_R(f)$ consists of all vectors $\boldsymbol{w}$ such that $\sigma([\boldsymbol{w}]_{\mathcal{B}})$ is in the null space of A. This implies that both $Rad_L(f)$ and $Rad_R(f)$ are subspaces of V with dimension equal to $dim(V) - rank(A)$.*

A consequence of Lemma (9.4) is that $Rad_L(f) = \{\boldsymbol{0}\}$ if and only if $Rad_R(f) = \{\boldsymbol{0}\}$. We give a name to such forms:

Definition 9.7 *A σ-sesquilinear form f is* **non-degenerate** *if $Rad_L(f) = Rad_R(f) = \{\mathbf{0}\}$.*

Lemma 9.5 *Assume f is a non-degenerate σ-sesquilinear form and $F : V \to \mathbb{F}$ is a linear functional. Then there is a unique vector $\boldsymbol{v} \in V$ such that $F(\boldsymbol{w}) = f(\boldsymbol{w}, \boldsymbol{v})$.*

Proof *Let $\mathcal{B} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ be a basis for V. Denote by g_i the linear function on V which is given by $g_i(\boldsymbol{w}) = f(\boldsymbol{w}, \boldsymbol{v}_i)$. We claim that $(g_1, \dots, g_n)$ is linearly independent in $\mathcal{L}(V, \mathbb{F})$. Suppose $\sum_{i=1}^n a_i g_i = \mathbf{0}_{V \to \mathbb{F}}$. Set $b_i = \sigma^{-1}(a_i)$ and $\boldsymbol{v} = \sum_{i=1}^n b_i \boldsymbol{v}_i$. It then follows that $f(\boldsymbol{w}, \boldsymbol{v}) = 0$ for $\boldsymbol{w} \in V$, that is, $\boldsymbol{v} \in Rad_R(f)$. Since f is non-degenerate we can conclude that $\boldsymbol{v} = \mathbf{0}$. Since $\mathcal{B}$ is linearly independent, it then follows that $b_1 = b_2 = \cdots = b_n = 0$. Since σ is an automorphism of $\mathbb{F}$ we then have $a_1 = \cdots = a_n = 0$ and $(g_1, \dots, g_n)$ is linearly independent as claimed.*

Since the dimension of $\mathcal{L}(V, \mathbb{F})$ is n, it now follows that $(g_1, \dots, g_n)$ is a basis for $\mathcal{L}(V, \mathbb{F})$. Consequently, if $F \in V'$ then there are scalars $a_i \in \mathbb{F}$ such that $F = \sum_{i=1}^n a_i g_i$. Again set $b_i = \sigma^{-1}(a_i)$ and $\boldsymbol{v} = b_1 \boldsymbol{v}_1 + \cdots + b_n \boldsymbol{v}_n$. For a vector $\boldsymbol{w} \in V$ we compute $f(\boldsymbol{w}, \boldsymbol{v})$:

$$\begin{aligned} f(\boldsymbol{w}, \boldsymbol{v}) = f(\boldsymbol{w}, b_1 \boldsymbol{v}_1 + \dots b_n \boldsymbol{v}_n) &= f(\boldsymbol{w}, b_1 \boldsymbol{v}_1) + \cdots + f(\boldsymbol{w}, b_n \boldsymbol{v}_n) \\ &= \sigma(b_1) f(\boldsymbol{v}, \boldsymbol{v}_1) + \cdots + \sigma(b_n) f(\boldsymbol{w}, \boldsymbol{v}_n) \\ &= a_1 f(\boldsymbol{w}, \boldsymbol{v}_1) + \cdots + a_n f(\boldsymbol{w}, \boldsymbol{v}_n) \\ &= a_1 g_1(\boldsymbol{v}) + \cdots + a_n g_n(\boldsymbol{v}) \\ &= [a_1 g_1 + \cdots + a_n g_n](\boldsymbol{v}) \\ &= F(\boldsymbol{v}). \end{aligned}$$

This shows the existence of $\boldsymbol{v}$. On the other hand, if also $F(\boldsymbol{w}) = f(\boldsymbol{w}, \boldsymbol{v}')$ for all $\boldsymbol{w}$ then $\boldsymbol{v} - \boldsymbol{v}'$ is in the right radical of f and consequently, $\boldsymbol{v}' = \boldsymbol{v}$ since f is non-degenerate.

In a similar way we can prove:

Lemma 9.6 *Assume f is a non-degenerate σ-sesquilinear form and $F : V \to \mathbb{F}$ is a σ-semilinear transformation. Then there is a unique vector $\boldsymbol{v} \in V$ such that $F(\boldsymbol{w}) = f(\boldsymbol{v}, \boldsymbol{w})$.*

Definition 9.8 *Let f be a σ-sesquilinear form. Define a relation $\perp_f$ on V by $\boldsymbol{u} \perp_f \boldsymbol{v}$ if and only if $f(\boldsymbol{u}, \boldsymbol{v}) = 0$. The form f is said to be* **reflexive** *when $\perp_f$ is a symmetric relation. Following are examples of reflexive sesquilinear forms:*

Definition 9.9 *Assume the automorphism σ has order two, $\sigma^2 = I_{\mathbb{F}} \neq \sigma$, and for $a \in \mathbb{F}$ denote by $\overline{a}$ the σ image of a, $\sigma(a)$. Let $\epsilon \in \mathbb{F}$ be chosen such so that $\epsilon\sigma(\epsilon) = 1$. A σ-sesquilinear from f on a vector space V is said to be* (ϵ, σ)**-Hermitian** *if for all $\boldsymbol{v}, \boldsymbol{w} \in V, f(\boldsymbol{v}, \boldsymbol{w}) = \epsilon\overline{f(\boldsymbol{w}, \boldsymbol{v})}$.*

When $\epsilon = 1$, we say f is σ-Hermitian and when $\epsilon = -1$ we say f is σ-skew Hermitian.

We will usually drop the use of σ and just refer to an ϵ-Hermitian form.

Example 9.4 *Hermitian and skew-Hermitian forms are reflexive. We leave this as an exercise.*

Notation. Let σ be an automorphism of $\mathbb{F}$. We will denote images under σ using the bar notation: $\sigma(a) = \overline{a}$. If $\boldsymbol{v} \in \mathbb{F}^n$, the expression $\overline{\boldsymbol{v}}$ denotes the result of applying σ to every entry of $\boldsymbol{v}$ and, similarly, for a matrix A, the symbol $\overline{A}$ denotes the matrix obtained from A by applying σ to every entry of A.

Lemma 9.7 *Assume σ has order 2, f is a σ-sesquilinear form on V, and $\mathcal{B} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ is a basis for V. Let $A = \mathcal{M}_f(\mathcal{B})$. Then the following hold:*

i) The form f is Hermitian if and only if $A^{tr} = \overline{A}$.

ii) The form f is skew-Hermitian if and only if $A^{tr} = -\overline{A}$.

We leave this as an exercise.

Definition 9.10 *Assume that σ has order 2. An $n \times n$ matrix A is* σ**-Hermitian** *if $A^{tr} = \overline{A}$. A is* σ**-skew-Hermitian** *if $A^{tr} = -\overline{A}$.*

We will complete this section with a characterization of reflexive σ-sesquilinear forms. We begin with a lemma.

Lemma 9.8 *Assume $\sigma \neq I_{\mathbb{F}}$ and f is a non-degenerate σ-sesquilinear form on the space V. Then there exists a vector $\boldsymbol{v}$ such that $f(\boldsymbol{v}, \boldsymbol{v}) \neq 0$.*

Proof *Assume $f(\boldsymbol{v},\boldsymbol{v}) = 0$ for all $\boldsymbol{v}$. Then*

$$0 = f(\boldsymbol{v}+\boldsymbol{w},\boldsymbol{v}+\boldsymbol{w}) = f(\boldsymbol{v},\boldsymbol{w}) + f(\boldsymbol{w},\boldsymbol{v}).$$

If $char(\mathbb{F}) \neq 2$ then f is alternating and $\sigma = I_V$. If $char(\mathbb{F}) = 2$ then f is symmetric and again $\sigma = I_{\mathbb{F}}$.

Corollary 9.2 *Assume that $\sigma \neq I_{\mathbb{F}}$, and f is a non-degenerate reflexive σ-sesquilinear form on the space V. Then there exists a basis $(\boldsymbol{v}_1,\dots,\boldsymbol{v}_n)$ for V such that $a_i = f(\boldsymbol{v}_i,\boldsymbol{v}_i) \neq 0$ while $f(\boldsymbol{v}_i,\boldsymbol{v}_j) = 0$ for every $i \neq j$.*

Proof *The proof is by induction on $n = dim(V)$. If $n = 1$ there is nothing to prove. Assume that $n \geq 2$ and the result holds for spaces with dimension $n-1$. By Lemma (9.8) there is a vector $\boldsymbol{v}$ such that $a = f(\boldsymbol{v},\boldsymbol{v}) \neq 0$. Now f restricted to $U = \boldsymbol{v}^{\perp} = \{\boldsymbol{w} \in V | f(\boldsymbol{w},\boldsymbol{v}) = 0\}$ is non-degenerate. By the induction hypothesis there exists a basis $(\boldsymbol{v}_1,\dots,\boldsymbol{v}_{n-1})$ of U such that $a_i = f(\boldsymbol{v}_i,\boldsymbol{v}_i) \neq 0$ and $f(\boldsymbol{v}_i,\boldsymbol{v}_j) = 0$ for $i \neq j$. Set $\boldsymbol{v}_n = \boldsymbol{v}$ and $a_n = a$.*

We will need the following result in the course of proving our main theorem. It is a special case of Hilbert's theorem 90.

Lemma 9.9 *Let $\mathbb{E} \subset \mathbb{F}$ be a Galois extension of degree two with Galois group generated by σ. Assume $a \in \mathbb{F}$ satisfies $a\sigma(a) = 1$. Then there is an element $b \in \mathbb{F}$ such that $a = \frac{b}{\sigma(b)}$.*

Proof *Since the degree of the extension is two, $\sigma^2 = I_{\mathbb{F}}$. The sequence $(I_{\mathbb{F}},\sigma)$ of the Galois group of the extension are $\mathbb{E} \subset \mathbb{F}$ is linearly independent as elements of $\mathcal{L}_{\mathbb{E}}(\mathbb{F},\mathbb{F})$, the space of $\mathbb{E}$-linear transformations of the space $\mathbb{F}$. Consequently, there must be an element $c \in \mathbb{F}$ such that $b = c + a\sigma(c) \neq 0$. Applying σ to b we get*

$$\sigma(b) = \sigma(c) + \sigma(a)\sigma^2(c) = \sigma(c) + \sigma(a)c.$$

Multiplying by a we get

$$a\sigma(b) = a\sigma(c) + a\sigma(a)c = a\sigma(c) + c = b.$$

We now prove our main result.

Theorem 9.2 *Assume $\sigma \neq I_{\mathbb{F}}$ and f is a reflexive σ-sesquilinear form on the space V and $dim(V/Rad(f)) \geq 2$. Then σ has order two and there is an element $\gamma \in \mathbb{F}$ such that $g = \gamma f$ is Hermitian.*

Proof *Let R be the radical of f and choose a complement U to R. Then $f_{|U\times U}$ is non-degenerate. It suffices to prove the result for $(U, f_{|U\times U})$ and therefore we may assume that f is non-degenerate. By Lemma (9.2) there exists a basis $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ such that $a_i = f(\boldsymbol{v}_i, \boldsymbol{v}_i) \neq 0$ and $f(\boldsymbol{v}_i, \boldsymbol{v}_j) = 0$ for $i \neq j$. We will first show for $i \neq j$, that $\sigma(a_i)a_j = a_i\sigma(a_j)$, equivalently, that $\frac{a_i}{\sigma(a_i)}$ is independent of i. Toward that purpose, note that $f(a_j\boldsymbol{v}_i - a_i\boldsymbol{v}_j, \boldsymbol{v}_i + \boldsymbol{v}_j) = 0$. By reflexivity, $f(\boldsymbol{v}_i + \boldsymbol{v}_j, a_j\boldsymbol{v}_i - a_i\boldsymbol{v}_i) = \sigma(a_j)a_i - \sigma(a_i)a_j = 0$ which proves the claim.*

It follows from what we have just proved that $\frac{a_i}{a_j} \in \mathbb{F}^{\langle\sigma\rangle} := \{a \in \mathbb{F} | \sigma(a) = a\}$, the fixed field of σ which we denote by $\mathbb{E}$. We next prove that $\sigma^2 = I_{\mathbb{F}}$.

Let $c \in \mathbb{F}$ and set $\boldsymbol{v}_1' = c\boldsymbol{v}_1$ and $a_1' = f(\boldsymbol{v}_1', \boldsymbol{v}_1') = c\sigma(c)a_1$. By the above proof it follows that $\frac{a_1'}{a_2} \in \mathbb{E}$. This implies that $c\sigma(c) \in \mathbb{E}$. We then have

$$\begin{aligned} c\sigma(c) &= \sigma(c\sigma(c)) \\ &= \sigma(c)\sigma^2(c), \end{aligned}$$

from which we conclude that $\sigma^2(c) = c$. Since c is arbitrary, it follows that $\sigma^2 = I_{\mathbb{F}}$. Now set $\epsilon = \frac{a_1}{\sigma(a_1)} = \frac{a_i}{\sigma(a_i)}$. For the remainder of this proof we use the bar notation: $\sigma(a) = \overline{a}$. We will show that for any $\boldsymbol{v}, \boldsymbol{w} \in V$, $f(\boldsymbol{w}, \boldsymbol{v}) = \epsilon\overline{f(\boldsymbol{v}, \boldsymbol{w})}$. Let $\boldsymbol{v} = \sum_{i=1}^n c_i\boldsymbol{v}_i, \boldsymbol{w} = \sum_{i=1}^n d_i\boldsymbol{v}_i$. Then

$$f(\boldsymbol{v}, \boldsymbol{w}) = \sum_{i=1}^n c_i a_i \overline{d_i}, f(\boldsymbol{w}, \boldsymbol{v}) = \sum_{i=1}^n d_i a_i \overline{c_i}.$$

Since $\frac{a_i}{\sigma(a_i)} = \epsilon, \epsilon\overline{a_i} = a_i$. Thus,

$$\epsilon\overline{f(\boldsymbol{v}, \boldsymbol{w})} = \epsilon\sum_{i=1}^n \overline{c_i a_i} d_i = \sum_{i=1}^n \overline{c_i}\epsilon\overline{a_i} d_i =$$

$$\sum_{i=1}^n d_i a_i \overline{c_i} = f(\boldsymbol{w}, \boldsymbol{v}).$$

Now set $\gamma = \overline{a_1}$ and $g = \gamma f$. Then f and g are equivalent. We claim that $g(\boldsymbol{w}, \boldsymbol{v}) = \overline{g(\boldsymbol{v}, \boldsymbol{w})}$ for all $\boldsymbol{v}, \boldsymbol{w} \in V$. Thus,

$$\begin{aligned} g(\boldsymbol{w}, \boldsymbol{v}) &= \gamma f(\boldsymbol{w}, \boldsymbol{v}) \\ &= \gamma\epsilon\overline{f(\boldsymbol{v}, \boldsymbol{w})} \\ &= \overline{a_1}\epsilon\overline{f(\boldsymbol{v}, \boldsymbol{w})} \\ &= a_1\overline{f(\boldsymbol{v}, \boldsymbol{w})} \\ &= \overline{\gamma}\overline{f(\boldsymbol{v}, \boldsymbol{w})} \\ &= \overline{\gamma f(\boldsymbol{v}, \boldsymbol{w})} \\ &= \overline{g(\boldsymbol{v}, \boldsymbol{w})}. \end{aligned}$$

Exercises

1. Prove Lemma (9.2).

2. Prove Lemma (9.3).

3. Prove Theorem (9.1).

4. Prove Lemma (9.6).

5. Prove Lemma (9.7).

6. Assume f is a non-degenerate σ-sesquilinear form on a space V and that $\mathcal{B} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ is a basis of V. Prove that there exists a basis $\mathcal{B}' = (\boldsymbol{v}'_1, \dots, \boldsymbol{v}'_n)$ such that $f(\boldsymbol{v}'_i, \boldsymbol{v}_j) = 0$ if $i \neq j$ and $f(\boldsymbol{v}'_i, \boldsymbol{v}_i) = 1$.

7. We continue with the notation and assumptions of Exercise 6. Let $\mathcal{B}^* = (\boldsymbol{v}^*_1, \dots, \boldsymbol{v}^*_n)$ be the basis of V such that $f(\boldsymbol{v}^*_i, \boldsymbol{v}'_j) = 0$ if $i \neq j$ and $f(\boldsymbol{v}^*_i, \boldsymbol{v}'_i) = 1$. Assume $\mathcal{B}^* = \mathcal{B}$. Does this imply that f is reflexive? Prove or give a counterexample.

8. Let $\mathbb{F}$ be a field, σ a non-identity automorphism of $\mathbb{E}$ satisfying $\sigma^2 = I_{\mathbb{F}}$, and set $\mathbb{E} = \mathbb{F}^{\sigma}$. The extension $\mathbb{E} \subset \mathbb{F}$ is Galois of degree two. Define $tr_{\mathbb{F}/\mathbb{E}} : \mathbb{F} \to \mathbb{E}$ by $tr_{\mathbb{R}/\mathbb{E}}(a) = a + \sigma(a)$. Prove $Range(tr_{\mathbb{F}/\mathbb{E}}) = \mathbb{E}$.

9.2 Unitary Space

In this section we define the notion of a unitary space as well as an isometry between unitary spaces. We show that the set of all isometries from a unitary space to itself is a group. In our main theorem we prove Witt's theorem for non-degenerate unitary spaces.

What You Need to Know

To be successful in understanding the new material of this section, it is essential that you have already mastered the following concepts: vector space, basis of a vector space, dimension of a vector space, finite-dimensional vector space, linear transformation, coordinate vector with respect to a basis, matrix of a linear transformation, an algebra, determinant of a matrix or operator, semilinear transformation, sesquilinear form, Hermitian form, skew-Hermitian form, reflexive sesquilinear form, and the dual space of a vector space.

Let $\mathbb{F}$ be a field, σ an automorphism of $\mathbb{F}$ of order 2. For convenience we will write $\overline{a}$ for $\sigma(a)$ when $a \in \mathbb{F}$. We set $\mathbb{E} = \mathbb{F}^{\sigma} = \{a \in \mathbb{F} | \overline{a} = a\}$ so that the extension $\mathbb{E} \subset \mathbb{F}$ is a Galois extension of degree two. Let V be a vector space over $\mathbb{F}$. Recall a map $f : V \times V \to \mathbb{F}$ is said to be **σ-Hermitian** if

1) $f(a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2, \boldsymbol{w}) = a_1 f(\boldsymbol{v}_1, \boldsymbol{w}) + a_2 f(\boldsymbol{v}_2, \boldsymbol{w})$; and

2) $f(\boldsymbol{w}, \boldsymbol{v}) = \overline{f(\boldsymbol{v}, \boldsymbol{w})}$.

Also, f is σ skew-Hermitian if 1) holds as well as

2′) $f(\boldsymbol{w}, \boldsymbol{v}) = -f(\boldsymbol{v}, \boldsymbol{w})$.

Definition 9.11 *A* **unitary space** *is a pair (V, f) consisting of a finite-dimensional vector space V over $\mathbb{F}$ and a σ-Hermitian form f, for some automorphism of $\mathbb{F}$ satisfying $\sigma \neq I_{\mathbb{F}} = \sigma^2$.*

Definition 9.12 *Assume (V, f) is a unitary space. A non-zero vector $\boldsymbol{v}$ is* **isotropic** *if $f(\boldsymbol{v}, \boldsymbol{v}) = 0$. The space V is* **isotropic** *if there exist isotropic vectors in V. Otherwise the unitary space is* **anisotropic**.

Example 9.5 *If $(V, \langle\ ,\ \rangle)$ is a finite-dimensional complex inner product space, then it is an anisotropic unitary space.*

Definition 9.13 *Let (V, f) and (W, g) be unitary spaces over the field $\mathbb{F}$ with respect to the same automorphism σ. An* **isometry** *from V to W is a linear isomorphism $T : V \to W$ such that for all vectors $\boldsymbol{u}, \boldsymbol{v} \in V, g(T(\boldsymbol{u}), T(\boldsymbol{v})) = f(\boldsymbol{u}, \boldsymbol{v})$.*

Definition 9.14 *Let (V, f) be a non-degenerate unitary space. A sequence $\mathcal{S} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_m)$ such that $a_i = f(\boldsymbol{v}_i, \boldsymbol{v}_i) \neq 0$ for $1 \leq i \leq m$ and $f(\boldsymbol{v}_i, \boldsymbol{v}_j) = 0$ for $i \neq j$ is said to be* **orthogonal**. *If $\mathcal{S}$ is a basis of V, then it is referred to as an* **orthogonal basis**.

Lemma 9.10 *Let (V, f) be a non-degenerate unitary space and $\mathcal{S} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_m)$ be an orthogonal sequence. Then $\mathcal{S}$ is linearly independent.*

This is left as an exercise.

Lemma 9.11 *Let (V, f) be a non-degenerate unitary space, $\mathcal{S} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ an orthogonal basis, and T an operator on V. Set $\boldsymbol{w}_i = T(\boldsymbol{v}_i)$. Then T is an isometry if and only if $f(\boldsymbol{w}_i, \boldsymbol{w}_i) = f(\boldsymbol{v}_i, \boldsymbol{v}_i)$ for all $i, 1 \leq i \leq n$ and $f(\boldsymbol{w}_i, \boldsymbol{w}_j) = 0$ for all $i \neq j$.*

This is left as an exercise.

Lemma 9.12 *Assume (V, f) is a non-degenerate unitary space and assume T is an isometry. Then T is invertible, T^{-1} is an isometry, and the collection of all isometries is a subgroup of $GL(V)$.*

Proof *Let $\mathcal{B} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$. Set $\boldsymbol{w}_i = T(\boldsymbol{v}_i)$ and $\mathcal{B}' = (\boldsymbol{w}_1, \dots, \boldsymbol{w}_n)$. By Lemma (9.11) $\mathcal{B}'$ is an orthogonal basis and, consequently, T is invertible. On the other hand, $T^{-1}(\boldsymbol{w}_i) = \boldsymbol{v}_i$ and by the aforementioned lemma it follows that T^{-1} is an isometry.*

Clearly, the composition of isometries is an isometry and it then follows that the collection of all isometries is a subgroup of $GL(V)$.

Definition 9.15 *Let (V, f) be a non-degenerate unitary space. Denote by $U(V, f)$ the set $\{T \in \mathcal{L}(V, V) \; | f(T(\boldsymbol{v}), T(\boldsymbol{w})) = f(\boldsymbol{v}, \boldsymbol{w})$ for all $\boldsymbol{v} \in V\}$. This is referred to as the* **unitary group of** *(V, f). Often, when the f is understood, we will write $U(V)$ in place of $U(V, f)$.*

Definition 9.16 *Let (V, f) be a unitary space. A U a subspace of V is said to be* **non-degenerate** *if the restriction of f to $U \times U$ is non-degenerate. This means for every $\boldsymbol{u} \in U, \boldsymbol{u} \neq \boldsymbol{0}$, there is a vector $\boldsymbol{w} \in U$, such that $f(\boldsymbol{u}, \boldsymbol{w}) \neq 0$.*

Lemma 9.13 *Assume (V, f) is a non-degenerate unitary space, X is a non-degenerate subspace, and $\sigma : X \to X$ is an isometry. Define $S : V \to V$ as follows: If $\boldsymbol{v} = \boldsymbol{x} + \boldsymbol{y}$ where $\boldsymbol{x} \in X, \boldsymbol{y} \in X^{\perp}$ then $S(\boldsymbol{x} + \boldsymbol{y}) = \sigma(\boldsymbol{x}) + \boldsymbol{y}$. Then S is an isometry of V. Often, when the f is understood, we will write $U(V)$ in place of*

Proof *Let $\boldsymbol{x}_1, \boldsymbol{x}_2 \in X, \boldsymbol{y}_1, \boldsymbol{y}_2 \in X^{\perp}$. Then*

$$f(S(\boldsymbol{x}_1 + \boldsymbol{y}_1), S(\boldsymbol{x}_2 + \boldsymbol{y}_2)) = f(\sigma(\boldsymbol{x}_1) + \boldsymbol{y}_1, \sigma(\boldsymbol{x}_2)) + \boldsymbol{y}_2) =$$

$$f(\sigma(\boldsymbol{x}_1), \sigma(\boldsymbol{x}_2)) + f(\sigma(\boldsymbol{x}_1), \boldsymbol{y}_2) + f(\boldsymbol{y}_1, \sigma(\boldsymbol{x}_2)) + f(\boldsymbol{y}_1, \boldsymbol{y}_2)) =$$

$$f(\sigma(\boldsymbol{x}_1), \sigma(\boldsymbol{x}_2) + f(\boldsymbol{y}_1 + \boldsymbol{y}_2) = f(\boldsymbol{x}_1, \boldsymbol{x}_2) + f(\boldsymbol{y}_1 + \boldsymbol{y}_2) = f(\boldsymbol{x}_1 + \boldsymbol{y}_1, \boldsymbol{x}_2 + \boldsymbol{y}_2).$$

Lemma 9.14 *Assume (V, f) is a non-degenerate unitary space, $\boldsymbol{v}$ is an isotropic vector in V, and $\boldsymbol{u}$ is a vector satisfying $f(\boldsymbol{v}, \boldsymbol{u}) \neq 0$. Then there exists an isotropic vector $\boldsymbol{w} \in Span(\boldsymbol{v}, \boldsymbol{u})$ such that $f(\boldsymbol{v}, \boldsymbol{w}) = 1$.*

Proof *Set $c = f(\boldsymbol{v}, \boldsymbol{u})$. By replacing $\boldsymbol{u}$ with $\frac{1}{c}\boldsymbol{u}$ we can assume that $f(\boldsymbol{v}, \boldsymbol{u}) = 1$. If $\boldsymbol{u}$ is isotropic we are done; so assume $f(\boldsymbol{u}, \boldsymbol{u}) = d \neq 0$. Now $f(\boldsymbol{u}, \boldsymbol{u}) = \overline{f(\boldsymbol{u}, \boldsymbol{u})}$ so that $f(\boldsymbol{u}, \boldsymbol{u}) \in \mathbb{E} = \mathbb{F}^{\langle \sigma \rangle}$. By Exercise 8 of Section (9.1), there exists an element $a \in \mathbb{F}$ such that $a + \overline{a} + f(\boldsymbol{u}, \boldsymbol{u}) = 0$. Set $\boldsymbol{w} = a\boldsymbol{v} + \boldsymbol{u}$. Then $f(\boldsymbol{v}, \boldsymbol{w}) = f(\boldsymbol{v}, a\boldsymbol{v} + \boldsymbol{u}) = \overline{a}f(\boldsymbol{v}, \boldsymbol{v}) + f(\boldsymbol{v}, \boldsymbol{u}) = 1$. Also,*

$$\begin{aligned} f(\boldsymbol{w}, \boldsymbol{w}) &= f(a\boldsymbol{v} + \boldsymbol{u}, a\boldsymbol{v} + \boldsymbol{u}) \\ &= a\overline{a}f(\boldsymbol{v}, \boldsymbol{v}) + af(\boldsymbol{v}, \boldsymbol{u}) + \overline{a}f(\boldsymbol{u}, \boldsymbol{v}) + f(\boldsymbol{u}, \boldsymbol{u}) \\ &= a + \overline{a} + f(\boldsymbol{u}, \boldsymbol{u}) \\ &= 0. \end{aligned}$$

Definition 9.17 *Let (V, f) be a unitary space. A pair of vectors $(\boldsymbol{v}, \boldsymbol{w})$ such that $f(\boldsymbol{v}, \boldsymbol{v}) = f(\boldsymbol{w}, \boldsymbol{w}) = 0, f(\boldsymbol{v}, \boldsymbol{w}) = 1$ is a* **hyperbolic pair**.

Corollary 9.3 *Assume (V, f) is a non-degenerate isotropic unitary space and $\boldsymbol{v} \in V$ is isotropic. Then there exists $\boldsymbol{w}$, an isotropic vector such that $(\boldsymbol{v}, \boldsymbol{w})$ is a hyperbolic pair.*

This is left as an exercise.

Lemma 9.15 *Assume (V, f) is a two dimensional non-degenerate isotropic unitary space. Assume $(\boldsymbol{v}_1, \boldsymbol{w}_1)$ and $(\boldsymbol{v}_2, \boldsymbol{w}_2)$ are hyperbolic pairs. Define the operator T on V by $T(a\boldsymbol{v}_1 + b\boldsymbol{w}_1) = a\boldsymbol{v}_2 + b\boldsymbol{w}_2$. Then T is an isometry.*

This is left as an exercise.

Lemma 9.16 *Assume (V, f) is an non-degenerate isotropic unitary space and $\boldsymbol{v}, \boldsymbol{u}$ are isotropic vectors. Then there exists an isometry T such that $T(\boldsymbol{v}) = \boldsymbol{u}$.*

Proof *First, assume that $\boldsymbol{u} = a\boldsymbol{v}$ for some $a \in \mathbb{F}$. Let $\boldsymbol{w}$ be an isotropic vector such that $(\boldsymbol{v}, \boldsymbol{w})$ is a hyperbolic pair. Then $(a\boldsymbol{v}, \frac{1}{\overline{a}}\boldsymbol{w})$ is also a hyperbolic pair. By Lemma (9.15), the map T such that $T(\boldsymbol{v}) = a\boldsymbol{v}, T(\boldsymbol{w}) = \frac{1}{\overline{a}}\boldsymbol{w}$ and $T(\boldsymbol{x}) = \boldsymbol{x}$ for $\boldsymbol{x} \in Span(\boldsymbol{v}, \boldsymbol{w})^\perp$ is an isometry. Next, assume that $f(\boldsymbol{v}, \boldsymbol{u}) \neq 0$. If $f(\boldsymbol{v}, \boldsymbol{u}) = 1$, then the map T such that $T(\boldsymbol{v}) = \boldsymbol{u}, T(\boldsymbol{u}) = \boldsymbol{v}$, and $T(\boldsymbol{x}) = \boldsymbol{x}$ for $\boldsymbol{x} \in Span(\boldsymbol{u}, \boldsymbol{v})^\perp$ is an isometry by the aforementioned lemma. Suppose then that $f(\boldsymbol{v}, \boldsymbol{u}) = c \neq 0$. Then. by what we have just proved, there is an isometry which takes $\boldsymbol{v}$ to $\frac{1}{\overline{c}}\boldsymbol{u}$. By the first case, there is an isometry which takes $\frac{1}{\overline{c}}\boldsymbol{u}$ to $\boldsymbol{u}$. Composing yields an isometry taking $\boldsymbol{v}$ to $\boldsymbol{u}$. Thus, we may assume that $(\boldsymbol{v}, \boldsymbol{u})$ is linearly independent and $\boldsymbol{u} \perp \boldsymbol{v}$.*

By Lemma (9.14), there exists an isotropic vector $\boldsymbol{x}$ such that $(\boldsymbol{v}, \boldsymbol{x})$ is a hyperbolic pair and there is an isometry T with $T(\boldsymbol{v}) = \boldsymbol{x}$. If $f(\boldsymbol{x}, \boldsymbol{u}) \neq 0$ then there is an isometry S such that $S(\boldsymbol{x}) = \boldsymbol{u}$. Then the composition ST takes $\boldsymbol{v}$ to $\boldsymbol{u}$. Thus, we may assume that $f(\boldsymbol{x}, \boldsymbol{u}) = 0$. By the above argument there exists an isotropic vector $\boldsymbol{y}$ such that $(\boldsymbol{y}, \boldsymbol{u})$ is a hyperbolic pair and therefore an isometry taking $\boldsymbol{y}$ to $\boldsymbol{u}$. If $f(\boldsymbol{v}, \boldsymbol{y}) \neq 0$, then we are done by the above arguments, so we may assume that $f(\boldsymbol{v}, \boldsymbol{y}) = 0$. If $f(\boldsymbol{x}, \boldsymbol{y}) \neq 0$ then there are isometries T_1, T_2, T_3 such that $T_1(\boldsymbol{v}) = \boldsymbol{x}, T_2(\boldsymbol{x}) = \boldsymbol{y}, T_3(\boldsymbol{y}) = \boldsymbol{u}$ and the composition $T_3T_2T_1$ is the desired isometry taking $\boldsymbol{v}$ to $\boldsymbol{u}$. Thus, we may assume that $f(\boldsymbol{x}, \boldsymbol{y}) = 0$. But now $\boldsymbol{z} = \boldsymbol{x} + \boldsymbol{y}$ is isotropic and $f(\boldsymbol{v}, \boldsymbol{z}) \neq 0 \neq f(\boldsymbol{z}, \boldsymbol{u})$ and we are done.

For the remainder of this section we will assume that (V, f) is a non-degenerate unitary space. Our main objective is to prove Witt's Extension theorem. This will imply that the unitary group $U(V, f)$ has lots of transitivity on subspaces.

Definition 9.18 *Let (V, f) be a unitary space with subspcaes X and Y. We say that an isomorphism σ from X to Y is an isometry if $f(\sigma(\boldsymbol{x}_1), \sigma(\boldsymbol{x}_2)) = f(\boldsymbol{x}_1, \boldsymbol{x}_2)$.*

Theorem 9.3 *Assume X and Y are subspaces of the non-degenerate unitary space (V, f) and $\tau : X \to Y$ is an isometry. Then there exists an isometry $T : V \to V$ such that $T_{|X} = \tau$.*

Proof *Case 1) First assume $X \cap Y$ is a hyperplane of X (and therefore Y) and that τ restricted to $U = X \cap Y$ is the identity. Set $W = \{\tau(\boldsymbol{z}) - \boldsymbol{z} | \boldsymbol{z} \in X\}$ so that dim$(W) = 1$ and let $\boldsymbol{x}$ be chosen from X such that $\boldsymbol{w} = \tau(\boldsymbol{x}) - \boldsymbol{x}$ spans W. We also set $\boldsymbol{y} = \tau(\boldsymbol{x})$. We treat separately the two subcases: a) $X \nsubseteq \boldsymbol{w}^\perp$ and b) $X \subseteq \boldsymbol{w}^\perp$.*

a) Suppose $\boldsymbol{u} \in U$. We claim that $f(\boldsymbol{u}, \boldsymbol{w}) = 0$:

$$\begin{aligned} f(\boldsymbol{u}, \boldsymbol{w}) &= f(\boldsymbol{u}, \tau(\boldsymbol{x}) - \boldsymbol{x}) \\ &= f(\boldsymbol{u}, \tau(\boldsymbol{x})) - f(\boldsymbol{u}, \boldsymbol{x}) \\ &= f(\tau(\boldsymbol{u}), \tau(\boldsymbol{x})) - f(\boldsymbol{u}, \boldsymbol{x}) \\ &= f(\boldsymbol{u}, \boldsymbol{x}) - f(\boldsymbol{u}, \boldsymbol{x}) \\ &= 0. \end{aligned}$$

Since U is a hyperplane of X it follows that $X \cap \boldsymbol{w}^\perp = U$. We next show that $\boldsymbol{y} = \tau(\boldsymbol{x}) \notin \boldsymbol{w}^\perp$.

$$\begin{aligned} f(\boldsymbol{y}, \boldsymbol{w}) &= f(\tau(\boldsymbol{x}), \boldsymbol{w}) \\ &= f(\tau(\boldsymbol{x}), \boldsymbol{w}) \\ &= f(\tau(\boldsymbol{x}), \tau(\boldsymbol{x}) - \boldsymbol{x}) \\ &= f(\tau(\boldsymbol{x}), \tau(\boldsymbol{x})) - f(\tau(\boldsymbol{x}), \boldsymbol{x}) \\ &= f(\boldsymbol{x}, \boldsymbol{x}) - f(\tau(\boldsymbol{x}), \boldsymbol{x}) \\ &= f(\boldsymbol{x} - \tau(\boldsymbol{x}), \boldsymbol{x}) \\ &= f(-\boldsymbol{w}, \boldsymbol{x}) \\ &\neq 0. \end{aligned}$$

Consequently, $Y = \tau(X)$ is not contained in $\boldsymbol{w}^\perp$. Then $Y \cap \boldsymbol{w}^\perp$ is a hyperplane of Y. Since U is a hyperplane of Y contained in $\boldsymbol{w}^\perp$ it follows that $Y \cap \boldsymbol{w}^\perp = U$. Choose a subspace Z so that $\boldsymbol{w}^\perp = U \oplus Z$. Since $U \subset X$, we have $\boldsymbol{w}^\perp = U \oplus Z \subset X + Z$. Since $Z \subset \boldsymbol{w}^\perp$ it follows that

$$\begin{aligned} X \cap Z &= (X \cap \boldsymbol{w}^\perp) \cap Z \\ &= U \cap X = \{\boldsymbol{0}\}. \end{aligned}$$

In exactly the same way, $Y \cap Z = \{\boldsymbol{0}\}$. We claim that $X \oplus Z = Y \oplus Z = V$. Now $X \oplus Z$ contains $U \oplus Z = \boldsymbol{w}^\perp$. However, since X is not contained in $\boldsymbol{w}^\perp$ it follows that $\boldsymbol{w}^\perp$ is properly contained in $X \oplus Z$. Since $\boldsymbol{w}^\perp$ is a hyperplane of V we can conclude that $X \oplus Z$. In exactly the same way, $Y \oplus Z = V$.

Suppose now that $\boldsymbol{x}' \in X$ and $\boldsymbol{z} \in Z$. Then $\tau(\boldsymbol{x}') - \boldsymbol{x}' \in W \subset Z^\perp$ and *therefore* $f(\tau(\boldsymbol{x}') - \boldsymbol{x}', \boldsymbol{z}) = 0$*, equivalently,* $f(\tau(\boldsymbol{x}'), \boldsymbol{z}) = f(\boldsymbol{x}', \boldsymbol{z})$*. Thus,* $f(\boldsymbol{z}, \boldsymbol{x}') = f(\boldsymbol{z}, \tau(\boldsymbol{x}'))$*. Assume now that* $\boldsymbol{v}$ *is arbitrary in* V*. We can write* $\boldsymbol{v} = \boldsymbol{x}' + \boldsymbol{z}$ *for unique vectors* $\boldsymbol{x}' \in X$ *and* $\boldsymbol{z} \in Z$*. Now set* $T(\boldsymbol{v}) = \tau(\boldsymbol{x}') + \boldsymbol{z}$*. We claim that* T *is an isometry which extends* τ*. Thus, suppose* $\boldsymbol{v}_1 = \boldsymbol{x}_1 + \boldsymbol{z}_1$ *and* $\boldsymbol{v}_2 = \boldsymbol{x}_2 + \boldsymbol{z}_2$ *are two arbitrary vectors in* V *with* $\boldsymbol{x}_1, \boldsymbol{x}_2 \in X, \boldsymbol{z}_1, \boldsymbol{z}_2 \in Z$*.*

$$\begin{aligned}
f(T(\boldsymbol{v}_1), T(\boldsymbol{v}_2)) &= f(T(\boldsymbol{x}_1 + \boldsymbol{z}_1), T(\boldsymbol{x}_2 + \boldsymbol{z}_2)) \\
&= f(\tau(\boldsymbol{x}_1) + \boldsymbol{z}_1, \tau(\boldsymbol{x}_2) + \boldsymbol{z}_2) \\
&= f(\tau(\boldsymbol{x}_1), \tau(\boldsymbol{x}_2)) + f(\tau(\boldsymbol{x}_1), \boldsymbol{z}_2) + f(\boldsymbol{z}_1, \tau(\boldsymbol{x}_2)) + f(\boldsymbol{z}_1, \boldsymbol{z}_2) \\
&= f(\boldsymbol{x}_1, \boldsymbol{x}_2) + f(\boldsymbol{x}_1, \boldsymbol{z}_2) + f(\boldsymbol{z}_1, \boldsymbol{x}_2) \\
&= f(\boldsymbol{x}_1 + \boldsymbol{z}_1, \boldsymbol{x}_2 + \boldsymbol{z}_2) \\
&= f(\boldsymbol{v}_1, \boldsymbol{v}_2).
\end{aligned}$$

Thus, T *is an isometry.*

b. Now assume that $X \subset \boldsymbol{w}^\perp$*. Then, of course,* $U \subset \boldsymbol{w}^\perp$*. We claim that* $Y \subset \boldsymbol{w}^\perp$*. Since* U *is a hyperplane of* Y *contained in* Y*, it suffices to prove that* $\boldsymbol{y} \in \boldsymbol{w}^\perp$*.*

$$\begin{aligned}
f(\boldsymbol{w}, \boldsymbol{y}) &= f(\boldsymbol{y} - \boldsymbol{x}, \boldsymbol{y}) \\
&= f(\boldsymbol{y}, \boldsymbol{y}) - f(\boldsymbol{x}, \boldsymbol{y}) \\
&= f(\tau(\boldsymbol{x}), \tau(\boldsymbol{x})) - f(\boldsymbol{x}, \boldsymbol{y}) \\
&= f(\boldsymbol{x}, \boldsymbol{x}) - f(\boldsymbol{x}, \boldsymbol{y}) \\
&= f(\boldsymbol{x}, \boldsymbol{x} - \boldsymbol{y}) \\
&= f(\boldsymbol{x}, -\boldsymbol{w}) \\
&= 0.
\end{aligned}$$

In the above we have used the fact that $f(\boldsymbol{y}, \boldsymbol{y}) = f(\tau(\boldsymbol{x}), \tau(\boldsymbol{x})) = f(\boldsymbol{x}, \boldsymbol{x})$ *since* τ *is an isometry. We she also made use of the fact that* $-\boldsymbol{w} = x - \tau(\boldsymbol{x}) = \boldsymbol{x} - \boldsymbol{y}$*.*

It now follows that $\boldsymbol{w}$ *is isotropic since*

$$\begin{aligned}
f(\boldsymbol{w}, \boldsymbol{w}) &= f(\boldsymbol{w}, \boldsymbol{y} - \boldsymbol{x}) \\
&= f(\boldsymbol{w}, \boldsymbol{x}) - f(\boldsymbol{w}, \boldsymbol{y}) \\
&= 0.
\end{aligned}$$

Thus, $\boldsymbol{w} \in \boldsymbol{w}^\perp$*. By Exercise 14 of Section (1.6), there exists a subspace* Z *such that* $\boldsymbol{w}^\perp = X \oplus Z = Y \oplus Z$*. Let* γ *be the operator on* $\boldsymbol{w}^\perp$ *such that* $\gamma_{|X} = \tau$ *and* $\gamma_{|Z}$ *is the identity map on* Z*. We claim that this is an isometry of* $\boldsymbol{w}^\perp$*. A typical element of* $\boldsymbol{w}^\perp$ *can be written as* $a\boldsymbol{x} + \boldsymbol{v}$ *where* $\boldsymbol{v} \in U \oplus Z$*.*

For such an element, $\gamma(a\boldsymbol{x}+\boldsymbol{v}) = a\boldsymbol{y}+\boldsymbol{v}$. *We show that this is an isometry: Let* $a_1, a_2 \in \mathbb{F}, \boldsymbol{v}_1, \boldsymbol{v}_2 \in U \oplus Z$. *Since* $\boldsymbol{v}_i \in \boldsymbol{w}^{\perp}$ *for* $i = 1, 2$ *and* $\boldsymbol{w} = \boldsymbol{y} - \boldsymbol{x}$ *it follows that* $f(\boldsymbol{y}, \boldsymbol{v}_i) = f(\boldsymbol{x}, \boldsymbol{v}_i)$ *for* $i = 1, 2$. *We then have*

$$\begin{aligned} f(a_1\boldsymbol{y}+\boldsymbol{v}_1, a_2\boldsymbol{y}+\boldsymbol{v}_2) &= a_1\overline{a_2}f(\boldsymbol{y},\boldsymbol{y}) + a_1 f(\boldsymbol{y},\boldsymbol{v}_2) + \overline{a_2}f(\boldsymbol{v}_1,\boldsymbol{y}) + f(\boldsymbol{v}_1,\boldsymbol{v}_2) \\ &= a_1\overline{a_2}f(\boldsymbol{x},\boldsymbol{x}) + a_1 f(\boldsymbol{x},\boldsymbol{v}_2) + \overline{a_2}f(\boldsymbol{v}_1,\boldsymbol{x}) + f(\boldsymbol{v}_1,\boldsymbol{v}_2) \\ &= f(a_1\boldsymbol{x}+\boldsymbol{v}_1, a_2\boldsymbol{x}+\boldsymbol{v}_2). \end{aligned}$$

It remains to show that we can extend γ *to an isometry of* V. *We have therefore reduced to the case where* $X = Y = \boldsymbol{w}^{\perp}$, τ *acts as the identity on a hyperplane* U *of* $\boldsymbol{w}^{\perp}$ *and for some* $\boldsymbol{x} \in X \setminus U, \boldsymbol{w} = \tau(\boldsymbol{x}) - \boldsymbol{x}$. *Also, if we set* $\boldsymbol{y} = \tau(\boldsymbol{x})$ *then* $X = Span(\boldsymbol{y}) \oplus U$.

Now choose any element $\boldsymbol{v}_1 \in V, \boldsymbol{v}_1 \notin X = \boldsymbol{w}^{\perp}$. *Define* $F \in \mathcal{L}(V, \mathbb{F})$ *such that* $F(\boldsymbol{t}) = f(\tau^{-1}(\boldsymbol{t}), \boldsymbol{v}_1)$ *if* $\boldsymbol{t} \in \boldsymbol{w}^{\perp}$ *and such that* $F(\boldsymbol{v}_1) = 0$. *Since* f *is non-degenerate, by Lemma (9.5), there exists a vector* $\boldsymbol{v}_2$ *such that* $F(\boldsymbol{v}') = f(\boldsymbol{v}', \boldsymbol{v}_2)$ *for every vector* $\boldsymbol{v}' \in V$. *Then, for every vector* $\boldsymbol{v}' \in X = \boldsymbol{w}^{\perp}, f(\tau^{-1}(\boldsymbol{v}'), \boldsymbol{v}_1) = f(\boldsymbol{v}', \boldsymbol{v}_2)$. *Consequently,* $f(\boldsymbol{v}', \boldsymbol{v}_1) = f(\tau(\boldsymbol{v}'), \boldsymbol{v}_2)$ *for every* $\boldsymbol{v}' \in X = \boldsymbol{w}^{\perp}$. *If* $f(\boldsymbol{v}_1, \boldsymbol{v}_1) = f(\boldsymbol{v}_2, \boldsymbol{v}_2)$ *then we can extend* τ *to* T *by defining* $T(\boldsymbol{v}_1) = \boldsymbol{v}_2$. *Consider the element* $\boldsymbol{v}_3 = \boldsymbol{v}_2 + a\boldsymbol{w}$. *This element is not in* $\boldsymbol{w}^{\perp}$ *since* $f(\boldsymbol{v}_3, \boldsymbol{w}) = f(\boldsymbol{v}_2 + a\boldsymbol{w}, \boldsymbol{w}) = af(\boldsymbol{v}_2, \boldsymbol{w}) + af(\boldsymbol{w}, \boldsymbol{w}) = f(\boldsymbol{v}_2, \boldsymbol{w}) \neq 0$. *We now compute* $f(\boldsymbol{v}_3, \boldsymbol{v}_3)$:

$$\begin{aligned} f(\boldsymbol{v}_3,\boldsymbol{v}_3) &= f(\boldsymbol{v}_2+a\boldsymbol{w}, \boldsymbol{v}_2+a\boldsymbol{w}) \\ &= f(\boldsymbol{v}_2,\boldsymbol{v}_2) + \overline{a}f(\boldsymbol{v}_2,\boldsymbol{w}) + af(\boldsymbol{w},\boldsymbol{v}_2) + a\overline{a}f(\boldsymbol{w},\boldsymbol{w}) \\ &= f(\boldsymbol{v}_2,\boldsymbol{v}_2) + \overline{a}f(\boldsymbol{v}_2,\boldsymbol{w}) + af(\boldsymbol{w},\boldsymbol{v}_2). \end{aligned}$$

By Exercise 8 of Section (9.1), there is an element $b \in \mathbb{F}$ *such that* $b + \overline{b} = f(\boldsymbol{v}_1, \boldsymbol{v}_1) - f(\boldsymbol{v}_2, \boldsymbol{v}_2)$. *Set* $a = \frac{b}{f(\boldsymbol{w}, \boldsymbol{v}_2)}$. *With this choice of* a *we get*

$$\begin{aligned} f(\boldsymbol{v}_2+a\boldsymbol{w}, \boldsymbol{v}_2+a\boldsymbol{w}) &= f(\boldsymbol{v}_2,\boldsymbol{v}_2) + \overline{a}f(\boldsymbol{v}_2,\boldsymbol{w}) + af(\boldsymbol{w},\boldsymbol{v}_2) \\ &= f(\boldsymbol{v}_2,\boldsymbol{v}_2) + \frac{\overline{b}}{\overline{f(\boldsymbol{w},\boldsymbol{v}_2)}}f(\boldsymbol{v}_2,\boldsymbol{w}) + \frac{b}{f(\boldsymbol{w},\boldsymbol{v}_2)}f(\boldsymbol{w},\boldsymbol{v}_2) \\ &= f(\boldsymbol{v}_2,\boldsymbol{v}_2) + \frac{\overline{b}}{\overline{f(\boldsymbol{w},\boldsymbol{v}_2)}}\overline{f(\boldsymbol{w},\boldsymbol{v}_2)} + \frac{b}{f(\boldsymbol{w},\boldsymbol{v}_2)}f(\boldsymbol{w},\boldsymbol{v}_2) \\ &= f(\boldsymbol{v}_2,\boldsymbol{v}_2) + \overline{b} + b \\ &= f(\boldsymbol{v}_2,\boldsymbol{v}_2) + f(\boldsymbol{v}_1,\boldsymbol{v}_1) - f(\boldsymbol{v}_2,\boldsymbol{v}_2) \\ &= f(\boldsymbol{v}_1,\boldsymbol{v}_1). \end{aligned}$$

We can now extend τ *to* $T : V \to V$ *by defining* $T(\boldsymbol{v}_1) = \boldsymbol{v}_3$.

Case 2) We now do the general case. We proceed by mathematical induction on $k = dim(X)$. If $k = 1$ then we are in case 1. So assume the result holds for all isometries $\tau : X \to Y$ where $dim(Z) = k - 1 \geq 1$ and that $dim(X) = k$. Choose a hyperplane X_0 of X and set $Y_0 = \tau(X_0)$. By the inductive hypothesis there exists an isometry R of V such that $R_{|X_0} = \tau_{|X_0}$. Set $\rho = R^{-1}\tau$. Now ρ is an isometry of X and ρ restricted to X_0 is the identity. Now by case 1 there is an isometry S of V such that S restricted to X is ρ. Set $T = RS$. This is the desired isometry of V.

As corollaries we have the following:

Corollary 9.4 *Let (V, f) be a finite-dimensional non-degenerate isotropic unitary space. Let U_1, U_2 be maximal totally isotropic subspaces of V. Then $dim(U_1) = dim(U_2)$.*

This is left as an exercise.

Definition 9.19 *Let (V, f) be a finite-dimensional non-degenerate isotropic unitary space. The dimension of a maximal totally isotropic subspace of V is the* **Witt index** *of V.*

Corollary 9.5 *Let (V, f) be a finite-dimensional non-degenerate isotropic unitary space. Assume U_1 and U_2 are isometric subspaces of V. Then $U_1^\perp$ and $U_2^\perp$ are isometric.*

This is an exercise.

Exercises

1. Prove Lemma (9.10).

2. Prove Lemma (9.11).

3. Prove Corollary (9.3).

4.Prove Lemma (9.15).

5. Prove Corollary (9.4).

6. Prove Corollary (9.5).

7. Let (V, f) be a non-degenerate unitary space of dimension two over the field $\mathbb{F}$ and let $\mathbb{E}$ denote the fixed field of the automorphism $\sigma, \mathbb{E} = \{a \in \mathbb{F} \mid \sigma(a) = \overline{a} = a\}$. Define the norm of an element of $\mathbb{E}$ by $\parallel a \parallel = a\overline{a}$. Assume that the norm is surjective. Prove that (V, f) is isotropic and spanned by a hyperbolic pair.

8. Continue with the hypotheses on $\mathbb{F}, \mathbb{E}$, and the norm map $N : \mathbb{F} \to \mathbb{E}$.

Assume that (V, f) is a non-degenerate unitary space of dimension n. Prove that the Witt index of V is $\lfloor \frac{n}{2} \rfloor$.

9. Let (V, f) be a finite-dimensional non-degenerate isotropic unitary space over the field $\mathbb{F}$. Prove that V has a basis of isotropic vectors.

10. Let (V, f) be a finite-dimensional, non-degenerate unitary space. Prove that there exists an orthogonal basis for V.

11. Assume $\mathbb{E} \subset \mathbb{F}$ is a Galois extension of degree two with Galois group generated by σ. Denote images under σ with the bar notation. Assume that the norm map from $\mathbb{F}$ to $\mathbb{E}$ given by $N(a) = a\overline{a}$ is surjective. Assume (V, f) is a non-degenerate unitary space of dimension two over $\mathbb{F}$. Prove that (V, f) is isotropic.

This page intentionally left blank

10

Tensor Products

CONTENTS

This chapter is devoted to tensor products of vector spaces and related topics such as the symmetric and exterior algebras. The term, tensor product, arises from its applications in differential geometry where it may be applied to the tangent or cotangent space of a manifold, but its utility is ubiquitous throughout mathematics. For example, in group theory, the tensor product is used to construct group representations. In other algebraic contexts, the tensor product is used to extend the base field of a vector space, for example, from the field of real numbers to the field of complex numbers.

In the first section, we define the tensor product of vector spaces as the solution to a certain universal mapping problem and prove that it exists. In the second section, we make use of the definition of the tensor product to prove some "functorial" properties, such as how the tensor product behaves with respect to direct sums. We show how a tensor product of linear transformations can be defined to obtain a transformation from one tensor product to another. Finally, we investigate how to compute the matrix of a tensor product of transformations from the matrices of those transformations. In section three, we use the tensor product to construct a universal associative algebra for a given vector space V, the tensor algebra of V. In section four we introduce the notion of a $\mathbb{Z}$-graded algebra and related concepts such as a homogeneous ideal. We apply these ideas to the tensor algebra and construct the symmetric algebra of a vector space as the quotient space of the tensor algebra by a particular homogeneous ideal. We show that the symmetric algebra of an n-dimensional vector space over a field $\mathbb{F}$ is isomorphic to the algebra of polynomials in n commuting variables. We also show that the symmetric algebra is a solution to a universal mapping problem. In section five we construct the exterior algebra of a vector space V as the quotient of the tensor algebra of

V by a homogeneous ideal. We determine the dimension of this algebra as well as the dimensions of its homogeneous parts. We will further show how a linear transformation from a vector space V to a vector space W induces a linear transformation on the exterior algebra and its homogeneous pieces. In the final section we introduce the notion of a Clifford algebra of an orthogonal space (V, ϕ) and, making use of the tenor algebra of V, show that it exists.

10.1 Introduction to Tensor Products

In this section we define the tensor product of two or more vector spaces over a field $\mathbb{F}$ and prove its existence and uniqueness (up to isomorphism).

What You Need to Know

To be successful in understanding the new material of this section, it is essential that you have already mastered the following concepts: vector space, basis of a vector space, dimension of a vector space, finite-dimensional vector space, linear transformation, coordinate vector with respect to a basis, matrix of a linear transformation, an algebra over a field, multilinear map, multilinear form, bilinear map, bilinear form, quotient space defined by a subspace U of a vector space V, cosets of a subspace U contained in a vector space V.

The tensor product will be the solution to what is known as a ***universal mapping problem***. It is difficult to give even an informal definition without introducing category theory and so various examples will have to suffice. The following is a simple example which illustrates what is going on.

Definition 10.1 *Fix a field* $\mathbb{F}$ *and let* X *be any set. A vector space* V *over* $\mathbb{F}$ *is said to be* **based on** X *if there is a map* $i : X \to V$ *such that, whenever there is a map* $j : X \to W$*, where* W *is a vector space over* $\mathbb{F}$*, then there exists a unique linear transformation* $T : V \to W$ *such that* $j = T \circ i$*.*

This universal mapping problem is represented by diagrams such as the those in Figures (10.1) and (10.2). The first shows the initial conditions: the maps from X to V and W. The second shows the linear map from V to W. It is understood that the second diagram "commutes" which means that whichever path you take from X to W, directly via j or indirectly by first going to V via i and then to W via the linear map T, the result is the same, that is, $j = T \circ i$.

$$\begin{tikzcd} X \arrow[r, "i"] \arrow[dr, "j"'] & V \\ & W \end{tikzcd}$$

FIGURE 10.1
Initial condition: Vector space based on the set X

$$\begin{tikzcd}
X \arrow[r, "i"] \arrow[dr, "j"'] & V \arrow[d, "T"] \\
 & W
\end{tikzcd}$$

FIGURE 10.2
Solution: Vector space based on the set X

A solution to this particular problem will consist of any vector space V which has a basis $\mathcal{B}$ with the same cardinality as X. Then the map i can be taken to be any bijection between X and $\mathcal{B}$. However, how do we know that such a vector space exists? Since we will need this for the construction of the tensor product, we give a formal construction.

Recall by $\mathcal{M}_{fin}(X,\mathbb{F})$ we mean the set of all functions $f : X \to \mathbb{F}$ such that the support of f is finite. Here the ***support*** of f, denoted by $spt(f)$, consists of those elements in X such that $f(x) \neq 0$. Thus, set $V = \mathcal{M}_{fin}(X,\mathbb{F})$. For $x \in X$, let χ_x be the map from X to $\mathbb{F}$ such that $\chi_x(y) = 1$ if $y = x$ and 0 otherwise. Finally, define $i : X \to V$ by $i(x) = \chi_x$. Our first claim is the $\mathcal{B} = \{\chi_x | x \in X\}$ is a basis of V.

Suppose that $\{x_1, \dots, x_n\}$ is a finite subset of X, $c_1, \dots, c_n$ are scalars and $f = c_1\chi_{x_1} + \dots c_n\chi_{x_n} = \mathbf{0}$, the zero function. Evaluating f at x_i we get $0 = f(x_i) = c_i\chi_{x_i}(x_i) = c_i$. Thus, each $c_i = 0$ and $\mathcal{B}$ is linearly independent.

On the other hand, suppose $f \in V, f \neq \mathbf{0}$. Let $spt(f) = \{x_1, \dots, x_n\}$ and $f(x_i) = c_i$. Set $g = c_1\chi_{x_1} + \dots + c_n\chi_{x_n}$. If $x \in X \setminus \{x_1, \dots, x_n\}$ then $f(x) = g(x) = 0$. On the other hand, $g(x_i) = \sum_{j=1}^n c_j\chi_{x_j}(x_i) = c_i = f(x_i)$. Thus, $f = g$, a linear combination of $\mathcal{B}$.

Finally, we claim that (V, i) is a vector space over $\mathbb{F}$ based on X. So assume W is a vector space over $\mathbb{F}$ and $j : X \to W$ is any map. We need to prove that there is a unique linear map $T : V \to W$ such that $T \circ i = j$. Well, we can define a map $\tau : \mathcal{B} \to W$ by $\tau(\chi_x) = j(x)$. Since $\mathcal{B}$ is a basis of V by Theorem (2.7), there is a unique linear map $T : V \to W$ such that T restricted to $\mathcal{B}$ is τ. It then follows that $(T \circ i)(x) = T(\chi_x) = \tau(\chi_x) = j(x)$ as required.

Similar problems will define the tensor product, but before we get to that, we recall an essential definition:

Let $V_1, \dots, V_m, W$ be vector spaces over a field $\mathbb{F}$. A map $f : V_1 \times \dots \times V_m \to W$ is m-multilinear, or just multilinear, if the function obtained from V_i to W, when all the other arguments are fixed, is a linear transformation. That is, for $\boldsymbol{v}_1 \in V_1, \dots, \boldsymbol{v}_{i-1} \in V_{i-1}, \boldsymbol{v}_{i+1} \in V_{i+1}, \dots, \boldsymbol{v}_m \in V_m, \boldsymbol{v}_i, \boldsymbol{v}_i' \in V_i$ and scalars c, c' we have

$$f(\boldsymbol{v}_1, \dots, \boldsymbol{v}_{i-1}, c\boldsymbol{v}_i + c'\boldsymbol{v}_i', \boldsymbol{v}_{i+1}, \dots, \boldsymbol{v}_m)$$

$$= cf(\boldsymbol{v}_1, \dots, \boldsymbol{v}_{i-1}, \boldsymbol{v}_i, \boldsymbol{v}_{i+1}, \dots, \boldsymbol{v}_m) + c'(\boldsymbol{v}_1, \dots, \boldsymbol{v}_{i-1}, \boldsymbol{v}_i', \boldsymbol{v}_{i+1}, \dots, \boldsymbol{v}_m).$$

Definition 10.2 *Let $V_1, \dots, V_m$ be vector spaces over a field $\mathbb{F}$. A pair (V, γ) consisting of a vector space V over $\mathbb{F}$ and a multilinear map $\gamma : V_1 \times \cdots \times V_m \to V$ is a* **tensor product** *of $V_1, \dots, V_m$ over $\mathbb{F}$ if, whenever W is a vector space over $\mathbb{F}$ and $f : V_1 \times \cdots \times V_m \to W$ is a multilinear map, then there exists a unique linear map $T : V \to W$ such that $T \circ \gamma = f$.*

Remark 10.1 *Let $V_1, \dots, V_m$ be vector spaces over $\mathbb{F}$ and suppose (V, γ) is a tensor product of $V_1, \dots, V_m$ over $\mathbb{F}$. Since $\gamma : V_1 \times \cdots \times V_m \to V$ is a multilinear map, it is a consequence of the fact that (V, γ) is a tensor product that there is a unique linear map $S : V \to V$ such that $S \circ \gamma = \gamma$. Since, in fact, $I_V \circ \gamma = \gamma$ it follows that $S = I_V$.*

Notation Hereafter, when $f : X \to Y$ and $g : Y \to Z$ are functions, we will write gf for the composition $g \circ f$ unless that latter is required for clarity.

Before we give the construction and prove the existence of the tensor product we first show that it is essentially unique (up to isomorphism).

Lemma 10.1 *Let $V_1, \dots, V_m$ be vector spaces over the field $\mathbb{F}$ and assume that (V, γ) and (Z, δ) are tensor products of $V_1, \dots, V_m$ over $\mathbb{F}$. Then there exist unique maps $T : V \to Z$ and $S : Z \to V$ satisfying the following:*

i) $ST = I_V$ and $TS = I_Z$; and

ii) $T\gamma = \delta, S\delta = T$.

Proof *Since (V, γ) is a tensor product of $V_1, \dots, V_m$ over $\mathbb{F}$ and δ is a multilinear map from $V_1, \dots, V_m$ to Z, there exists a unique linear map $T : V \to Z$ such that $T\gamma = \delta$. In exactly the same way, there exists a unique linear map $S : Z \to V$ such that $S\delta = \gamma$. It then follows that $\gamma = S\delta = S(T\gamma) = (ST)\gamma$. By Remark (10.1), we have $ST = I_V$. In exactly the same way, $TS = I_Z$.*

As a consequence of Lemma (10.1), we can speak of *the* tensor product of vector spaces $V_1, \dots, V_m$.

We now proceed to the general construction which makes use of quotient spaces and cosets of a subspace U of a vector space V. The main idea is to create a very large vector space, one with basis the set $V_1 \times \cdots \times V_m$ and then to take the quotient of this by a subspace that is created to take into account the desired multilinearity.

Theorem 10.1 *Let $V_1, \dots, V_m$ be vector spaces over the field $\mathbb{F}$. Then the tensor product of $V_1, \dots, V_m$ over $\mathbb{F}$ exists.*

Proof *Set $X = V_1 \times \cdots \times V_m$ and let (Z, i) be the vector space based on X. We identify each element $x \in X$ with χ_x. It is important to remember that elements of X are m-tuples. Because we are in the vector space Z, we can take scalar multiples of these objects and add them (formally). So, for example, if $\boldsymbol{v}_i, \boldsymbol{v}_i' \in V_i, 1 \le i \le m$, then there is an element $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_m) + (\boldsymbol{v}_1', \dots, \boldsymbol{v}_m')$ in Z but we cannot combine them in any other way.*

Given elements $\boldsymbol{v}_i \in V_i, 1 \le i \le m$ and a scalar c, denote by $\boldsymbol{u}_{i,c}(\boldsymbol{v}_1, \dots, \boldsymbol{v}_m)$ the following element of Z:

$$(\boldsymbol{v}_1, \dots, \boldsymbol{v}_{i-1}, c\boldsymbol{v}_i, \boldsymbol{v}_{i+1}, \dots, \boldsymbol{v}_m) - c(\boldsymbol{v}_1, \dots, \boldsymbol{v}_{i-1}, \boldsymbol{v}_i, \boldsymbol{v}_{i+1}, \dots, \boldsymbol{v}_m).$$

Next, assume $\boldsymbol{v}_1 \in V_1, \dots, \boldsymbol{v}_m \in V_m$ and $\boldsymbol{v}_i' \in V_i$.

Let $\boldsymbol{u}_i(\boldsymbol{v}_1, \dots, \boldsymbol{v}_{i-1}, (\boldsymbol{v}_i, \boldsymbol{v}_i'),\ \boldsymbol{v}_{i+1}, \dots, \boldsymbol{v}_m)$ denote the following expression, which is an element of Z:

$$(\boldsymbol{v}_1, \dots, \boldsymbol{v}_i + \boldsymbol{v}_i', \dots, \boldsymbol{v}_m) - (\boldsymbol{v}_1, \dots, \boldsymbol{v}_i, \dots, \boldsymbol{v}_m) - (\boldsymbol{v}_1, \dots, \boldsymbol{v}_i', \dots, \boldsymbol{v}_m).$$

Let U be the subspace of Z generated by all elements $\boldsymbol{u}_{i,c}(\boldsymbol{v}_1, \dots, \boldsymbol{v}_m)$ and $\boldsymbol{u}_i(\boldsymbol{v}_1, \dots, \boldsymbol{v}_{i-1}, (\boldsymbol{v}_i, \boldsymbol{v}_i'), \boldsymbol{v}_{i+1}, \dots, \boldsymbol{v}_m)$. Set $V = Z/U$, the quotient space of Z by the subspace U. Further, define the map $\gamma : V_1 \times \cdots \times V_m \to V$ by

$$\gamma(\boldsymbol{v}_1, \dots, \boldsymbol{v}_m) = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_m) + U.$$

The image of $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_m) \in V_1 \times \cdots \times V_m$ is the coset of U in Z with representative $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_m)$. We claim that (V, γ) is the tensor product of $V_1, \dots, V_m$ over $\mathbb{F}$. To demonstrate this, we must first prove that γ is a multilinear map. To do so, we have to show the following:

1) If $\boldsymbol{v}_i \in V_i, 1 \leq i \leq m$ *and* $c \in \mathbb{F}$*, then*

$$\gamma(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, c\boldsymbol{v}_i, \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m) = c\gamma(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m). \tag{10.1}$$

2) If $\boldsymbol{v}_j \in V_j, 1 \leq j \leq n$ *and* $\boldsymbol{v}_i' \in V_i$*, then*

$$\gamma(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, \boldsymbol{v}_i + \boldsymbol{v}_i', \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m)$$

$$= \gamma(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, \boldsymbol{v}_i, \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m) + \gamma(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, \boldsymbol{v}_i', \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m). \tag{10.2}$$

1) The equality (10.1) is equivalent to

$$\gamma(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, c\boldsymbol{v}_i, \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m) - c\gamma(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m) = \mathbf{0}_V.$$

By the definition of γ*, we must show that*

$$[(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, c\boldsymbol{v}_i, \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m) + U] - [c(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m) + \ U] = \mathbf{0}_V.$$

Equivalently, we must show that

$$[(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, c\boldsymbol{v}_i, \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m) - c(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)] + U = \mathbf{0}_V.$$

Now it is imperative to recall what the zero vector of V *is: It is the coset* U *and for an element* $\boldsymbol{z} \in Z$ *we get* $\boldsymbol{z} + U = U$ *precisely when* $\boldsymbol{z} \in U$*. In the present case, the representative of the coset is* $\boldsymbol{u}_{i,c}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)$*, which, indeed, belongs to* U*.*

2) is equivalent to showing that

$$\gamma(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, \boldsymbol{v}_i + \boldsymbol{v}_i', \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m)$$

$$-\gamma(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, \boldsymbol{v}_i, \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m)$$

$$-\gamma(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, \boldsymbol{v}_i', \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m) = \mathbf{0}_V.$$

Using the definition of γ*, we need to show that*

$$(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, \boldsymbol{v}_i + \boldsymbol{v}_i', \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m)$$

$$-(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, \boldsymbol{v}_i, \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m)$$

$$-(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, \boldsymbol{v}_i', \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m) \in U.$$

However, this is just the element $\boldsymbol{u}_i(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, (\boldsymbol{v}_i, \boldsymbol{v}_i'), \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m)$*, which is in* U *as required.*

Now that we have established that γ *is multilinear we need to prove that the universal mapping property is satisfied. Toward that end, suppose* W *is a vector space over* $\mathbb{F}$ *and* $f : V_1 \times \cdots \times V_m \to W$ *is a multilinear map. We need to show that there exists a unique linear map* $T : V \to W$ *such that* $T\gamma = f$.

Recall that $V_1 \times \cdots \times V_m = X$ *and that* Z *is the vector space based on* X. *Since* W *is a vector space and* f *is a map from* X *to* W*, by the universal property of* Z *there exists a unique linear transformation* $S : Z \to W$ *such that* S *restricted to* X *is* f. *We next claim that the subspace* U *is contained in the kernel of* S. *It suffices to prove that the generators* $\boldsymbol{u}_{i,c}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)$ *and* $\boldsymbol{u}_i(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, (\boldsymbol{v}_i, \boldsymbol{v}_i'), \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m)$ *are in the kernel of* S. *Consider* $S(\boldsymbol{u}_{i,c}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n))$.

$$S(\boldsymbol{u}_{i,c}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n))$$

$$= S((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, c\boldsymbol{v}_i, \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m) - c(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)). \tag{10.3}$$

By the linearity of S *we get that (10.3) is equal to*

$$S((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, c\boldsymbol{v}_i, \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m)) - cS((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)). \tag{10.4}$$

Since both $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, c\boldsymbol{v}_i, \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m)$ *and* $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)$ *are elements of* $X = V_1 \times \cdots \times V_m$*, we therefore have*

$$S((\boldsymbol{v}_1, \ldots, c\boldsymbol{v}_i, \ldots, \boldsymbol{v}_m)) = f((\boldsymbol{v}_1, \ldots, c\boldsymbol{v}_i, \ldots, \boldsymbol{v}_m)), \tag{10.5}$$

$$S((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i, \ldots, \boldsymbol{v}_m)) = f((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i, \ldots, \boldsymbol{v}_m)). \tag{10.6}$$

Substituting (10.5) and (10.6) into (10.4) we get

$$S((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, c\boldsymbol{v}_i, \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m)) - cS((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m))$$

$$= f((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, c\boldsymbol{v}_i, \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m)) - cf((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)) = \mathbf{0}_W. \tag{10.7}$$

The latter equality in (10.7) holds because f *is multilinear.*

Now consider $S(\boldsymbol{u}_i(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, (\boldsymbol{v}_i, \boldsymbol{v}_i'), \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m))$. *Set* $\boldsymbol{x} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, \boldsymbol{v}_i, \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m), \boldsymbol{x}' = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, \boldsymbol{v}_i', \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m)$*, and* $\boldsymbol{y} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, \boldsymbol{v}_i + \boldsymbol{v}_i', \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m)$ *so that* $\boldsymbol{u}_i(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, (\boldsymbol{v}_1, \boldsymbol{v}_i'), \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m) = \boldsymbol{y} - \boldsymbol{x} - \boldsymbol{x}'$. *Now*

$$S(\boldsymbol{u}_i(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, (\boldsymbol{v}_i, \boldsymbol{v}_i'), \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_m))$$

$$S(\boldsymbol{y} - \boldsymbol{x} - \boldsymbol{x}') \tag{10.8}$$

By the linearity of S*, (10.8) is equal to*

$$S(\boldsymbol{y}) - S(\boldsymbol{x}) - S(\boldsymbol{x}') =$$

$$S((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i + \boldsymbol{v}_i', \ldots, \boldsymbol{v}_m)) - S((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i, \ldots, \boldsymbol{v}_m)) - S((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i', \ldots, \boldsymbol{v}_m)).$$

Each of $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i + \boldsymbol{v}_i', \ldots, \boldsymbol{v}_m), (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i, \ldots, \boldsymbol{v}_m)$*, and* $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i', \ldots, \boldsymbol{v}_m)$ *belongs to* $V_1 \times \cdots \times V_m = X$ *and therefore*

$$\begin{aligned} S((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i + \boldsymbol{v}_i', \ldots, \boldsymbol{v}_m)) &= f((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i + \boldsymbol{v}_i', , \ldots, \boldsymbol{v}_m)), \\ S((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i, \ldots, \boldsymbol{v}_m)) &= f((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i, \ldots, \boldsymbol{v}_m)), \\ S((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i', \ldots, \boldsymbol{v}_m)) &= f((\boldsymbol{v}_1, \ldots, , \boldsymbol{v}_i', \ldots, \boldsymbol{v}_m)). \end{aligned}$$

Then

$$S((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i + \boldsymbol{v}_i', \ldots, \boldsymbol{v}_m)) - S((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i, \ldots, \boldsymbol{v}_m)) - S((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i', \ldots, \boldsymbol{v}_m))$$

$$= f((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i + \boldsymbol{v}_i', \ldots, \boldsymbol{v}_m)) - f((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i, \ldots, \boldsymbol{v}_m)) - f((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i', \ldots, \boldsymbol{v}_m))$$

$$= \mathbf{0}_W.$$

The last equality follows by the multilinearity of f*.*

Since U *is contained in kernel*(S) *we may use Theorem (2.16) to conclude that there is a unique linear transformation* $T : Z/U \to W$ *such that* $T(\boldsymbol{z} + U) = S(\boldsymbol{z})$*. We finally claim that* $T\gamma = f$*:*

$$(T\gamma)(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m) = T(\gamma(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)) = T((\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m) + U)$$

$$= S(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m) = f(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m).$$

We will denote the quotient space Z/U by $V_1 \otimes \cdots \otimes V_m$ and refer to this as the tensor product of $V_1, \ldots, V_m$. Also, for $\boldsymbol{v}_i \in V_i, 1 \leq i \leq m$, we will denote by $\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_n$ the element $\gamma(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m) = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m) + U$. Using this notation, we can reformulate the multilinearity of γ as follows:

For vectors $\boldsymbol{v}_j \in V_j, 1 \leq j \leq m$ and scalar c,

$$\boldsymbol{v}_1 \otimes \ldots \boldsymbol{v}_{i-1} \otimes c\boldsymbol{v}_i \otimes \boldsymbol{v}_{i+1} \otimes \cdots \otimes \boldsymbol{v}_m = c(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_m).$$

For vectors $\boldsymbol{v}_j \in V_j, 1 \leq j \leq m$ and $\boldsymbol{v}_i' \in V_i$,

$$\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_{i-1} \otimes (\boldsymbol{v}_i + \boldsymbol{v}_i') \otimes \boldsymbol{v}_{i+1} \otimes \cdots \otimes \boldsymbol{v}_m =$$

$$(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_{i-1} \otimes \boldsymbol{v}_i \otimes \boldsymbol{v}_{i+1} \otimes \boldsymbol{v}_m) + (\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_{i-1} \otimes \boldsymbol{v}_i' \otimes \boldsymbol{v}_{i+1} \otimes \cdots \otimes \boldsymbol{v}_m.$$

In our next result, we show how, given bases for $V_1, \ldots, V_m$, to obtain a basis for $V_1 \otimes \cdots \otimes V_m$.

Theorem 10.2 *For each $i, 1 \leq i \leq m$, let V_i be a vector space over $\mathbb{F}$ with basis $\mathcal{B}_i$. Set $\mathcal{B} = \{\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_m | \boldsymbol{v}_i \in \mathcal{B}_i, 1 \leq i \leq m\}$. Then $\mathcal{B}$ is a basis for $V_1 \otimes \cdots \otimes V_m$.*

Proof *Set $X' = \mathcal{B}_1 \times \cdots \times \mathcal{B}_m$ and let Z' be the subspace of Z which is spanned by X'. Identify each element $x = (\boldsymbol{v}_1, \ldots \boldsymbol{v}_m) \in X'$ with $\chi_x \in Z'$. Since V_i is spanned by $\mathcal{B}_i$ for each i there is a unique multilinear map $\gamma' : V_1 \times \cdots \times V_m \to Z'$ such that γ' restricted to X' is the identity. We claim that (Z', γ') is the tensor product of $V_1, \ldots, V_m$.*

Toward that end, assume that W is a vector space and $f : V_1 \times \cdots \times V_m \to W$ is a multilinear map. Let $\widehat{f}$ be the restriction of f to $X' \subset V_1 \times \cdots \times V_m$. Since X' is a basis for Z', there is a unique linear transformation $\tau : Z' \to W$ such that τ restricted to X' is $\widehat{f}$. We will be done if we can prove that $\tau \circ \gamma' = f$. Now $\tau \circ \gamma'$ restricted to X' is $\widehat{f}$. Since each V_i is spanned by $\mathcal{B}_i$ and f is multilinear, it follows that $\tau \circ \gamma' = f$ as required.

Now by Lemma (10.1) there are isomorphisms $\tau : Z/U \to Z'$ and $\tau' : Z' \to Z/U$ such that $\tau \circ \tau' = I_{Z'}$ and $\tau' \circ \tau = I_{Z/U}$. Since X' is a basis for Z' and τ' is an isomorphism, it then follows that $\tau'(X')$ is a basis for $Z/U = V_1 \otimes \cdots \otimes V_m$.

When V_i is finite-dimensional for each $i, 1 \leq i \leq m$, we get the following result:

Corollary 10.1 *Let $V_1, \ldots, V_m$ be vector spaces over $\mathbb{F}$ with $dim(V_i) = n_i$. Then $dim(V_1 \otimes \cdots \otimes V_m) = n_1 n_2 \ldots n_m$.*

We complete this section with an application of the tensor product to algebras.

Let $\mathcal{A}, \mathcal{A}'$ be algebras over the field $\mathbb{F}$. Consider the tensor product $A = \mathcal{A} \otimes \mathcal{A}'$. We will define a product on this which will make it into an $\mathbb{F}$-algebra. Let ζ be the map from $\mathcal{A} \times \mathcal{A}' \times \mathcal{A} \times \mathcal{A}'$ to $\mathcal{A} \otimes \mathcal{A}'$ defined by

$$\zeta(\boldsymbol{a}, \boldsymbol{a}', \boldsymbol{b}, \boldsymbol{b}') = (\boldsymbol{a}\boldsymbol{b}) \otimes (\boldsymbol{a}'\boldsymbol{b}').$$

Then ζ is a four-linear map. It then follows that there is a linear map $\mathcal{Z}$ from $\mathcal{A} \otimes \mathcal{A}' \otimes \mathcal{A} \otimes \mathcal{A}'$ to $\mathcal{A} \otimes \mathcal{A}'$ such that

$$\mathcal{Z}(\boldsymbol{a} \otimes \boldsymbol{a}' \otimes \boldsymbol{b} \otimes \boldsymbol{b}') = (\boldsymbol{a}\boldsymbol{b}) \otimes (\boldsymbol{a}'\boldsymbol{b}').$$

This then defines a bilinear map $\mathcal{Z}'$ from $[\mathcal{A} \otimes \mathcal{A}']^2$ such that

$$\mathcal{Z}'(\boldsymbol{a} \otimes \boldsymbol{a}', \boldsymbol{b} \otimes \boldsymbol{b}') = (\boldsymbol{a}\boldsymbol{b}) \otimes (\boldsymbol{a}'\boldsymbol{b}').$$

Taking $\mathcal{Z}'$ as multiplication in $\mathcal{A} \otimes \mathcal{A}'$, this space becomes an algebra.

Exercises

Many of these exercises involve tensor products of two vector spaces. These can be generalized to m vector spaces in a straightforward way but have been limited to this case to simplify the statements and the solutions.

1. Let V_1, V_2 be vector spaces with respective bases $\mathcal{B}_1, \mathcal{B}_2$. Suppose W is a vector space and $f : \mathcal{B}_1 \times \mathcal{B}_2 \to W$ is a (set) map. Prove that there is a unique bilinear map $\widehat{f}$ from $V_1 \times V_2 \to W$ such that $\widehat{f}$ restricted to $\mathcal{B}_1 \times \mathcal{B}_2$ is f.

2. Let V_1 and V_2 be vector spaces over the field $\mathbb{F}$. Use the fact that the tensor product is a solution to a universal mapping problem to prove that $V_1 \otimes V_2$ and $V_2 \otimes V_1$ are isomorphic.

3. Let V_1 and V_2 be vector spaces over the field $\mathbb{F}$. Assume $f_i \in \mathcal{L}(V_i, \mathbb{F})$, $i = 1, 2$. Define $f : V_1 \times V_2 \to \mathbb{F}$ by $f(\boldsymbol{v}_1, \boldsymbol{v}_2) = f_1(\boldsymbol{v}_1)f_2(\boldsymbol{v}_2)$. Prove that f is a bilinear form.

4. Let V and W be vector spaces over $\mathbb{F}$. An element $\boldsymbol{t}$ of $V \otimes W$ is said to be ***decomposable*** if there are vectors $\boldsymbol{v} \in V$ and $\boldsymbol{w} \in W$ such that $\boldsymbol{t} = \boldsymbol{v} \otimes \boldsymbol{w}$ and ***indecomposable*** otherwise. Prove if $dim(V) > 1$ and $dim(W) > 1$, then there exists indecomposable elements in $V \otimes W$.

5. Let $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ be linearly independent in the vector space V and $\boldsymbol{w}_i \in W, 1 \leq i \leq n$, be vectors in the space W. Assume $\sum_{i=1}^n \boldsymbol{v}_i \otimes \boldsymbol{w}_i = \boldsymbol{0}_{V \otimes W}$. Prove that $\boldsymbol{w}_1 = \cdots = \boldsymbol{w}_n = \boldsymbol{0}_W$.

6. Let V and W be finite-dimensional vector spaces over $\mathbb{F}$ and Z a vector space over $\mathbb{F}$. Assume there is a bilinear map $f : V \times W \to Z$ which satisfies the following:

a) For every $\boldsymbol{z} \in Z$, there is a natural number m and vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in V, \boldsymbol{w}_1, \ldots, \boldsymbol{w}_m \in W$ such that $\boldsymbol{z} = f(\boldsymbol{v}_1, \boldsymbol{w}_1) + \cdots + f(\boldsymbol{v}_m, \boldsymbol{w}_m)$.

b) If $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ is a basis for V, $\boldsymbol{y}_i \in W, 1 \leq i \leq n$, and $f(\boldsymbol{x}_1, \boldsymbol{y}_1) + \cdots + f(\boldsymbol{x}_n, \boldsymbol{y}_n) = 0$, then $\boldsymbol{y}_1 = \cdots = \boldsymbol{y}_n = \mathbf{0}_W$.

Prove that (Z, f) is the tensor product of V and W.

7. Let V, W, and Z be vector spaces over a field $\mathbb{F}$. Use the fact that the tensor product is a solution to a universal mapping problem to prove that $B(V, W; Z)$ is isomorphic to $\mathcal{L}(V \otimes W, Z)$.

8. Let V be a vector space over the field $\mathbb{F}$ and treat $\mathbb{F}$ as a vector space over $\mathbb{F}$ of dimension 1. Prove that $\mathbb{F} \otimes V$ is isomorphic to V.

9. Let V, W be vector spaces over a field $\mathbb{F}$ and assume that X is a subspace of V and Y is a subspace of W. Let Z be the subspace of $V \otimes W$ spanned by all elements $\boldsymbol{x} \otimes \boldsymbol{y}$ where $\boldsymbol{x} \in X, \boldsymbol{y} \in Y$. Prove that Z can be identified with $X \otimes Y$.

10. Let V and W be finite-dimensional vector spaces over the field $\mathbb{F}$ and Y_1, Y_2 subspaces of W. From Exercise 9, we may identify $V \otimes Y_1$ and $V \otimes Y_2$ as subspaces of $V \otimes W$. Prove that $(V \otimes Y_1) \cap (V \otimes Y_2) = V \otimes (Y_1 \cap Y_2)$.

10.2 Properties of Tensor Products

In this section we make use of the definition of the tensor product as the solution to a universal mapping problem to prove several functorial properties. We show how a tensor product of linear transformations can be defined to obtain a transformation from one tensor product to another. We also show how to compute the matrix of a tensor product of transformations from the matrices of the transformations.

What You Need to Know

To make sense of the new material in this section, it is essential that you have mastery over the following concepts: vector space, basis of a vector space, dimension of a vector space, finite-dimensional vector space, linear transformation, coordinate vector with respect to a basis, matrix of a linear transformation, an algebra over a field, multilinear map, multilinear form, bilinear map, bilinear form, and the tensor product of vector spaces.

Most of the proofs in this section will make use of the definition of a tensor product of vector spaces and exploit the uniqueness of the tensor product as demonstrated in Theorem (10.1). Our first result will lead to an associativity property and ultimately be used in the definition of the tensor algebra of a vector space.

Theorem 10.3 *Let $V_1, \dots, V_s, W_1, \dots, W_t$ be vector spaces over the field $\mathbb{F}$. Then $(V_1 \otimes \cdots \otimes V_s) \otimes (W_1 \otimes \cdots \otimes W_t)$ is isomorphic to $V_1 \otimes \cdots \otimes V_s \otimes W_1 \otimes \cdots \otimes W_t$.*

Proof *For notational convenience, set*

$$V = V_1 \otimes \cdots \otimes V_s, W = W_1 \otimes \cdots \otimes W_t$$

$$X = V \otimes W, Y = V_1 \otimes \cdots \otimes V_s \otimes W_1 \otimes \cdots \otimes W_t.$$

Let f be the map from $V_1 \times \cdots \times V_s \times W_1 \times \cdots \times W_t$ to X given by

$$f(\boldsymbol{v}_1, \dots, \boldsymbol{v}_s, \boldsymbol{w}_1, \dots, \boldsymbol{w}_t) = (\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_s) \otimes (\boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{w}_t).$$

The map f is multilinear and therefore by the universality of Y there is a linear map $T : Y \to X$ such that

$$T(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_s \otimes \boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{w}_t) = (\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_s) \otimes (\boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{w}_t).$$

We will prove the existence of a linear map $S : X \to Y$ such that

$$S((\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_s) \otimes (\boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{w}_t)) = \boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_s \otimes \boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{w}_t.$$

Since X is generated by all elements $(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_s) \otimes (\boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{w}_t)$ and Y is generated by all elements $\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_s \otimes \boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{w}_t$, it follows that S and T are inverses of each other and consequently X and Y are isomorphic.

Let $\boldsymbol{w}_j \in W_j, 1 \leq j \leq t$ and let $g(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_t)$ be the map from $V_1 \times \cdots \times V_s$ to Y given by $g(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_t)(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s) = \boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_t \otimes \boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{w}_t$. Then $g(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_t)$ is a multilinear map and therefore by the universality of V there exists a linear map $\sigma(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_t)$ from V to Y. By varying $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_t) \in W_1 \times \cdots \times W_t$, we get a map σ from $W_1 \times \cdots \times W_t$ to $\mathcal{L}(V, Y)$. We claim that σ is a multilinear map. For example, suppose $\boldsymbol{w}'_1 \in W_1$. Then

$$\begin{aligned}
\sigma(\boldsymbol{w}_1 + \boldsymbol{w}'_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_t)(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_s) &= g(\boldsymbol{w}_1 + \boldsymbol{w}'_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_t)(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s) \\
&= \boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_s \otimes (\boldsymbol{w}_1 + \boldsymbol{w}'_1) \otimes \cdots \otimes \boldsymbol{w}_t \\
&= \boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_s \otimes \boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{w}_t + \boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_s \otimes \boldsymbol{w}'_1 \otimes \cdots \otimes \boldsymbol{w}_t \\
&= g(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_t)(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s) + g(\boldsymbol{w}'_1, \ldots, \boldsymbol{w}_t)(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s) \\
&= \sigma(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_t)(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_s) + \sigma(\boldsymbol{w}'_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_t)(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_s).
\end{aligned}$$

Since V is spanned by all vectors of the form $\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_s$ it follows that $\sigma(\boldsymbol{w}_1 + \boldsymbol{w}'_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_t) = \sigma(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_t) + \sigma(\boldsymbol{w}'_1, \ldots, \boldsymbol{w}_t)$.

In a similar way, we can prove that $\sigma(c\boldsymbol{w}_1, \ldots, \boldsymbol{w}_t) = c\sigma(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_t)$. The other arguments are proved in exactly the same way.

Since σ is a multilinear map from $W_1 \times \cdots \times W_t$ to $\mathcal{L}(V, Y)$, there is a linear map $\widehat{\sigma} : W \to \mathcal{L}(V, X)$ such that for $\boldsymbol{w}_j \in W_j, 1 \leq j \leq t$, $\widehat{\sigma}(\boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{w}_t) = \sigma(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_t)$. Now define the map $h : V \times W \to Y$ by $h(\boldsymbol{v}, \boldsymbol{w}) = \sigma(\boldsymbol{w})(\boldsymbol{v})$. This is a bilinear map as can be easily checked. It follows by the universal property of $V \otimes W$ that there is a linear map $S : V \otimes W \to Y$ such that for $\boldsymbol{v} \in V, \boldsymbol{w} \in W, S(\boldsymbol{v} \otimes \boldsymbol{w}) = h(\boldsymbol{v}, \boldsymbol{w}) = \widehat{\sigma}(\boldsymbol{w})(\boldsymbol{v})$. In particular, this is true if $\boldsymbol{v} = \boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_s$ and $\boldsymbol{w} = \boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{w}_t$. We then get

$$\begin{aligned}
S((\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_s) \otimes (\boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{w}_t)) &= \widehat{\sigma}(\boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{w}_t)(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_s) \\
&= \sigma(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_t)(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_s) \\
&= \boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_s \otimes \boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{w}_t.
\end{aligned}$$

As an immediate corollary we have

Corollary 10.2 *Let V, W, X be vector spaces over the field $\mathbb{F}$. Then the tensor products $V \otimes (W \otimes X), (V \otimes W) \otimes X,$ and $V \otimes W \otimes X$ are isomorphic.*

The following result can be proved by similar methods using the universal property of the tensor product. It generalizes Exercise 2 of Section (10.1).

Theorem 10.4 *Let $V_1, \ldots, V_m$ be vector spaces over the field $\mathbb{F}$ and π a permutation of $\{1, 2, \ldots, m\}$. Then $V_1 \otimes \cdots \otimes V_m$ is isomorphic to $V_{\pi(1)} \otimes \cdots \otimes V_{\pi(m)}$ by a linear map which takes $\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_m$ to $\boldsymbol{v}_{\pi(1)} \otimes \cdots \otimes \boldsymbol{v}_{\pi(m)}$.*

Our next result shows how to extend transformations defined on two or more vector spaces to a transformation of their tensor product.

Theorem 10.5 *Let $V_1, \ldots, V_n, W_1, \ldots, W_n$ be vector spaces over the field $\mathbb{F}$ and for each i, let $S_i : V_i \to W_i$ be a linear transformation. Then there is a unique linear transformation $S : V_1 \otimes \cdots \otimes V_n \to W_1 \otimes \cdots \otimes W_n$ such that if $\boldsymbol{v}_i \in V_i, 1 \leq i \leq n$, then $S(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_n) = S_1(\boldsymbol{v}_1) \otimes \cdots \otimes S_n(\boldsymbol{v}_n)$.*

Proof *Denote by γ the canonical map from $V_1 \times \cdots \times V_n$ to $V_1 \otimes \cdots \otimes V_n$,*

$$\gamma(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) = \boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_n$$

and similarly denote by γ' the corresponding map from $W_1 \times \cdots \times W_n$ to $W_1 \otimes \cdots \otimes W_n$.

Let σ be the map from $V_1 \times \cdots \times V_n$ to $W_1 \otimes \cdots \otimes W_n$ defined by

$$\sigma(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) = S_1(\boldsymbol{v}_1) \otimes \cdots \otimes S_n(\boldsymbol{v}_n).$$

Since γ' is multilinear and each S_i is linear, it follows that σ is multilinear. By the universal property for $V_1 \otimes \cdots \otimes V_n$, it follows that there exists a unique linear map S from $V_1 \otimes \cdots \otimes V_n$ to $W_1 \otimes \cdots \otimes W_n$ such that $S \circ \gamma = \sigma$. Taking the image of $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ we get

$$S(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_n) = S_1(\boldsymbol{v}_1) \otimes \cdots \otimes S_n(\boldsymbol{v}_n).$$

Definition 10.3 *Let $V_i, W_i, 1 \leq i \leq n$ be vector spaces over the field $\mathbb{F}$ and $S_i : V_i \to W_i$ be linear transformations. We denote by $S_1 \otimes \cdots \otimes S_n$ the unique linear transformation $S : V_1 \otimes \cdots \otimes V_n \to W_1 \otimes \cdots \otimes W_n$ such that $S(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_n) = S_1(\boldsymbol{v}_1) \otimes \cdots \otimes S_n(\boldsymbol{v}_n)$ for $\boldsymbol{v}_i \in V_i$. We refer to this as the* **tensor product** *of the linear transformations $S_1, \ldots, S_n$.*

The next lemma indicates what conclusions we can draw about the tensor product of linear transformations from information about the individual transformations.

Lemma 10.2 *Let $S_i : V_i \to W_i$ be linear transformations of the vectors spaces $V_1, \dots, V_n, W_1, \dots, W_n$ over the field $\mathbb{F}$. Then the following hold:*

i) If each S_i is surjective, then $S_1 \otimes \cdots \otimes S_n$ is surjective.

ii) If each S_i is injective, then $S_1 \otimes \cdots \otimes S_n$ is injective.

iii) If each S_i is an isomorphism, then $S_1 \otimes \cdots \otimes S_n$ is an isomorphism.

iv) If $T_i : W_i \to X_i$ is a linear transformation where $X_1, \dots, X_n$ are vector spaces over $\mathbb{F}$, then $(T_1 \otimes \cdots \otimes T_n)(S_1 \otimes \cdots \otimes S_n) = (T_1 S_1) \otimes \cdots \otimes (T_n S_n)$.

v) If each S_i is an isomorphism, then $(S_1 \otimes \cdots \otimes S_n)^{-1} = S_1^{-1} \otimes \cdots \otimes S_n^{-1}$.

vi) If $S'_j : V_j \to W_j$ is also a linear transformation, then

$$S_1 \otimes \cdots \otimes (S_j + S'_j) \otimes \cdots \otimes S_n = (S_1 \otimes \cdots \otimes S_j \otimes \cdots \otimes S_n) + (S_1 \otimes \cdots \otimes S'_j \otimes \cdots \otimes S_n).$$

vii) If c is a scalar, then for $1 \leq j \leq n$

$$S_1 \otimes \cdots \otimes cS_j \otimes \cdots \otimes S_n = c(S_1 \otimes \cdots \otimes S_j \otimes \cdots \otimes S_n).$$

Proof *For notational ease we will prove these in the case that $n = 2$. The general proof can be obtained in exactly the same way by changing 2 to n and inserting dots (...) between 2 and n.*

i) We know that $W_1 \otimes W_2$ is spanned by all decomposable vectors $\boldsymbol{w}_1 \otimes \boldsymbol{w}_2$, where $\boldsymbol{w}_i \in W_i, i = 1, 2$. It therefore suffices to prove that every decomposable vectors in $W_1 \otimes W_2$ is in the range of $S_1 \otimes S_2$. However, as each S_i is surjective, given $\boldsymbol{w}_1 \in W_1, \boldsymbol{w}_2 \in W_2$, there exists $\boldsymbol{v}_1 \in V_1, \boldsymbol{v}_2 \in V_2$ such that $S_1(\boldsymbol{v}_1) = \boldsymbol{w}_1, S_2(\boldsymbol{v}_2) = \boldsymbol{w}_2$. Then

$$(S_1 \otimes S_2)(\boldsymbol{v}_1 \otimes \boldsymbol{v}_2) = S(\boldsymbol{v}_1) \otimes S_2(\boldsymbol{v}_2) = \boldsymbol{w}_1 \otimes \boldsymbol{w}_2.$$

ii) Let $\mathcal{B}_i$ be a basis for V_i for $i = 1, 2$. Then $\mathcal{B}_1 \otimes \mathcal{B}_2 = \{\boldsymbol{v}_1 \otimes \boldsymbol{v}_2 | \boldsymbol{v}_1 \in \mathcal{B}_1, \boldsymbol{v}_2 \in \mathcal{B}_2\}$ is a basis for $V_1 \otimes V_2$. To show that $S_1 \otimes S_2$ is injective, we need to show that $(S_1 \otimes S_2)(\mathcal{B}_1 \otimes \mathcal{B}_2) = \{(S_1 \otimes S_2)(\boldsymbol{v}_1 \otimes \boldsymbol{v}_2) | \boldsymbol{v}_1 \in \mathcal{B}_1, \boldsymbol{v}_2 \in \mathcal{B}_2\} = \{S_1(\boldsymbol{v}_1) \otimes S_2(\boldsymbol{v}_2) | \boldsymbol{v}_1 \in \mathcal{B}_1, \boldsymbol{v}_2 \in \mathcal{B}_2\}$ is linearly independent. To do so we need to show that for every finite subset of D of $\mathcal{B}_1 \otimes \mathcal{B}_2$ that $(S_1 \otimes S_2)(D)$ is linearly independent.

Suppose $D = \{\boldsymbol{x}_1 \otimes \boldsymbol{y}_1, \dots, \boldsymbol{x}_t \otimes \boldsymbol{y}_t\}$, where $\boldsymbol{x}_i \in \mathcal{B}_1$ and $\boldsymbol{y}_i \in \mathcal{B}_2$. Of course, it *may be the case that not all $\boldsymbol{x}_i$ or $\boldsymbol{y}_i$ are distinct, so let $(\boldsymbol{v}_{11}, \ldots, \boldsymbol{v}_{1,m_1})$ be distinct such that $\{\boldsymbol{v}_{11}, \ldots, \boldsymbol{v}_{1,m_1}\} = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_t\}$ and, similarly, $(\boldsymbol{v}_{21}, \ldots, \boldsymbol{v}_{2,m_2})$ be distinct such that $\{\boldsymbol{v}_{21}, \ldots, \boldsymbol{v}_{2,m_2}\} = \{\boldsymbol{y}_1, \ldots, \boldsymbol{y}_t\}$. Then D is contained in $E = \{\boldsymbol{v}_{1i} \otimes \boldsymbol{v}_{2j} | 1 \leq i \leq m_1, 1 \leq j \leq m_2\}$. Therefore, it is suffices to show that $(S_1 \otimes S_2)(E)$ is linearly independent.*

Since S_1 is injective and $(\boldsymbol{v}_{11}, \ldots, \boldsymbol{v}_{1,m_1})$ is linearly independent, it follows that $(S_1(\boldsymbol{v}_{11}), \ldots, S_1(\boldsymbol{v}_{1,m_1}))$ is linearly independent in W_1. Likewise, $(S_2(\boldsymbol{v}_{21}), \ldots, S_2(\boldsymbol{v}_{2,m_2}))$ is linearly independent in W_2. Then $(S_1(\boldsymbol{v}_{11}), \ldots, S_1(\boldsymbol{v}_{1,m_1}))$ can be extended to a basis $\mathcal{B}_1'$ of W_1 and $(S_2(\boldsymbol{v}_{21}), \ldots, S_2(\boldsymbol{v}_{2,m_2}))$ can be extended to a basis $\mathcal{B}_2'$ of W_2. By Theorem (10.2), $\mathcal{B}_1' \otimes \mathcal{B}_2'$ is a basis of $W_1 \otimes W_2$. In particular, $\mathcal{B}_1' \otimes \mathcal{B}_2'$ is linearly independent. Consequently, $(S_1 \otimes S_2)(E)$ is linearly independent.

iii) This follows from i) and ii).

iv) The linear map $(T_1 S_1) \otimes (T_2 S_2)$ is the unique linear map from $V_1 \otimes V_2$ to $X_1 \otimes X_2$ that takes $\boldsymbol{v}_1 \otimes \boldsymbol{v}_2$ to $(T_1 S_1)(\boldsymbol{v}_1) \otimes (T_2 S_2)(\boldsymbol{v}_2)$. However, the image of $\boldsymbol{v}_1 \otimes \boldsymbol{v}_2$ under the linear map $(T_1 \otimes T_2)(S_1 \otimes S_2)$ is $(T_1 \otimes T_2)(S_1(\boldsymbol{v}_1) \otimes S_2(\boldsymbol{v}_2)) = T_1(S_1(\boldsymbol{v}_1)) \otimes T_2(S_2(\boldsymbol{v}_2)) = (T_1 S_1)(\boldsymbol{v}_1) \otimes (T_2 S_2)(\boldsymbol{v}_2)$. Therefore, by the uniqueness $(T_1 \otimes T_2)(S_1 \otimes S_2) = (T_1 S_1) \otimes (T_2 S_2)$.

v) By part iv), we have $(S_1 \otimes S_2)(S_1^{-1} \otimes S_2^{-1}) = (S_1 S_1^{-1}) \otimes (S_2 S_2^{-1}) = I_{W_1} \otimes I_{W_2} = I_{W_1 \otimes W_2}$ and $(S_1^{-1} \otimes S_2^{-1})(S_1 \otimes S_2) = (S_1^{-1} S_1) \otimes (S_2^{-1} S_2) = I_{V_1} \otimes I_{V_2} = I_{V_1 \otimes V_2}$.

vi) Both maps $(S_1 + S_1') \otimes S_2$ and $S_1 \otimes S_2 + S_1' \otimes S_2$ take a vector $\boldsymbol{v}_1 \otimes \boldsymbol{v}_2$ to $(S_1 + S_1')(\boldsymbol{v}_1) \otimes S_2(\boldsymbol{v}_2)$ and consequently they are identical. Likewise, $S_1 \otimes (S_2 + S_2') = (S_1 \otimes S_2) + (S_1' \otimes S_2)$.

vii) Each of the linear maps $(cS_1) \otimes S_2, S_1 \otimes (cS_2)$ and $c(S_1 \otimes S_2)$ take $\boldsymbol{v}_1 \otimes \boldsymbol{v}_2$ to the vector $c[S_1(\boldsymbol{v}_1) \otimes S_2(\boldsymbol{v}_2)]$ and so they are identical linear transformations.

We will shortly investigate the relationship between the matrix of $S_1 \otimes \cdots \otimes S_n$ and the matrices of the transformations $S_1, \ldots, S_n$. However, before doing so, we determine how the tensor product behaves with respect to direct sums. In order to obtain our main result we need to get a characterization of the direct sum of finitely many vector spaces.

Assume the vector space $V = V_1 \oplus \cdots \oplus V_n$ is the ***external direct sum*** of the spaces $V_1, \ldots, V_n$. Recall that V has as its underlying set the Cartesian product $V_1 \times \cdots \times V_n$. Addition is given by

$$(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) + (\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n) = (\boldsymbol{v}_1 + \boldsymbol{w}_1, \ldots, \boldsymbol{v}_n + \boldsymbol{w}_n)$$

and scalar multiplication by

$$c(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) = (c\boldsymbol{v}_1, \ldots, c\boldsymbol{v}_n).$$

Let $\mathbf{0}_i$ denote the zero vector of V_i and $\epsilon_i : V_i \to V$ be the linear map defined by $\epsilon_i(\boldsymbol{v}_i) = (\mathbf{0}_1, \dots, \mathbf{0}_{i-1}, \boldsymbol{v}_i, \mathbf{0}_{i+1}, \dots, \mathbf{0}_n)$. Also, let $\pi_i : V \to V_i$ be given by $\pi_i(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n) = \boldsymbol{v}_i$. Then the following hold:

a) $\pi_i \epsilon_i = I_{V_i}$; and

b) $\sum_{i=1}^n \epsilon_i \pi_i = I_V$.

In fact, these properties characterize the space V as the direct sum of the spaces $V_1, \dots, V_n$. Making use of this we can now prove our result on direct sums and tensor products:

Theorem 10.6 *Assume W and V are vector spaces over the field $\mathbb{F}$ and $V = V_1 \oplus \cdots \oplus V_n$. Then $W \otimes V$ is isomorphic to $(W \otimes V_1) \oplus \cdots \oplus (W \otimes V_n)$.*

Proof *Set $\widehat{\epsilon}_i = I_W \otimes \epsilon_i$, a linear map from $W \otimes V_i$ to $W \otimes V$, and $\widehat{\pi}_i = I_W \otimes \pi_i$, a linear map from $W \otimes V$ to $W \otimes V_i$.*

By part iv) of Theorem (10.4), we have $\widehat{\pi}_i \widehat{\epsilon}_i = I_W \otimes \pi_i \epsilon_i = I_W \otimes I_{V_i}$. Furthermore, by parts iv) and vi) of that result

$$\sum_{i=1}^n \widehat{\epsilon}_i \widehat{\pi}_i = \sum_{i=1}^n (I_W \otimes \epsilon_i \pi_i)$$

$$= I_W \otimes \sum_{i=1}^n \epsilon_i \pi_i = I_W \otimes I_V.$$

By the remarks preceding the theorem, these two conditions imply that $W \otimes V = W \otimes (V_1 \oplus \cdots \oplus V_n)$ is isomorphic to $(W \otimes V_1) \oplus \cdots \oplus (W \otimes V_n)$.

We complete this section by determining the matrix for a linear transformation obtained as the tensor product of linear transformations. We do this for the case of the tensor product of two spaces, but the results can be extended to the tensor product of finitely many spaces.

Let X be a vector space with basis $\mathcal{B}_X = (\boldsymbol{x}_1, \dots, \boldsymbol{x}_m)$ and Y a vector space with basis $(\boldsymbol{y}_1, \dots, \boldsymbol{y}_n)$. We have shown by taking the tensor products of the $\boldsymbol{x}_i$ with the $\boldsymbol{y}_j$ we obtain a basis for $X \otimes Y$. However, our bases are more than just independent spanning sets: they are ordered. We will adopt the convention that we order a basis for a tensor product obtained by taking the tensor product of bases ***lexicographically***. This means that $\boldsymbol{x}_i \otimes \boldsymbol{y}_j$ comes before $\boldsymbol{x}_k \otimes \boldsymbol{y}_l$ if either $i < k$ or $i = k$ and $j < l$. We will denote this basis by $\mathcal{B}_X \otimes \mathcal{B}_Y$.

Let $S_i : V_i \to W_i$ be linear transformations for $i = 1, 2$ and let $\mathcal{B}_{V_i} = (\boldsymbol{v}_{i1}, \dots, \boldsymbol{v}_{i,n_i})$ be a basis for $V_i, i = 1, 2$ and $\mathcal{B}_{W_i} = (\boldsymbol{w}_{i1}, \dots, \boldsymbol{w}_{i,m_i})$ be a basis for $W_i, i = 1, 2$. Let $A = \mathcal{M}_{S_1}(\mathcal{B}_{V_1}, \mathcal{B}_{W_1})$ and $B = \mathcal{M}_{S_2}(\mathcal{B}_{V_2}, \mathcal{B}_{W_2})$. Then A is an $m_1 \times n_1$ matrix and B is an $m_2 \times n_2$ matrix. Assume the entries of A are a_{ij} and the entries of B are b_{kl}. Recall that this means that

$$[S_1(\boldsymbol{v}_{1j})]_{\mathcal{B}_{W_1}} = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{m_1,j} \end{pmatrix} \text{ and } [S_2(\boldsymbol{v}_{2j})]_{\mathcal{B}_{W_2}} = \begin{pmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{m_2,j} \end{pmatrix}.$$

We want to determine the matrix of $S_1 \otimes S_2$ with respect to the bases $\mathcal{B}_{V_1} \otimes \mathcal{B}_{V_2}$ and $\mathcal{B}_{W_1} \otimes \mathcal{B}_{W_2}$. Thus, we have to determine the coordinates of the image $(S_1 \otimes S_2)(\boldsymbol{v}_{1i} \otimes \boldsymbol{v}_{2j})$ with respect to the basis $\mathcal{B}_{W_1} \otimes \mathcal{B}_{W_2}$.

$$\begin{aligned} (S_1 \otimes S_2)(\boldsymbol{v}_{1i} \otimes \boldsymbol{v}_{2j}) &= S_1(\boldsymbol{v}_{1i}) \otimes S_2(\boldsymbol{v}_{2j}) \\ &= \sum_{k=1}^{m_1} a_{ki}\boldsymbol{w}_{1k} \otimes \sum_{l=1}^{m_2} b_{lj}\boldsymbol{w}_{2l} \\ &= \sum_{k=1}^{m_1}\sum_{l=1}^{m_2} a_{ki}b_{lj}\boldsymbol{w}_{1k} \otimes \boldsymbol{w}_{2l}. \end{aligned}$$

Taking into account our lexicographical order, the coordinate vector of $(S_1 \otimes S_2)(\boldsymbol{v}_{1i} \otimes \boldsymbol{v}_{2j})$ with respect to $\mathcal{B}_{W_1} \otimes \mathcal{B}_{W_2}$ is the following vector:

$$\begin{pmatrix} a_{1i}b_{1j} \\ a_{1i}b_{2j} \\ \vdots \\ a_{1i}b_{m_2,j} \\ a_{2i}b_{1j} \\ a_{2i}b_{2j} \\ \vdots \\ a_{2i}b_{m_2,j} \\ \vdots \\ a_{m_1,i}b_{1j} \\ a_{m_1,i}b_{2j} \\ \vdots \\ a_{m_1,i}b_{m_2,j} \end{pmatrix}.$$

Let $\boldsymbol{b} = [S_2(\boldsymbol{v}_{2j})]_{\mathcal{B}_{W_2}}$. In words, the coordinate vector of $(S_1 \otimes S_2)$ of $\boldsymbol{v}_{1i} \otimes \boldsymbol{v}_{2j}$ with respect to $\mathcal{B}_{W_1} \otimes \mathcal{B}_{W_2}$ is $\boldsymbol{b}$ multiplied by a_{1i} followed by $\boldsymbol{b}$ multiplied by a_{2i} and so on until the last m_1 coordinates are obtained by multiplying $\boldsymbol{b}$ by $a_{m_1,i}$. The form of this matrix will be much clearer after the next definition.

Definition 10.4 *Let A be an $m_1 \times n_1$ matrix with entries $a_{ij}, 1 \le i \le m_1, 1 \le j \le n_1$ and B an $m_2 \times n_2$ matrix. The* **tensor or Kronecker product** *of A and B, denoted by $A \otimes B$, is the block matrix*

$$\begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1,n_1}B \\ a_{21}B & a_{22}B & \dots & a_{2,n_1}B \\ \vdots & \vdots & \dots & \vdots \\ a_{m_1,1}B & a_{m_1,2}B & \dots & a_{m_1,n_1}B. \end{pmatrix}$$

$A \otimes B$ is an $m_1m_2 \times n_1n_2$ matrix.

We have thus proved

Theorem 10.7 *Let $S_i : V_i \to W_i$ be linear transformations for $i = 1, 2$, $\mathcal{B}_{V_i} = (\boldsymbol{v}_{i1}, \dots, \boldsymbol{v}_{i,n_i})$ be a basis for $V_i, i = 1, 2$, and $\mathcal{B}_{W_i} = (\boldsymbol{w}_{i1}, \dots, \boldsymbol{w}_{i,m_i})$ be a basis for $W_i, i = 1, 2$. Finally, set $A = \mathcal{M}_{S_1}(\mathcal{B}_{V_1}, \mathcal{B}_{W_1})$ and $B = \mathcal{M}_{S_2}(\mathcal{B}_{V_2}, \mathcal{B}_{W_2})$.*

Then

$$\mathcal{M}_{S_1 \otimes S_2}(\mathcal{B}_{V_1} \otimes \mathcal{B}_{V_2}, \mathcal{B}_{W_1} \otimes \mathcal{B}_{W_2}) = A \otimes B.$$

Exercises

1. Let V_1, V_2, V_3 be vector spaces over a field $\mathbb{F}$ and π a permutation of $\{1, 2, 3\}$. Prove that $V_1 \otimes V_2 \otimes V_3$ is isomorphic to $V_{\pi(1)} \otimes V_{\pi(2)} \otimes V_{\pi(3)}$.

2. Let $S_i : V_i \to W_i, 1 \le i \le m$ be linear transformations, where $V_1, \dots, V_m$ are finite-dimensional vector spaces over the field $\mathbb{F}$. Set $R_i = Range(S_i)$ and $R = Range(S_1 \otimes \dots \otimes S_m)$. Prove that $R = R_1 \otimes \dots \otimes R_m$.

3. Let $S_i : V_i \to W_i, 1 \le i \le m$ be linear transformations, where $V_1, \dots, V_m$ are finite-dimensional vector spaces over the field $\mathbb{F}$. Set $K_i = Ker(S_i)$ and $K = Ker(S_1 \otimes \dots \otimes S_m)$. For $1 \le j \le m$, set $X_j = V_1 \otimes \dots \otimes V_{j-1} \otimes K_j \otimes V_{j+1} \otimes \dots \otimes V_m$. Prove that $K = X_1 + \dots + X_m$.

4. Let A be a $k \times l$ matrix and B an $m \times n$ matrix. Prove that the rank of $A \otimes B$ is $rank(A)rank(B)$.

5. Let V and W be finite-dimensional vectors spaces, S an operator on V, and T an operator on W. Prove that $S \otimes T$ is nilpotent if and only if S is nilpotent or T is nilpotent.

6. Let V and W be finite-dimensional vector spaces, S a cyclic diagonalizable operator on V with eigenvalues $\alpha_1, \dots, \alpha_m$, and T a cyclic diagonalizable operator on W with eigenvalues $\beta_1, \dots, \beta_n$. Assume that $\alpha_i\beta_j$ are all distinct. Prove that $S \otimes T$ is cyclic.

7. Give an example of a cyclic diagonalizable operator S on a space V with

distinct eigenvalues and a cyclic diagonalizable operator T on a space W with distinct eigenvalues such that $S \otimes T$ is not cyclic.

8. Let V and W be finite-dimensional vector spaces, S an operator on V, and T an operator on W. Assume $(S - \alpha I_V)^k = 0_{V \to V}$ and $(T - \beta I_W)^l = 0_{W \to W}$. Prove that $[(S \otimes T) - \alpha\beta(I_V \otimes I_W)]^{kl} = 0_{V \otimes W \to V \otimes W}$.

9. Let V be a vector space over the field $\mathbb{F}$ and let $\mathbb{K}$ be an extension of $\mathbb{F}$ (a field which contains $\mathbb{F}$.) We have seen that by using the addition of $\mathbb{K}$ and the restriction of the multiplication of $\mathbb{K}$ to $\mathbb{F} \times \mathbb{K}$, that $\mathbb{K}$ becomes a vector space over $\mathbb{F}$.

Set $V_{\mathbb{K}} = \mathbb{K} \otimes_{\mathbb{F}} V$ (we have attached the subscript $\mathbb{F}$ to the tensor product to indicate that this is a tensor product of $\mathbb{F}$-spaces). Let $c \in \mathbb{K}$ and $\widehat{\boldsymbol{v}} = \sum_{i=1}^{n} a_i \otimes_{\mathbb{F}} \boldsymbol{v}_i$, an element in $\mathbb{K} \otimes_{\mathbb{F}} V$. Define the product $c\widehat{\boldsymbol{v}}$ by

$$c\left[\sum_{i=1}^{n} a_i \otimes_{\mathbb{F}} \boldsymbol{v}_i\right] = \sum_{i=1}^{n} (ca_i) \otimes_{\mathbb{F}} \boldsymbol{v}_i.$$

Prove that this satisfies the axioms for scalar multiplication and, consequently, $V_{\mathbb{K}}$, is a vector space over $\mathbb{K}$. This construction is known as “extending the base field” of the space V. It is often used when non-linear irreducible factors divide the minimum polynomial of an operator on a space V. In such a situation the field $\mathbb{K}$ is taken to be an extension of $\mathbb{F}$ which contains all the roots of all the irreducible polynomials that divide the minimum polynomial.

10. Assume V is a finite-dimensional vector space over $\mathbb{F}$ with basis $\mathcal{B} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ and that $\mathbb{K}$ is an extension field of $\mathbb{F}$. Set $\widehat{\boldsymbol{v}}_i = 1 \otimes_{\mathbb{F}} \boldsymbol{v}_i$ and $\widehat{\mathcal{B}} = (\widehat{\boldsymbol{v}}_1, \ldots, \widehat{\boldsymbol{v}}_n)$. Prove that $\widehat{\mathcal{B}}$ is a basis for $V_{\mathbb{K}}$.

11. Let V, W be finite-dimensional vector spaces over $\mathbb{F}$ and $\mathbb{K}$ an extension field of $\mathbb{F}$. Let $\mathcal{L}_{\mathbb{K}}(V_{\mathbb{K}}, W_{\mathbb{K}})$ denote all $\mathbb{K}$-linear transformations from the $\mathbb{K}$-space $V_{\mathbb{K}}$ to the $\mathbb{K}$-space $W_{\mathbb{K}}$. Prove that $\mathcal{L}_{\mathbb{K}}(V_{\mathbb{K}}, W_{\mathbb{K}})$ is isomorphic to $\mathbb{K} \otimes_{\mathbb{F}} \mathcal{L}(V, W)$ as $\mathbb{K}$-spaces.

12. Assume $S_i : V_i \to V_i, i = 1, 2$ are operators of the finite-dimensional vector spaces V_1, V_2. Prove that $Tr(S_1 \otimes S_2) = Tr(S_1)Tr(S_2)$.

13. Let E be an $m \times m$ elementary matrix. Prove that $det(E \otimes I_n) = det(E)^n$.

14. Let V_1 have dimension m, V_2 have dimension n, and let $S_i : V_i \to V_i$ be operators. Prove that $det(S_1 \otimes S_2) = det(S_1)^n det(S_2)^m$.

10.3 The Tensor Algebra

In this section we use the tensor product to construct a universal algebra for a given vector space V.

What You Need to Know

To make sense of the new material in this section, it is essential that you have mastery over the following concepts: vector space, direct sum of a family of vector spaces, basis of a vector space, dimension of a vector space, finite-dimensional vector space, linear transformation, coordinate vector with respect to a basis, matrix of a linear transformation, an associative algebra over a field, multilinear map, multilinear form, bilinear map, bilinear form, the tensor product of vector spaces, and the tensor product of operators.

Before we begin our construction, we recall the definition of the ***direct sum*** of an arbitrary collection of vector spaces:

Let $\mathcal{C} = \{V_i | i \in I\}$ be a collection of vector spaces over $\mathbb{F}$. By the direct sum $\oplus_{i\in I} V_i$ we mean the set of all maps $f : I \to \cup_{i\in I} V_i$ such that a) $f(i) \in V_i$; and b) $spt(f)$ is finite.

Addition and scalar multiplication in $\oplus\, \mathcal{C}$ are defined pointwise: $(f+g)(i) = f(i)+g(i)$ and $(cf)(i) = cf(i)$. Clearly, $spt(f+g) \subset spt(f) \cup spt(g)$ and $spt(cf) = spt(f)$ for $c \neq 0$, so, indeed, $f+g, cf \in \oplus\, \mathcal{C}$.

Let $\epsilon_i : V_i \to \oplus_{i\in I} V_i$ be the map such that $\epsilon_i(\boldsymbol{v})(j) = \mathbf{0}_{V_j}$ if $j \neq i$ and $\epsilon_i(\boldsymbol{v})(i) = \boldsymbol{v}$.

We will need the following theorem that characterizes the direct sum of a family of subspaces $\mathcal{C}$ as the solution to a universal mapping problem.

Theorem 10.8 *Let $\mathcal{C} = \{V_i | i \in I\}$ be a family of vector spaces over a field $\mathbb{F}$. Let W be a vector space over $\mathbb{F}$ and assume there are linear maps $g_i : V_i \to W$. Then there exists a unique linear transformation $G : \oplus_{i\in I} V_i \to W$ such that $G \circ \epsilon_i = g_i$.*

Proof *Let $f \in \oplus_{i\in I} V_i$ so that f is a map from I to $\cup_{i\in I} V_i$ with $f(i) \in V_i$ and $spt(f)$ finite. Suppose then that $spt(f) = \{i_1, \ldots, i_t\}$. Then define $G(f) =$*

$$\sum_{j=1}^{t} g_{i_j}(f(i_j)).$$

We leave it to the reader to show that this is a linear transformation and if G exists then it must be defined this way, that is, it is unique.

Theorem 10.9 *Assume $\mathcal{C} = \{V_i | i \in I\}$ and $\mathcal{D} = \{W_i | i \in I\}$ are two families of vector spaces over a field $\mathbb{F}$, both indexed by the set I. Assume $S_i : V_i \to W_i$ are linear transformations. Then there exists a unique linear transformation $S : \oplus_{i \in I} V_i \to \oplus_{i \in I} W_i$ such that $S(f)(i) = S_i(f(i))$.*

Proof *Let $i \in I$ and let $\widehat{S}_i : V_i \to \oplus_{i \in I} W_i$ as follows: $\widehat{S}_i(\boldsymbol{x})(j) = \mathbf{0}_{W_j}$ if $j \neq i$ and $\widehat{S}_i(\boldsymbol{x})(i) = S_i(\boldsymbol{x})$. This is a linear transformation. By Theorem (10.8) there is a unique linear map $S : \oplus_{i \in I} V_i \to \oplus_{i \in I} W_i$ such that $S(f)(i) = \widehat{S}_i(f(i)) = S(f(i))$.*

We will need the following lemma:

Lemma 10.3 *Let $\mathcal{C} = \{V_i | I \in I\}$ and $\mathcal{D} = \{W_i | i \in I\}$ be two families of vector spaces over a field $\mathbb{F}$ and for each $i \in I$, let $S_i : V_i \to W_i$ be a linear transformation. Let $S : \oplus_{i \in I} V_i \to \oplus_{i \in I} W_i$ be the linear map such that $S(f)(i) = S_i(f(i))$. Then the following hold:*

i) If each S_i is surjective then S is surjective.

ii) If each S_i is injective then S is injective.

iii) If each S_i is bijective then S is bijective.

Proof *i) Let $g \in \oplus_{i \in I} W_i$. Let $J = spt(g)$. Since each S_j is surjective for $j \in J$ there exists $\boldsymbol{v}_j \in V_j$ such that $S_j(\boldsymbol{v}_j) = g(j)$. Now let $f \in \oplus_{i \in I} V_i$ be the element with $spt(f) = J$ and for $j \in J, f(j) = \boldsymbol{v}_j$. Then $S(f) = g$ and S is surjective.*

ii) Suppose $f \in Ker(S)$. Then for each $i \in I, S_i(f(i)) = \mathbf{0}_{W_i}$. However, since S_i is injective it follows that $f(i) = \mathbf{0}_{V_i}$ and therefore f is the identity of $\oplus_{i \in I} V_i$.

iii. This follows from i) and ii).

We will also need to recall some concepts about algebras over a field $\mathbb{F}$.

An ***associative algebra*** over a field $\mathbb{F}$ is a pair $(\mathcal{A}, \cdot)$ consisting of a vector space $\mathcal{A}$ over $\mathbb{F}$ together with a map $\cdot : \mathcal{A} \times \mathcal{A}$ denoted by $(a_1, a_2) \to a_1 \cdot a_2$, which is bilinear and also satisfies $(a_1 \cdot a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3)$.

Also, if $\mathcal{A}$ and $\mathcal{A}'$ are algebras over $\mathbb{F}$, by an algebra homomorphism we mean a linear transformation $\sigma : \mathcal{A} \to \mathcal{A}'$ such that $\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$.

Now let V be a vector space over the field $\mathbb{F}$. We define a sequence of vector spaces $\mathcal{T}_k(V)$ for $k \in \mathbb{N} \cup \{0\} = \mathbb{Z}_{\geq 0}$ as follows:

$$\mathcal{T}_0(V) = \mathbb{F}, \mathcal{T}_1(V) = V \text{ and for } k > 1$$

$$\mathcal{T}_k(V) = \overbrace{V \otimes V \cdots \otimes V}^{k \text{ times}}.$$

Finally, set

$$\mathcal{T}(V) = \oplus_{k=0}^{\infty} \mathcal{T}_k(V).$$

Remark 10.2 *Assume V is an n-dimensional vector space and $k \in \mathbb{Z}_{\geq 0}$. Then the dimension of $\mathcal{T}_k(V)$ is n^k.*

It is our goal to show that there is a natural definition of multiplication on $\mathcal{T}(V)$ that makes it into an associative algebra. Before doing so, we introduce some terminology and notation.

Definition 10.5 *Assume $\boldsymbol{x} \in \mathcal{T}(V), \boldsymbol{x} \neq \mathbf{0}_{T(V)}$. Then $spt(\boldsymbol{x}) \neq \emptyset$ and is finite. Assume $\boldsymbol{x}(d) \neq \mathbf{0}_{\mathcal{T}_d(V)}$ but $\boldsymbol{x}(k) = \mathbf{0}_{\mathcal{T}_k(V)}$ for all $k > d$. Then we will say that the* **degree** *of $\boldsymbol{x}$ is d.*

An element $\boldsymbol{x} \in \mathcal{T}(V)$ is said to be **homogeneous of degree** *d if $\boldsymbol{x} \in \mathcal{T}_d(V)$.*

More generally, when $\boldsymbol{x} \in \mathcal{T}(V)$ and $i \in spt(\boldsymbol{x})$ we will say that $\boldsymbol{x}(i)$ is the **homogeneous part** *of $\boldsymbol{x}$ of degree i. We will often abuse notation and express $\boldsymbol{x}$ as a sum of its homogeneous parts rather than as a function from $\mathbb{Z}_{\geq 0}$.*

Example 10.1 *Let V have dimension one with basis $\boldsymbol{v}$.*

Then $\mathcal{T}_k(V) = \{c\overbrace{\boldsymbol{v} \otimes \cdots \otimes \boldsymbol{v}}^{k \text{ times}} | c \in \mathbb{F}\}$. Thus, the dimension of $\mathcal{T}_k(V)$ is one for each k. The general element of degree 3 is

$$c_0 + c_1\boldsymbol{v} + c_2(\boldsymbol{v} \otimes \boldsymbol{v}) + c_3(\boldsymbol{v} \otimes \boldsymbol{v} \otimes \boldsymbol{v}) \text{ with } c_3 \neq 0.$$

Example 10.2 *Let V have dimension 2 with a basis $(\boldsymbol{v}_1, \boldsymbol{v}_2)$. Then $\mathcal{T}_2(V)$ is spanned by $(\boldsymbol{v}_1 \otimes \boldsymbol{v}_1, \boldsymbol{v}_1 \otimes \boldsymbol{v}_2, \boldsymbol{v}_2 \otimes \boldsymbol{v}_1, \boldsymbol{v}_2 \otimes \boldsymbol{v}_2)$. The typical element of degree two is*

$$c_0 + c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + c_{11}\boldsymbol{v}_1 \otimes \boldsymbol{v}_1 + c_{12}\boldsymbol{v}_1 \otimes \boldsymbol{v}_2 + c_{21}\boldsymbol{v}_2 \otimes \boldsymbol{v}_1 + c_{22}\boldsymbol{v}_2 \otimes \boldsymbol{v}_2,$$

where at least one of $c_{11}, c_{12}, c_{21}, c_{22}$ is not zero.

Suppose $\boldsymbol{x} \in \mathcal{T}_k(V)$ and $\boldsymbol{y} \in \mathcal{T}_l(V)$. Then $\boldsymbol{x} \otimes \boldsymbol{y} \in \mathcal{T}_k(V) \otimes \mathcal{T}_l(V) =$

$$\overbrace{V \otimes \cdots \otimes V}^{k\ times} \otimes \overbrace{V \otimes \cdots \otimes V}^{l\ times}.$$

By Theorem (10.3), $\mathcal{T}_k(V) \otimes \mathcal{T}_l(V)$ is isomorphic to $\mathcal{T}_{k+l}(V)$ by a transformation that takes $(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_k) \otimes (\boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{v}_l)$ to $\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_k \otimes \boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{w}_l$. Using this isomorphism, we will identify $\mathcal{T}_k(V) \otimes \mathcal{T}_l(V)$ with $\mathcal{T}_{k+l}(V)$. We extend this to a multiplication of $\mathcal{T}(V)$ in the following way:

Assume $\boldsymbol{x}$ has degree $d, \boldsymbol{x} = \boldsymbol{x}_0 + \dots \boldsymbol{x}_d$, where $\boldsymbol{x}_i \in \mathcal{T}_i(V)$ and $\boldsymbol{y}$ has degree $e, \boldsymbol{y} = \boldsymbol{y}_0 + \cdots + \boldsymbol{y}_e$ and assume $0 \leq k \leq d+e$. Define

$$(\boldsymbol{x} \cdot \boldsymbol{y})_k = \sum_{i+j=k} \boldsymbol{x}_i \otimes \boldsymbol{y}_j.$$

We then set $\boldsymbol{x} \cdot \boldsymbol{y} = \sum_{k=0}^{d+e} (\boldsymbol{x} \cdot \boldsymbol{y})_k$.

Example 10.3 *Let V be two-dimensional and spanned by $\boldsymbol{v}_1, \boldsymbol{v}_2$ over $\mathbb{R}$. Suppose $\boldsymbol{x} = 3 + [-2\boldsymbol{v}_1 + \boldsymbol{v}_2] + [4(\boldsymbol{v}_1 \otimes \boldsymbol{v}_1) - 3(\boldsymbol{v}_2 \otimes \boldsymbol{v}_2)]$ and $\boldsymbol{y} = 1 + [2(\boldsymbol{v}_1 \otimes \boldsymbol{v}_2) - (\boldsymbol{v}_2 \otimes \boldsymbol{v}_1)] + 2(\boldsymbol{v}_1 \otimes \boldsymbol{v}_1 \otimes \boldsymbol{v}_1 \otimes \boldsymbol{v}_2)$. Then*

$$(\boldsymbol{x} \cdot \boldsymbol{y})_0 = 3,$$

$$(\boldsymbol{x} \cdot \boldsymbol{y})_1 = -2\boldsymbol{v}_1 + \boldsymbol{v}_2,$$

$$(\boldsymbol{x} \cdot \boldsymbol{y})_2 = 4(\boldsymbol{v}_1 \otimes \boldsymbol{v}_1) + 6(\boldsymbol{v}_1 \otimes \boldsymbol{v}_2) - 3(\boldsymbol{v}_2 \otimes \boldsymbol{v}_1) - 3(\boldsymbol{v}_2 \otimes \boldsymbol{v}_2),$$

$$(\boldsymbol{x} \cdot \boldsymbol{y})_3 = -4\boldsymbol{v}_1 \otimes \boldsymbol{v}_1 \otimes \boldsymbol{v}_2 + 2\boldsymbol{v}_1 \otimes \boldsymbol{v}_2 \otimes \boldsymbol{v}_1 + 2\boldsymbol{v}_2 \otimes \boldsymbol{v}_1 \otimes \boldsymbol{v}_2 - \boldsymbol{v}_2 \otimes \boldsymbol{v}_2 \otimes \boldsymbol{v}_1,$$

$$\begin{aligned}(\boldsymbol{x} \cdot \boldsymbol{y})_4 &= 14(\boldsymbol{v}_1 \otimes \boldsymbol{v}_1 \otimes \boldsymbol{v}_1 \otimes \boldsymbol{v}_2) - 4(\boldsymbol{v}_1 \otimes \boldsymbol{v}_1 \otimes \boldsymbol{v}_2 \otimes \boldsymbol{v}_1) \\ &\quad - 6(\boldsymbol{v}_2 \otimes \boldsymbol{v}_2 \otimes \boldsymbol{v}_1 \otimes \boldsymbol{v}_2) + 3(\boldsymbol{v}_2 \otimes \boldsymbol{v}_2 \otimes \boldsymbol{v}_2 \otimes \boldsymbol{v}_1).\end{aligned}$$

We will henceforth write $\boldsymbol{xy}$ for $\boldsymbol{x} \cdot \boldsymbol{y}$ when $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{T}(V)$.

Lemma 10.4 *The multiplication of $\mathcal{T}(V)$ is bilinear: If $\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{y} \in T(V)$ and $c \in \mathbb{F}$, then*

$$(\boldsymbol{x}_1 + \boldsymbol{x}_2)\boldsymbol{y} = \boldsymbol{x}_1\boldsymbol{y} + \boldsymbol{x}_2\boldsymbol{y},$$

$$\boldsymbol{y}(\boldsymbol{x}_1 + \boldsymbol{x}_2) = \boldsymbol{y}\boldsymbol{x}_1 + \boldsymbol{y}\boldsymbol{x}_2,$$

$$(c\boldsymbol{x})\boldsymbol{y} = \boldsymbol{x}(c\boldsymbol{y}) = c(\boldsymbol{xy}).$$

Proof *The additive properties hold because of the way multiplication has been defined. If $\boldsymbol{x}$ and $\boldsymbol{y}$ are decomposable tensors, then the scalar property is satisfied because of the multilinearity of the tensor product. The scalar property then holds for arbitrary $\boldsymbol{x}$ and $\boldsymbol{y}$ as a consequence of the additive properties.*

Lemma 10.5 *For any elements $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in \mathcal{T}(V)$,*

$$(\boldsymbol{x}\boldsymbol{y})\boldsymbol{z} = \boldsymbol{x}(\boldsymbol{y}\boldsymbol{z}). \tag{10.9}$$

Proof *This follows from the bilinearity of multiplication and the fact that (10.9) holds for decomposable vectors.*

In consequence of the previous two lemmas, we have:

Theorem 10.10 *Let V be a vector space over a field $\mathbb{F}$. Then $\mathcal{T}(V)$ is an associative algebra over $\mathbb{F}$.*

Definition 10.6 *Let V be vector space over the field $\mathbb{F}$. Let $\iota : V \to \mathcal{T}(V)$ be the map $\iota(\boldsymbol{v}) = (0, \boldsymbol{v}, \boldsymbol{0}_{\mathcal{T}_2(V)}, \boldsymbol{0}_{\mathcal{T}_3(V)}, \dots)$. This is an injective linear map and can be used to identify V with the subspace of $\mathcal{T}(V)$ consisting of all homogenous elements of degree 1 together with 0. The pair $(\mathcal{T}(V), \iota)$ is the* **tensor algebra** *of V over $\mathbb{F}$.*

Not only is $\mathcal{T}(V)$ an associative algebra, but the pair $(\mathcal{T}(V), \iota)$ is ***universal***. We make the concept of universal precise and prove this assertion in the following theorem.

Theorem 10.11 *Let V be a vector space over a field $\mathbb{F}$, $\mathcal{A}$ an associative algebra over $\mathbb{F}$, and $S : V \to \mathcal{A}$ a linear transformation. Then there exists a unique algebra homomorphism $\sigma : \mathcal{T}(V) \to \mathcal{A}$ such that $\sigma \circ \iota = S$.*

Proof *Set $V^k = \overbrace{V \times \cdots \times V}^{k\ times}$. Define a map $S^k : V^k \to \mathcal{A}$ by $S^k(\boldsymbol{v}_1, \dots, \boldsymbol{v}_k) = S(\boldsymbol{v}_1)S(\boldsymbol{v}_2)\dots S(\boldsymbol{v}_k)$. Then S^k is a multilinear map. By the universality of $\mathcal{T}_k(V)$, there is then a unique linear map $\sigma_k : \mathcal{T}_k(V) \to \mathcal{A}$ which maps a decomposable tensor $\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_k$ to $S(\boldsymbol{v}_1)\dots S(\boldsymbol{v}_k)$.*

By the universality of the direct sum $\oplus_{k \geq 0}\mathcal{T}_k(V)$, there is then a unique linear transformation $\sigma : \mathcal{T}(V) \to \mathcal{A}$ such that σ restricted to $\mathcal{T}_k(V)$ is σ_k. We claim that σ is an algebra homomorphism. Since σ is a linear transformation it only *remains to show that $\sigma(\boldsymbol{xy}) = \sigma(\boldsymbol{x})\sigma(\boldsymbol{y})$. However, since σ is linear we need only prove this for $\boldsymbol{x}, \boldsymbol{y}$ homogenous and, in fact, only for the case where $\boldsymbol{x}$ and $\boldsymbol{y}$ are decomposable tensors. Thus, we may assume that $\boldsymbol{x} = \boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_k$ and $\boldsymbol{y} = \boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{w}_l$. Then*

$$\begin{aligned} \boldsymbol{xy} &= \boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_k \otimes \boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{w}_l, \\ \sigma(\boldsymbol{xy}) &= \sigma_{k+l}(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_k \otimes \boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{w}_l) \\ &= S(\boldsymbol{v}_1) \ldots S(\boldsymbol{v}_k) S(\boldsymbol{w}_1) \ldots S(\boldsymbol{w}_l). \end{aligned}$$

On the other hand

$$\begin{aligned} \sigma(\boldsymbol{x}) &= \sigma_k(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_k) = S(\boldsymbol{v}_1) \ldots S(\boldsymbol{v}_k) \\ \sigma(\boldsymbol{y}) &= \sigma_l(\boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{w}_l) = S(\boldsymbol{w}_1) \ldots S(\boldsymbol{w}_l). \end{aligned}$$

Then

$$\sigma(\boldsymbol{x})\sigma(\boldsymbol{y}) = [S(\boldsymbol{v}_1) \ldots S(\boldsymbol{v}_k)][S(\boldsymbol{w}_1) \ldots S(\boldsymbol{w}_l)] = \sigma(\boldsymbol{xy}).$$

In addition to being universal, the tensor algebra, $\mathcal{T}(V)$, of a vector space V is an example of a graded algebra, a concept we now introduce.

Definition 10.7 *An algebra $\mathcal{A}$ is said to be* **$\mathbb{Z}$-graded** *if it is the internal direct sum of subspaces $\mathcal{A}_k, k \in \mathbb{Z}$, such that*

$$\mathcal{A}_k \mathcal{A}_l \subset \mathcal{A}_{k+l}.$$

Elements of $\mathcal{A}_k$ are said to be **homogeneous of degree** *k.*

When $\mathbf{0} \neq \boldsymbol{x} \in \mathcal{A}$, we can write $\boldsymbol{x}$ uniquely as a sum $\boldsymbol{a}_{j_1} + \cdots + \boldsymbol{a}_{j_t}$ where $j_1 < \cdots < j_t$ and $\mathbf{0}_{\mathcal{A}} \neq \boldsymbol{a}_{j_i} \in \mathcal{A}_{j_i}$. We will refer to $\boldsymbol{a}_{j_i}$ as the **homogeneous part** *of $\boldsymbol{x}$ of degree j_i.*

We work out a couple of examples to give the reader a feel for the tensor algebra.

Example 10.4 *Let V be a one-dimensional vector space with basis $\boldsymbol{x}$. Let $\boldsymbol{x}^k$ denote the vector $\overbrace{\boldsymbol{x} \otimes \cdots \otimes \boldsymbol{x}}^{k\ times}$, which is a basis for $\mathcal{T}_k(V)$. Note that $\boldsymbol{x}^k \cdot \boldsymbol{x}^l = \boldsymbol{x}^k \otimes \boldsymbol{x}^l = \boldsymbol{x}^{k+l}$.*

A typical element of $\mathcal{T}(V)$ of degree d is $(a_0, a_1\boldsymbol{x}, a_2\boldsymbol{x}^2, \ldots, a_d\boldsymbol{x}^d, 0, \ldots)$. Recall *we represent this by the expression* $a_0 + a_1\boldsymbol{x} + a_2\boldsymbol{x}^2 + \cdots + a_d\boldsymbol{x}^d$*. Moreover, the product of this element with an element* $b_0 + b_1\boldsymbol{x} + \cdots + b_e\boldsymbol{x}^e$ *is*

$$\sum_{k=0}^{d+e} \sum_{i,j\geq 0, i+j=k} a_ib_j\boldsymbol{x}^k.$$

This should be familiar. In this case, the tensor algebra $\mathcal{T}(V)$ *is isomorphic to* $\mathbb{F}[x]$*, the algebra of polynomials in a single variable with coefficients in* $\mathbb{F}$*.*

Definition 10.8 *Let x and y be two indeterminates over $\mathbb{F}$, that is, symbols not used to represent elements in $\mathbb{F}$. Let $W_k\{x,y\}$ consist of all words of length k in x and y. We define the product $w \cdot w'$ of a word w of length k and a word w' of length l as the word of length $k+l$ obtained by concatenating w' to the right of w. Set $\mathbb{F}_0\{x,y\} = \mathbb{F}$ and define $\mathbb{F}_k\{x,y\}$ to be the $\mathbb{F}$-vector space based on $W_k\{x,y\}$. Finally, let $\mathbb{F}\{x,y\}$ be the direct sum of $\{\mathbb{F}_k\{x,y\} | k \geq 0\}$. This is the algebra of polynomials in two non-commuting variables over $\mathbb{F}$.*

When V has dimension two with a basis $(\boldsymbol{x}, \boldsymbol{y})$ then $\mathcal{T}(V)$ is isomorphic as an $\mathbb{F}$-algebra to $\mathbb{F}\{x,y\}$. This can be generalized to larger, finite-dimensional spaces.

We now investigate the extension of linear transformations between vector spaces to their respective tensor algebras. Before doing so we define what is meant by a homomorphism of $\mathbb{Z}$-graded algebras.

Definition 10.9 *Assume $\mathcal{A} = \oplus_{n\in\mathbb{Z}}\mathcal{A}_n$ and $\mathcal{B} = \oplus_{n\in\mathbb{Z}}\mathcal{B}_n$ are $\mathbb{Z}$-graded algebras. A $\mathbb{Z}$-graded algebra homomorphism from $\mathcal{A}$ to $\mathcal{B}$ is a linear map $\gamma : \mathcal{A} \to \mathcal{B}$ such that*

1) for every $a_1, a_2 \in \mathcal{A}, \gamma(a_1a_2) = \gamma(a_1)\gamma(a_2)$; and

2) for every $n \in \mathbb{Z}, \gamma(\mathcal{A}_n) \subset \mathcal{B}_n$.

In our next theorem we show how a linear transformation $S : V \to W$ induces a $\mathbb{Z}$-graded homomorphism $\mathcal{T}(S) : \mathcal{T}(V) \to \mathcal{T}(W)$.

Theorem 10.12 *Assume V and W are vector spaces over $\mathbb{F}$ and $S : V \to W$ is a linear transformation. Then then there exists a unique $\mathbb{Z}$-graded algebra homomorphism $\mathcal{T}(S) : \mathcal{T}(V) \to \mathcal{T}(W)$ such that $\iota_W \circ S = \mathcal{T}(S) \circ \iota_V$. Moreover, for $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k \in V, \mathcal{T}(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_k) = S(\boldsymbol{v}_1) \otimes \cdots \otimes S(\boldsymbol{v}_k)$.*

Proof *The composition $\iota_W \circ S$ is a linear map from V to the associative algebra $\mathcal{T}(W)$. By Theorem (10.11) there is a unique algebra homomorphism $\mathcal{T}(S) : \mathcal{T}(V) \to \mathcal{T}(W)$ such that $\iota_W \circ S = \mathcal{T}(S) \circ \iota_V$. It remains to show that $\mathcal{T}(S)$ preserves the gradings, that is, for $k \in \mathbb{Z}_{\geq 0}, \mathcal{T}(S)(\mathcal{T}_k(V)) \subset \mathcal{T}_k(W)$. For $k \in \{0, 1\}$ this is clear. Suppose $k \geq 2$. It suffices to prove if $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)$ is a sequence of vectors from V then $\mathcal{T}(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_k) \in \mathcal{T}_k(W)$. However, $\mathcal{T}(S)(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_k) = S(\boldsymbol{v}_1) \otimes \cdots \otimes S(\boldsymbol{v}_k) \in \mathcal{T}_k(W)$. The last part follows since $\mathcal{T}(S)$ is an algebra homomorphism.*

Let $S : V \to W$ be a linear transformation of vector spaces. We can use Lemma (10.2) to draw conclusions about the algebra homomorphism $\mathcal{T}(S)$ from information about S. We leave the proof as an exercise.

Lemma 10.6 *Let $S : V \to W$ be a linear transformation of vector spaces. Then the following hold:*

i) If S is surjective, then $\mathcal{T}(S)$ is surjective.

ii) If S is injective, then $\mathcal{T}(S)$ is injective.

iii) If S is an isomorphism, then $\mathcal{T}(S)$ is an isomorphism.

The map $S \to \mathcal{T}(S)$ behaves well with respect to composition:

Theorem 10.13 *Let V, W, and X be vector spaces over $\mathbb{F}$, R a linear map from V to W, and S a linear map from W to X. Then $\mathcal{T}(S \cdot R) = \mathcal{T}(S) \cdot \mathcal{T}(R)$.*

By specializing in Theorem (10.13) to the situation where $X = W = V$, we get the following.

Theorem 10.14 *The map $\mathcal{T}$ induces a homomorphism from the group of units, $GL(V)$, in $\mathcal{L}(V, V)$ to the group of units in $\mathcal{L}(\mathcal{T}(V), \mathcal{T}(V)), GL(\mathcal{T}(V))$.*

Exercises

1. Complete the proof of Theorem (10.8).

2. Prove part i) of Lemma (10.6).

3. Prove part ii) of Lemma (10.6).

4. Prove Theorem (10.13).

5. Let V be a three-dimensional vector space over $\mathbb{R}$ and assume $S \in \mathcal{L}(V, V)$ is an operator with distinct eigenvalues $2, 3, 5$. Determine the eigenvalues of $\mathcal{T}_3(S) : \mathcal{T}_3(V) \to \mathcal{T}_3(V)$ along with their multiplicities.

6. Let V be two-dimensional vector space over $\mathbb{R}$ and assume $S \in \mathcal{L}(V, V)$ is

an operator with distinct eigenvalues $2, 3$. Then S is a cyclic operator. Prove that $\mathcal{T}_2(S) : \mathcal{T}_2(V) \to \mathcal{T}_2(V)$ is not cyclic.

7. Let R, S be operators on a vector space V. Either give a proof or else a counterexample to the statement $\mathcal{T}(R + S) = \mathcal{T}(R) + \mathcal{T}(S)$.

8. Assume S is an operator on the n-dimensional vector space V and let $R = Range(S)$ and $K = Ker(S)$. Further, set $R_l = Range(\mathcal{T}_l(S))$ and $K_l = Ker(\mathcal{T}_l(S))$. Is $\mathcal{T}_l(V/K)$ isomorphic to $\mathcal{T}_l(V)/K_l$? Give a proof or a counterexample.

9. Define $\iota_k : V^k \to T_k(V)$ by $\iota_k(\boldsymbol{v}_1, \dots, \boldsymbol{v}_k) = \boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_k$. This map is k-multilinear. Prove that $(\mathcal{T}_k(V), \iota_k)$ is universal, that is, if W is an $\mathbb{F}$-vector space and $f : V^k \to W$ is a k-multilinear map then there exists a unique linear map $F : \mathcal{T}_k(V) \to W$ such that $F \circ \iota_k = f$.

10. Assume $S \in \mathcal{L}(V, V)$ is a nilpotent operator. Prove that $\mathcal{T}_k(S)$ is a nilpotent operator for all k.

11. Let V be a finite-dimensional vector space over a field $\mathbb{F}$ and S an operator on V. Find and prove a formula for $Tr(\mathcal{T}_k(S))$ in terms of $Tr(S)$.

12. Let V be an n-dimensional vector space over a field $\mathbb{F}$ and S an operator on V. Find and prove a formula for $det(\mathcal{T}_k(S))$ in terms of $det(S)$.

10.4 The Symmetric Algebra

In this section we introduce the notion of a homogeneous ideal in a $\mathbb{Z}$-graded algebra. We apply these ideas to the tensor algebra and construct the symmetric algebra of a vector space as quotient space of the tensor algebra by a particular homogeneous ideal. We also show that the symmetric algebra of an n-dimensional vector space over a field $\mathbb{F}$ is isomorphic to the algebra of polynomials in n commuting variables. We will prove that the symmetric algebra is a solution to universal mapping problem.

What You Need to Know

To be successful in understanding the material of this section, you should have already gained mastery of the following concepts: vector space, direct sum of a family of vector spaces, basis of a vector space, dimension of a vector space, finite-dimensional vector space, linear transformation, coordinate vector with respect to a basis, matrix of a linear transformation, an associative algebra over a field, ideal in an algebra, multilinear map, multilinear form, alternating multilinear map, alternating multilinear form, the tensor product of vector spaces, the tensor product of operators, the tensor algebra, and a $\mathbb{Z}$-graded algebra.

We will also make some use of concepts from ring theory, specifically what it means for an ideal in a ring to be generated by a set of elements of the ring.

We will need the concept of a homogeneous ideal of a $\mathbb{Z}$-graded algebra and we begin with this definition.

Definition 10.10 *Assume $\mathcal{A} = \oplus_{k\in\mathbb{Z}}\mathcal{A}_k$ is a $\mathbb{Z}$-graded algebra. An ideal $\mathcal{I}$ of $\mathcal{A}$ is* **homogeneous** *if whenever $\boldsymbol{x} \in \mathcal{I}$ and $\boldsymbol{a}$ is a homogeneous part of $\boldsymbol{x}$, then $\boldsymbol{a} \in \mathcal{I}$. This is equivalent to the statement that $\mathcal{I}$ is equal to the direct sum of its subspaces $\mathcal{I}_k = \mathcal{I} \cap \mathcal{A}_k$.*

Remark 10.3 *Assume $\mathcal{A} = \oplus_{k\in\mathbb{Z}}\mathcal{A}_k$ is a $\mathbb{Z}$-graded algebra and $\mathcal{I}$ is a homogeneous ideal. Set $\mathcal{I}_k = \mathcal{I} \cap \mathcal{A}_k$ for $k \in \mathbb{Z}$. Then*

$$\mathcal{A}/I \cong \oplus_{k\in\mathbb{Z}}\mathcal{A}_k/\mathcal{I}_k.$$

Consequently, $\mathcal{A}/\mathcal{I}$ is a $\mathbb{Z}$-graded algebra.

The following result characterizes homogeneous ideals.

Lemma 10.7 *Let $\mathcal{I}$ be an ideal in a $\mathbb{Z}$-graded algebra $\mathcal{A} = \oplus_{k\in\mathbb{Z}}\mathcal{A}_k$. Then $\mathcal{I}$ is homogeneous if and only if it is generated as an ideal by a set of homogeneous elements.*

Proof *Suppose $\mathcal{I}$ is a homogeneous ideal. Then*

$$\mathcal{I} = \oplus_{k\in\mathbb{Z}}\mathcal{I}_k,$$

where $\mathcal{I}_k = \mathcal{I} \cap \mathcal{A}_k$. Then $\mathcal{I}$ is generated by $\cup_{k\in\mathbb{Z}}\mathcal{I}_k$ as an ideal, a set of homogeneous elements.

On the other hand, assume that $\mathcal{I}$ is generated by a set S of homogeneous elements. Suppose $\boldsymbol{x} \in \mathcal{I}$. Then there are elements $\boldsymbol{s}_1, \dots, \boldsymbol{s}_t \in S$ and elements $\boldsymbol{a}_i, \boldsymbol{b}_i \in \mathcal{A}$, $1 \le i \le t$, such that $\boldsymbol{x} = \boldsymbol{a}_1\boldsymbol{s}_1\boldsymbol{b}_1 + \dots + \boldsymbol{a}_t\boldsymbol{s}_t\boldsymbol{b}_t$. Since the homogeneous part of $\boldsymbol{x}$ of degree k will be the sum of the homogeneous parts of $\boldsymbol{a}_i\boldsymbol{s}_i\boldsymbol{b}_i$ of degree k, it suffices to prove that the homogeneous parts of each $\boldsymbol{a}_i\boldsymbol{s}_i\boldsymbol{b}_i$ belong to $\mathcal{I}$.

Thus, we need to prove that for $\boldsymbol{a}, \boldsymbol{b} \in \mathcal{A}$ and $\boldsymbol{s} \in S$, the homogeneous parts of $\boldsymbol{asb}$ belong to $\mathcal{I}$. Now we can write $\boldsymbol{a} = \boldsymbol{c}_1 + \dots + \boldsymbol{c}_k$ and $\boldsymbol{b} = \boldsymbol{d}_1 + \dots + \boldsymbol{d}_l$, where each $\boldsymbol{c}_i$ and $\boldsymbol{d}_j$ is homogeneous. Then

$$\boldsymbol{asb} = \sum_{i=1}^{k}\sum_{j=1}^{l} \boldsymbol{c}_i\boldsymbol{s}\boldsymbol{d}_j.$$

Each $\boldsymbol{c}_i\boldsymbol{s}\boldsymbol{d}_j$ is homogeneous and belong to $\mathcal{I}$ and this completes the proof.

Let V be a vector space over a field $\mathbb{F}$. As we have remarked, the tensor algebra $\mathcal{T}(V)$ is a $\mathbb{Z}$-graded algebra. Recall that ι is the map from $V \to \mathcal{T}(V)$ which takes $\boldsymbol{v} \in V$ to $(0, \boldsymbol{v}, \boldsymbol{0}_{\mathcal{T}_2(V)}, \dots)$. For ease of notation we will identify $\boldsymbol{v}$ with $\iota(\boldsymbol{v})$, and in this way treat V as a subspace of $\mathcal{T}(V)$.

Now, let $\mathcal{I}$ be the ideal of $T(V)$ generated by all elements of the form $\boldsymbol{v}_1 \otimes \boldsymbol{v}_2 - \boldsymbol{v}_2 \otimes \boldsymbol{v}_1$. By Lemma (10.7), $\mathcal{I}$ is a homogeneous ideal.

Let $\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3 \in V$. We note that $(\boldsymbol{v}_1 \otimes \boldsymbol{v}_2 - \boldsymbol{v}_2 \otimes \boldsymbol{v}_1) \otimes \boldsymbol{v}_3 = \boldsymbol{v}_1 \otimes \boldsymbol{v}_2 \otimes \boldsymbol{v}_3 - \boldsymbol{v}_2 \otimes \boldsymbol{v}_1 \otimes \boldsymbol{v}_3$ is in $\mathcal{I}$. In a similar way, $\boldsymbol{v}_1 \otimes \boldsymbol{v}_2 \otimes \boldsymbol{v}_3 - \boldsymbol{v}_1 \otimes \boldsymbol{v}_3 \otimes \boldsymbol{v}_2 \in \mathcal{I}$. We also have

$$\boldsymbol{v}_1 \otimes \boldsymbol{v}_2 \otimes \boldsymbol{v}_3 - \boldsymbol{v}_2 \otimes \boldsymbol{v}_3 \otimes \boldsymbol{v}_1$$
$$= (\boldsymbol{v}_1 \otimes \boldsymbol{v}_2 \otimes \boldsymbol{v}_3 - \boldsymbol{v}_2 \otimes \boldsymbol{v}_1 \otimes \boldsymbol{v}_3) + (\boldsymbol{v}_2 \otimes \boldsymbol{v}_1 \otimes \boldsymbol{v}_3 - \boldsymbol{v}_2 \otimes \boldsymbol{v}_3 \otimes \boldsymbol{v}_1).$$

Since $\boldsymbol{v}_1 \otimes \boldsymbol{v}_2 \otimes \boldsymbol{v}_3 - \boldsymbol{v}_2 \otimes \boldsymbol{v}_3 \otimes \boldsymbol{v}_1$ is a sum of elements in $\mathcal{I}$, we conclude that it belongs to $\mathcal{I}$. Similarly, $\boldsymbol{v}_1 \otimes \boldsymbol{v}_2 \otimes \boldsymbol{v}_3 - \boldsymbol{v}_3 \otimes \boldsymbol{v}_1 \otimes \boldsymbol{v}_2 \in \mathcal{I}$. Finally,

$$\boldsymbol{v}_1 \otimes \boldsymbol{v}_2 \otimes \boldsymbol{v}_3 - \boldsymbol{v}_3 \otimes \boldsymbol{v}_2 \otimes \boldsymbol{v}_1$$

$$= (\boldsymbol{v}_1 \otimes \boldsymbol{v}_2 \otimes \boldsymbol{v}_3 - \boldsymbol{v}_2 \otimes \boldsymbol{v}_3 \otimes \boldsymbol{v}_1) + (\boldsymbol{v}_2 \otimes \boldsymbol{v}_3 \otimes \boldsymbol{v}_1 - \boldsymbol{v}_3 \otimes \boldsymbol{v}_2 \otimes \boldsymbol{v}_1) \in \mathcal{I}.$$

We have thus shown for π any permutation of $\{1,2,3\}$ and vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3 \in V$ that $\boldsymbol{v}_1 \otimes \boldsymbol{v}_2 \otimes \boldsymbol{v}_3 - \boldsymbol{v}_{\pi(1)} \otimes \boldsymbol{v}_{\pi(2)} \otimes \boldsymbol{v}_{\pi(3)} \in \mathcal{I}_3$. This can be generalized. We state the result as a lemma, but leave the proof as an exercise.

Lemma 10.8 *Let $k \geq 2$ be a natural number, π a permutation of $\{1, 2, \ldots, k\}$ and $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$ vectors in V. Then $\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_k - \boldsymbol{v}_{\pi(1)} \otimes \cdots \otimes \boldsymbol{v}_{\pi(k)}$ is in $\mathcal{I}_k$.*

We define the symmetric algebra to be the quotient of $\mathcal{T}(V)$ by the ideal $\mathcal{I}$.

Definition 10.11 *Let V be a vector space over a field $\mathbb{F}$. Denote by $Sym(V)$ the quotient $\mathcal{T}(V)/\mathcal{I}$ and by ψ the quotient map from $\mathcal{T}(V)$ to $Sym(V)$, an algebra over $\mathbb{F}$. Further, set $\widehat{\iota} = \psi \circ \iota : V \to Sym(V)$. Then the pair $(Sym(V), \widehat{\iota})$ is the* **symmetric algebra** *of V.*

The algebra $Sym(V)$ is a $\mathbb{Z}$-graded algebra with $Sym_k(V) = [\mathcal{T}_k(V) + \mathcal{I}]/\mathcal{I} \equiv \mathcal{T}_k(V)/\mathcal{I}_k$ where $\mathcal{I}_k = \mathcal{I} \cap \mathcal{T}_k(V)$ by Remark (10.3). Since $\mathcal{T}(V)$ is generated as an algebra by $\boldsymbol{v} \in V$ it follows that $Sym(V)$ is generated by all $\boldsymbol{v} + \mathcal{I}$. Let $\boldsymbol{v}, \boldsymbol{w} \in V$. Since $\boldsymbol{v} \otimes \boldsymbol{w} - \boldsymbol{w} \otimes \boldsymbol{v} \in \mathcal{I}$ it follows that $\boldsymbol{v} + \mathcal{I}$ and $\boldsymbol{w} + \mathcal{I}$ commute. Consequently, $Sym(V)$ is a commutative algebra.

The composition $\psi \circ \iota : V \to Sym(V)$ is an injection since $\mathcal{T}_1(V) \cap \mathcal{I} = \{\boldsymbol{0}_{\mathcal{T}(V)}\}$. We will identify an element $\boldsymbol{v} \in V$ with $\widehat{\iota}(\boldsymbol{v})$ and in this way treat V as a direct summand of $Sym(V)$. In the next theorem, we prove that the pair $(Sym(V), \widehat{\iota})$ satisfies a universal mapping property.

Theorem 10.15 *Let V be a vector space over a field $\mathbb{F}$. Assume that $\mathcal{A}$ is a commutative algebra over $\mathbb{F}$ and that $F : V \to \mathcal{A}$ is a linear transformation. Then there exists a unique algebra homomorphism $\widehat{F} : Sym(V) \to \mathcal{A}$ such that $\widehat{F} \circ \widehat{\iota} = F$.*

Proof *Since $(\mathcal{T}(V), \iota)$ is universal and F is a linear map from V to $\mathcal{A}$ there is a unique algebra homomorphism $F' : \mathcal{T}(V) \to \mathcal{A}$ such that $F' \circ \iota = F$. We claim that $\mathcal{I}$ is contained in $Ker(F')$. Thus, let $\boldsymbol{v}, \boldsymbol{w} \in V$. Then*

$$\begin{aligned} F'(\boldsymbol{v} \otimes \boldsymbol{w} - \boldsymbol{w} \otimes \boldsymbol{v}) &= F'(\boldsymbol{v} \otimes \boldsymbol{w}) - F'(\boldsymbol{w} \otimes \boldsymbol{v}) \\ &= F'(\boldsymbol{v})F'(\boldsymbol{w}) - F'(\boldsymbol{w})F'(\boldsymbol{v}) \\ &= F(\boldsymbol{v})F(\boldsymbol{w}) - F(\boldsymbol{w})F(\boldsymbol{v}) = \boldsymbol{0}_{\mathcal{A}}. \end{aligned}$$

This last equality is justified since $\mathcal{A}$ is a commutative algebra.

Since $\mathcal{I} \subset Ker(F')$, there is a unique algebra homomorphism $\widehat{F} : \mathcal{T}(V)/\mathcal{I} \to \mathcal{A}$ such that $\widehat{F} \circ \psi(\boldsymbol{x}) = \widehat{F}(\boldsymbol{x} + \mathcal{I}) = F'(\boldsymbol{x})$. It then follows that

$$\widehat{F} \circ \widehat{\iota} = \widehat{F} \circ (\psi \circ \iota) = (\widehat{F} \circ \psi) \circ \iota$$

$$= F' \circ \iota = F.$$

We now look at the homogenous parts, $Sym_k(V)$, of the symmetric algebra. There is a natural k-multilinear map τ_k from $V^k = V \times \cdots \times V$ (k factors) to $Sym_k(V)$, namely, $\tau_k(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k) = \psi(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_k) = \boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_k + \mathcal{I}$. Since this is the composition of $\iota_k : V^k \to \mathcal{T}_k(V)$, which is k-multilinear and ψ, which is linear, indeed, this map is $k-$multilinear. However, we have more. Since for any π, a permutation of $\{1, 2, \ldots, k\}$, and vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k \in V, \boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_k - \boldsymbol{v}_{\pi(1)} \otimes \cdots \otimes \boldsymbol{v}_{\pi(k)} \in \mathcal{I}$ we can conclude, in fact, that the map $\widehat{\tau_k} = \psi \circ \tau_k : V^k \to Sym_k(V)$ is a symmetric k-multilinear map.

Now suppose $f : V^k \to W$ is a symmetric k-multilinear map. We claim that there is a unique linear transformation $\widehat{f} : Sym_k(V) \to W$ such that $\widehat{f} \circ \widehat{\tau_k} = f$. First of all, by Exercise (9.3.9) we know that $(\mathcal{T}_k(V), \tau_k)$ is universal for k-multilinear maps. Therefore, there exists a linear map $f' : \mathcal{T}_k(V) \to W$ such that $f' \circ \tau_k = f$. We claim that $\mathcal{I}_k$ is contained in the kernel of f'. Any element of $\mathcal{I}_k$ can be written as a sum of elements of the form $\boldsymbol{x} \otimes (\boldsymbol{u} \otimes \boldsymbol{v} - \boldsymbol{v} \otimes \boldsymbol{u}) \otimes \boldsymbol{y}$ where $\boldsymbol{x}$ and $\boldsymbol{y}$ are decomposable vectors. Suppose $\boldsymbol{x} = \boldsymbol{x}_1 \otimes \cdots \otimes \boldsymbol{x}_s$ and $\boldsymbol{y} = \boldsymbol{y}_1 \otimes \cdots \otimes \boldsymbol{y}_t$ where $\boldsymbol{x}_i, \boldsymbol{y}_j \in V$ (and $s + 2 + t = k$). Now

$$f'(\boldsymbol{x} \otimes (\boldsymbol{u} \otimes \boldsymbol{v} - \boldsymbol{v} \otimes \boldsymbol{u}) \otimes \boldsymbol{y}) =$$
$$f'(\boldsymbol{x} \otimes \boldsymbol{u} \otimes \boldsymbol{v} \otimes \boldsymbol{y} - \boldsymbol{x} \otimes \boldsymbol{v} \otimes \boldsymbol{u} \otimes \boldsymbol{y}) =$$
$$f'(\boldsymbol{x} \otimes \boldsymbol{u} \otimes \boldsymbol{v} \otimes \boldsymbol{y}) - f'(\boldsymbol{x} \otimes \boldsymbol{v} \otimes \boldsymbol{u} \otimes \boldsymbol{y}) =$$
$$f'(\boldsymbol{x}_1 \otimes \cdots \otimes \boldsymbol{x}_t \otimes \boldsymbol{u} \otimes \boldsymbol{v} \otimes \boldsymbol{y}_1 \otimes \cdots \otimes \boldsymbol{y}_t) - f'(\boldsymbol{x}_1 \otimes \cdots \otimes \boldsymbol{x}_t \otimes \boldsymbol{v} \otimes \boldsymbol{u} \otimes \boldsymbol{y}_1 \otimes \cdots \otimes \boldsymbol{y}_t) =$$
$$f(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_s, \boldsymbol{u}, \boldsymbol{v}, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_t) - f(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_s, \boldsymbol{v}, \boldsymbol{u}, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_t) = 0.$$

The last equality is justified since f is a symmetric form. Since $\mathcal{I}_k$ is contained in $Ker(f')$, there is a unique induced linear transformation $\widehat{f} : Sym_k(V) = \mathcal{T}_k(V)/\mathcal{I}_k$ to W such that $\widehat{f} \circ \psi = f'$. We then have

$$\widehat{f} \circ \widehat{\tau_k} = \widehat{f} \circ (\psi \circ \tau_k) = (\widehat{f} \circ \psi) \circ \tau_k$$

$$= f' \circ \tau_k = f.$$

We have therefore proved:

Lemma 10.9 *Let V be a vector space over the field $\mathbb{F}$. Then the pair $(Sym_k(V), \widehat{\tau_k})$ is universal for symmetric k-multilinear maps on V.*

We next demonstrate that $Sym(V)$ is a familiar object when V is an n-dimensional vector space over $\mathbb{F}$. However, before moving on to this, a further word about notation. Recall that we are treating V as if it is a subspace of $Sym(V)$, specifically, the homogeneous elements of degree 1. Since $Sym(V)$ is commutative, the order in which we multiply elements does not matter. For ease of notation, when $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$ are elements of V we will denote by $\boldsymbol{v}_1 \ldots \boldsymbol{v}_k$ the element $\psi(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_k)$ in $Sym(V)$. We now prove:

Theorem 10.16 *Let V be a vector over $\mathbb{F}$ with basis $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$. Then $Sym(V)$ is isomorphic to $\mathbb{F}[x_1, \ldots, x_n]$ the polynomial algebra over $\mathbb{F}$ in n commuting variables.*

Proof *Define $T : V \to \mathbb{F}[x_1, \ldots, x_n]$ by $T(\boldsymbol{v}_i) = x_i$. Since $\mathbb{F}[x_1, \ldots, x_n]$ is a commutative algebra there exists an algebra homomorphism $\tau : Sym(V) \to \mathbb{F}[x_1, \ldots, x_n]$ such that $\tau(\boldsymbol{v}_i) = x_i$. Since $\mathbb{F}[x_1, \ldots, x_n]$ is generated by an algebra, τ is surjective. Let τ_k be the restriction of τ to $Sym_k(V)$. Then τ_k is injective and, consequently, τ is injective. Thus, τ is an isomorphism of algebras.*

As with the case of the tensor algebra, a transformation T from a vector space V to a vector space W induces an algebra homomorphism $Sym(T) : Sym(V) \to Sym(W)$.

Theorem 10.17 *Let V and W be vector spaces over $\mathbb{F}$ and $T : V \to W$ a linear transformation. Let $(Sym(V), \widehat{\iota}_V)$ and $(Sym(W), \widehat{\iota}_W)$ be the symmetric algebras of V and W, respectively. Then there exists a unique $\mathbb{Z}$-graded algebra homomorphism, $Sym(T) : Sym(V) \to Sym(W)$ such that $Sym(T) \circ \widehat{\iota}_V = \widehat{\iota}_W \circ T$. Moreover, if $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k \in V$ then $Sym(T)(\boldsymbol{v}_1 \ldots \boldsymbol{v}_k) = T(\boldsymbol{v}_1) \ldots T(\boldsymbol{v}_k)$.*

Proof *Consider the composition $\alpha = \iota_W \circ T : V \to Sym(W)$. By Theorem (10.15) there is a unique algebra homomorphism $Sym(T) : Sym(V) \to Sym(W)$ such that $\iota_W \circ T = Sym(T) \circ \iota_V$. The last statement follows since $Sym(T)$ is an algebra homomorphism. Finally, to show that $Sym(T)$ is a $\mathbb{Z}$-graded algebra homomorphism it suffices to show that a typical generator $\boldsymbol{v}_1 \ldots \boldsymbol{v}_k$ of $Sym_k(V)$ is mapped by $Sym(T)$ to an element of $Sym_k(W)$. Since $Sym(T)(\boldsymbol{v}_1 \ldots \boldsymbol{v}_k) = T(\boldsymbol{v}_1) \ldots T(\boldsymbol{v}_k) \in Sym(W)$ this is the case.*

For the symmetric algebra, we have a result similar to Lemma (10.6):

Lemma 10.10 *Let $T : V \to W$ be a linear transformation of vector spaces. Then the following hold:*

i) If T is surjective, then $Sym(T)$ is surjective.

ii) If T is injective, then $Sym(T)$ is injective.

iii) If T is an isomorphism, then $Sym(T)$ is an isomorphism.

The following is proved in a way entirely similar to the tensor case:

Lemma 10.11 *Let V, W, X be vector spaces over $\mathbb{F}$, $T : V \to W$ and $S : W \to X$ linear transformations. Then $Sym_k(ST) = Sym_k(S)Sym_k(T)$, and $Sym(ST) = Sym(S)Sym(T)$.*

Exercises

1. Let π be a permutation of $\{1, 2, \dots, n\}$ and $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ vectors in a vector space V. Prove that the element $(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_n) - (\boldsymbol{v}_{\pi(1)} \otimes \cdots \otimes \boldsymbol{v}_{\pi(n)})$ is in the ideal $\mathcal{I}$ of $\mathcal{T}(V)$, which is generated by all elements of the form $\boldsymbol{v} \otimes \boldsymbol{w} - \boldsymbol{w} \otimes \boldsymbol{v}$.

2. Assume V is an n-dimensional vector space over a field $\mathbb{F}$ and k is a natural number. Prove that $dim(Sym_k(V)) = \binom{k+n-1}{k}$.

3. Let T be a diagonalizable operator on a finite-dimensional vector space V over $\mathbb{R}$ with eigenvalues $\alpha_1 \leq \cdots \leq \alpha_n$ (not necessarily distinct). Prove that $Sym_k(T)$ is diagonalizable for all k and describe its eigenvalues.

4. Let T be an operator on $\mathbb{R}^3$ with eigenvalues 1, 2, 4. Determine the eigenvalues of $Sym_2(T)$ with their multiplicities. Is this operator cyclic?

5. Let T be an operator on a four-dimensional vector space V and assume the characteristic polynomial of T is $x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$. Express $Tr(Sym_2(T))$ in terms of $a_0, \dots, a_3$.

10.5 The Exterior Algebra

In this section we construct the exterior algebra of a vector space V as a quotient of the tensor algebra of V by a homogeneous ideal. We determine the dimension of this algebra as well as the dimensions of its homogeneous parts. Finally, we show how a linear transformation from a vector space V to a vector space W induces a linear transformation on the exterior algebra and its homogeneous pieces.

What You Need to Know

To be successful in understanding the material of this section, you should have already gained mastery of the following concepts: vector space, direct sum of a family of vector spaces, basis of a vector space, dimension of a vector space, finite-dimensional vector space, linear transformation, coordinate vector with respect to a basis, matrix of a linear transformation, an associative algebra over a field, ideal in an algebra, multilinear map, multilinear form, alternating multilinear map, alternating multilinear form, a $\mathbb{Z}$-graded algebra, homogenous ideal in a $\mathbb{Z}$-graded algebra, the tensor product of vector spaces, the tensor product of operators, and the tensor algebra.

Let V be a vector space over a field $\mathbb{F}$. Let $\mathcal{J}$ be the ideal of $\mathcal{T}(V)$ generated by all elements of the form $\boldsymbol{v}\otimes\boldsymbol{v}$. By Lemma (10.7), $\mathcal{J}$ is a homogeneous ideal. Let $\wedge(V)$ denote the quotient of $\mathcal{T}(V)$ by $\mathcal{J}$. Also, let ϕ denote the quotient map from $\mathcal{T}(V)$ to $\wedge(V)$ so that $\phi(\boldsymbol{v}) = \boldsymbol{v}+\mathcal{J}$ for $\boldsymbol{v}\in\mathcal{T}(V)$. Note that the typical generator $\boldsymbol{v}\otimes\boldsymbol{v}$ of $\mathcal{J}$ has degree two and therefore $\mathcal{J}\cap\mathcal{T}_1(V) = \{\mathbf{0}_{\mathcal{T}(V)}\}$. Consequently, the map $\epsilon = \phi\circ\iota : V\to\wedge(V)$ is an injection. We can now define the exterior algebra based on V:

Definition 10.12 *By the* **exterior algebra** *of the vector space V, we will mean the pair $(\wedge(V),\epsilon)$ consisting of the algebra $\wedge(V)$ and the injection $\epsilon : V\to\wedge(V)$.*

The exterior algebra of a vector space V satisfies a universal mapping property:

Theorem 10.18 *Let V be a vector space, A an associative algebra, and assume there is a linear map $T : V\to A$ such that for every $\boldsymbol{v}\in V, T(\boldsymbol{v})^2 = \mathbf{0}_A$. Then there exists a unique algebra homomorphism $\tau : \wedge(V)\to A$ such that $T = \tau\circ\epsilon$.*

Proof *Since $(\mathcal{T}(V),\iota)$ is universal, there is an algebra homomorphism $T' : \mathcal{T}(V)\to A$ such that $T'\circ\iota = T$. We claim that $\mathcal{J}$ is contained in ker(T'). It* *suffices to prove that a typical generating element,* $\boldsymbol{v} \otimes \boldsymbol{v}$*, of* $\mathcal{J}$ *is in ker*(T')*. Since* T' *is an algebra homomorphism,* $T'(\boldsymbol{v} \otimes \boldsymbol{v}) = T'(\boldsymbol{v})T'(\boldsymbol{v}) = \tau(\boldsymbol{v})^2 = \mathbf{0}_A$*, as required. It then follows that the map* $\tau : \wedge(V) \to A$ *such that for* $\boldsymbol{x} \in \mathcal{T}(V), \tau(\boldsymbol{x} + \mathcal{J}) = T'(\boldsymbol{x})$ *is well-defined (and a homomorphism of algebras). Since* $T' \circ \iota = T$ *and* $\tau \circ \phi = T'$ *we get* $T = (\tau \circ \iota) \circ \phi = \tau \circ (\iota \circ \phi) = \tau \circ \epsilon$ *as required.*

Note that the quotient algebra $\wedge(V) = \mathcal{T}(V)/\mathcal{J}$ is $\mathbb{Z}$-graded with $\wedge^k(V) = (\mathcal{T}_k(V) + \mathcal{J})/\mathcal{J}$ which is isomorphic to $\mathcal{T}_k(V)/\mathcal{J}_k$, where $\mathcal{J}_k = \mathcal{T}_k(V) \cap \mathcal{J}$. Since ϵ is an injection we use it to identify V with $\wedge^1(V)$ and in this way we treat V as a subspace of $\wedge(V)$. Note that since $\mathcal{T}(V)$ is generated as an algebra by $\mathcal{T}_1(V)$, the algebra $\wedge(V)$ is generated by V. We will use the symbol $\wedge$ to represent multiplication in $\wedge(V)$. So, for example, for $\boldsymbol{v}, \boldsymbol{w} \in V$ we have $\phi(\boldsymbol{v} \otimes \boldsymbol{w}) = \boldsymbol{v} \wedge \boldsymbol{w}$.

Next, consider the map from V^k to $\wedge^k(V)$ given by $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k) \to \boldsymbol{w}_1 \wedge \cdots \wedge \boldsymbol{w}_k$. First of all, this map is k-multilinear since it is the composition of the multilinear map taking $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k)$ to $\boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{w}_k$ with the linear map ϕ. However, whenever two consecutive arguments are equal, the result is zero since $\boldsymbol{v} \otimes \boldsymbol{v} \in \mathcal{J}$ and therefore $\boldsymbol{v} \wedge \boldsymbol{v} = 0$. Among other things, this implies that the map $\wedge$ is alternating and allows us to use the results of Section (7.3). In particular, we can conclude

$$\boldsymbol{w}_1 \wedge \cdots \wedge \boldsymbol{w}_k = 0 \tag{10.10}$$

whenever $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k)$ is linearly dependent in V; and for vectors $\boldsymbol{v}, \boldsymbol{w} \in V$

$$\boldsymbol{v} \wedge \boldsymbol{w} = -\boldsymbol{w} \wedge \boldsymbol{v}. \tag{10.11}$$

Our next result concerns the universality of $\wedge^k(V)$.

Lemma 10.12 *Let* V *and* W *be vector spaces over a field* $\mathbb{F}$ *and assume that* $f : V^k \to W$ *is an alternating* k*-multilinear map. Then there exists a unique linear map* $F : \wedge^k(V) \to W$ *such that for vectors* $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k \in V$

$$F(\boldsymbol{v}_1 \wedge \cdots \wedge \boldsymbol{v}_k) = f(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n).$$

Proof *Since* f *is a* k*-multilinear map there exists a unique linear map* $F' : \mathcal{T}_k(V) \to W$ *such that for vectors* $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k \in V$

$$F'(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_k) = f(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k).$$

However, since f *is alternating,* F' *vanishes identically on* $\mathcal{J}_k$*. This implies that there is a unique linear map* F *from* $\wedge^k(V) = \mathcal{T}_k(V)/\mathcal{J}_k$ *to* W *such that* *for vectors $\boldsymbol{x} \in \mathcal{T}_k(V), F(\phi(\boldsymbol{x})) = F'(\boldsymbol{x})$. In particular, if $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$ are in V, then*

$$F(\boldsymbol{v}_1 \wedge \cdots \wedge \boldsymbol{v}_k) = F'(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_k) = f(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k).$$

The next theorem begins to undercover some of the structure of $\wedge(V)$ when V is an n-dimensional vector space. Before we undertake this purpose, we introduce some notation which will prove useful in what follows.

Let k and n be natural numbers such that $1 \leq k \leq n$ As previously defined, we let $\Omega_n^{\{k\}}$ denote the collection of all sequences $(i_1, \ldots, i_k)$, where $1 \leq i_1 < \cdots < i_k \leq n$. Further, for $\mathcal{B} = (\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n)$, a sequence of vectors and $(i) = (i_1, \ldots, i_k) \in \Omega_n^{\{k\}}$ we let $\boldsymbol{w}_{(i)} = \boldsymbol{w}_{i_1} \wedge \cdots \wedge \boldsymbol{w}_{i_k}$. We now find a basis for each $\wedge^k(V)$ when V is an n-dimensional vector space.

Theorem 10.19 *Assume V is an n-dimensional vector space with a basis $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$. Then the following hold:*

i) If $k > n$, then $\wedge^k(V)$ is trivial.

ii) For $k \leq n$, the collection of vectors $\{\boldsymbol{v}_{(i)} | (i) \in \Omega_n^{\{k\}}\}$ is a basis for $\wedge^k(V)$. In particular, the dimension of $\wedge^k(V)$ is $\binom{n}{k}$.

Proof *i) This follows from Equation (10.10) and the fact that any sequence of $n + 1$ or more vectors in V is linearly dependent.*

ii) Let $\boldsymbol{w}_j = \sum_{i=1}^n a_{ij}\boldsymbol{v}_i$. Then using the fact that $\boldsymbol{w} \wedge \boldsymbol{w} = 0$ and $\boldsymbol{v} \wedge \boldsymbol{w} = -\boldsymbol{w} \wedge \boldsymbol{v}$ we can represent $\boldsymbol{w}_1 \wedge \cdots \wedge \boldsymbol{w}_k$ as a linear combination of $\{\boldsymbol{v}_{(i)} | (i) \in \Omega_n^{\{k\}}\}$. So it remains to show that this collection of vectors is linearly independent. We begin with the case that $k = n$.

We know that $\wedge^n(V)$ is spanned by $\boldsymbol{v}_1 \wedge \cdots \wedge \boldsymbol{v}_n$ and so $\wedge^n(V)$ has dimension at most 1. Define a map from V^n to $\mathbb{F}$ as follows. Denote by $T_{(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n)}$ the linear operator on V such that $T_{(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n)}(\boldsymbol{v}_j) = \boldsymbol{w}_j$. Now set $f(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n) = det(T_{(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n)})$. We saw in Section (7.3) that this is an alternating n-multilinear map. By Lemma (10.12), there exists a linear map $F : \wedge^n(V) \to \mathbb{F}$ such that for vectors $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n \in W, F(\boldsymbol{w}_1 \wedge \cdots \wedge \boldsymbol{w}_n) = f(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n)$. Since f is not trivial, F is not trivial and therefore $\wedge^n(V)$ is not trivial. Thus, $\wedge^n(V)$ has dimension 1 with basis $\boldsymbol{v}_1 \wedge \cdots \wedge \boldsymbol{v}_n$.

Now assume that $k < n$. Suppose now that we have a dependence relation

$$\sum_{(i) \in \Omega_n^{\{k\}}} c_{(i)}\boldsymbol{v}_{(i)} = \boldsymbol{0}_{\wedge(V)}. \tag{10.12}$$

For $(i) = (i_1 < \cdots < i_k) \in \Omega_n^{\{k\}}$, let $(i)'$ be the sequence $(j_1 < \cdots < j_{n-k})$

in $\Omega_n^{\{n-k\}}$ *such that* $\{i_1, \ldots, i_k\} \cup \{j_1, \ldots, j_{n-k}\} = \{1, \ldots, n\}$. *Note that if* $(i) \neq (i^*) \in \Omega_n^{\{k\}}$, *then* $\boldsymbol{v}_{(i^*)} \wedge \boldsymbol{v}_{(i)'} = \boldsymbol{0}_{\wedge(V)}$ *whereas* $\boldsymbol{v}_{(i)} \wedge \boldsymbol{v}_{(i)'} = \pm \boldsymbol{v}_1 \wedge \cdots \wedge \boldsymbol{v}_n \neq \boldsymbol{0}_{\wedge(V)}$ *by the case for* $k = n$ *established above.*

Multiplying (10.12) by $\boldsymbol{v}_{(i)'}$ *we obtain*

$$\pm c_{(i)} \boldsymbol{v}_1 \wedge \cdots \wedge \boldsymbol{v}_n = \boldsymbol{0}_{\wedge(V)}.$$

Therefore, $c_{(i)} = 0$ *for each* $(i) \in \Omega_n^{\{k\}}$, *and consequently,* $\{\boldsymbol{v}_{(i)} | (i) \in \Omega_n^{\{k\}}\}$ *is linearly independent and a basis for* $\wedge^k(V)$.

We next investigate how linear transformations between vector spaces give rise to algebra homomorphisms between the corresponding exterior algebras.

Theorem 10.20 *Let* V *and* W *be vector spaces over* $\mathbb{F}$ *and* $S : V \to W$ *a linear transformation. Then there exists a unique* $\mathbb{Z}$*-graded algebra homomorphism* $\wedge(S) : \wedge(V) \to \wedge(W)$ *such that* $\wedge(S) \circ \epsilon_V = \epsilon_W \circ S$. *Moreover, for* $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k \in V, \wedge(S)(\boldsymbol{v}_1 \wedge \cdots \wedge \boldsymbol{v}_k) = S(\boldsymbol{v}_1) \wedge \cdots \wedge S(\boldsymbol{v}_k)$.

Proof *Consider the composition* $\alpha = \epsilon_W \circ S : V \to \wedge(W)$. *For* $\boldsymbol{v} \in V, \alpha(\boldsymbol{v})^2 = \alpha(\boldsymbol{v}) \wedge_W \alpha(\boldsymbol{v}) = S(\boldsymbol{v}) \wedge_W S(\boldsymbol{v}) = \boldsymbol{0}_{\wedge(W)}$. *By Theorem (10.12) there is a unique algebra homomorphism* $\wedge(S) : \wedge(V) \to \wedge(W)$ *such that* $\wedge(S) \circ \epsilon_V = \epsilon_W \circ S$. *Since* $\wedge(S)$ *is an algebra homomorphism it follows for* $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k \in V$ *that* $\wedge(S)(\boldsymbol{v}_1 \wedge \cdots \wedge \boldsymbol{v}_k) = S(\boldsymbol{v}_1) \wedge \cdots \wedge S(\boldsymbol{v}_k)$. *That* $\wedge(S)$ *is a* $\mathbb{Z}$*-graded homomorphism follows from this.*

Let V and W be vector spaces over $\mathbb{F}$ and $S : V \to W$ a linear transformation. Define $S_k : V^k \to \wedge^k(W)$ by $S_k(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k) = S(\boldsymbol{v}_1) \wedge \cdots \wedge S(\boldsymbol{v}_k)$. This is an alternating k-multilinear map. By the universality of $\wedge^k(V)$, there exists a linear map, denoted by $\wedge^k(S)$, from $\wedge^k(V)$ to $\wedge^k(W)$, which takes $\boldsymbol{v}_1 \wedge \cdots \wedge \boldsymbol{v}_k$ to $S(\boldsymbol{v}_1) \wedge \cdots \wedge S(\boldsymbol{v}_k)$. Alternatively, $\wedge^k(S) = \wedge(S)$ restricted to $\wedge^k(V)$.

Not surprisingly, we have the following:

Lemma 10.13 *Let* $S : V \to W$ *be a linear transformation. Then the following hold:*

i) If S *is surjective, then* $\wedge^k(S) : \wedge^k(V) \to \wedge^k(W)$ *is surjective.*

ii) If S *is injective, then* $\wedge^k(S) : \wedge^k(V) \to \wedge^k(W)$ *is injective.*

iii) If S *is an isomorphism, then* $\wedge^k(S) : \wedge^k(V) \to \wedge^k(W)$ *is an isomorphism.*

Proof *We prove i) and leave the others as exercises. Let* $\mathcal{B}_W = (\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m)$ *be a basis for* W*. Clearly, we may assume that* $k \leq m$*. Then* $\{\boldsymbol{w}_{(i)} | (i) \in \Omega_m^{\{k\}}\}$ *is a basis for* $\wedge^k(W)$ *by part ii) of Theorem (10.19). Since* S *is surjective, there exist vectors* $\boldsymbol{v}_j \in V$ *such that* $S(\boldsymbol{v}_j) = \boldsymbol{w}_j$*. Since* $\mathcal{B}_W$ *is a basis for* W*, in particular, it is independent. It then follows that* $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)$ *is linearly independent. By the definition of* $\wedge^k(S)$ *we have* $\wedge^k(S)(\boldsymbol{v}_{(i)}) = \boldsymbol{w}_{(i)}$ *for* $(i) \in \Omega_n^{\{k\}}$*, which proves that* $\wedge^k(S)$ *is surjective.*

The maps induced on the exterior algebra behave nicely with respect to composition:

Lemma 10.14 *Let* $R : V \to W$ *and* $S : W \to X$ *be linear transformations. Then* $\wedge^k(SR) = \wedge^k(S) \wedge^k (R)$*.*

This is left as an exercise.

Lemmas (10.13) and (10.14) have the following consequence: Let V be a vector space. By restricting $\wedge^k$ to the units in $\mathcal{L}(V, V)$, we obtain a group homomorphism into the group of units in $\mathcal{L}(\wedge^k(V), \wedge^k(V))$.

We complete our treatment by considering an operator S on a finite-dimensional vector space V with a basis $\mathcal{B} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ and determine how to compute the matrix of $\wedge^k(S) : \wedge^k(V) \to \wedge^k(V)$ from the matrix of S with respect to $\mathcal{B}$.

First of all, we need a basis, which is an ordered, independent, spanning set of vectors for $\wedge^k(V)$. We already have an independent spanning set, namely $\{\boldsymbol{v}_{(i)} | \ (i) \in \Omega_n^{\{k\}}\}$ so we need to order this set. We do so lexicographically. Thus, we write

$$(i_1, \ldots, i_k) \prec (j_1, \ldots, j_k)$$

if either $i_1 < j_1$ or $i_1 = j_1$, and in the first place that these differ, say, in the t^{th} place, we have $i_t < j_t$.

For example, for $n = 4$ and $k = 2$ we have the order

$$(1, 2) \prec (1, 3) \prec (1, 4) \prec (2, 3) \prec (2, 4) \prec (3, 4).$$

Now assume that the matrix of S with respect to $\mathcal{B}$ is $A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ a_{21} & \ldots & a_{2n} \\ \vdots & \ldots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}$.

Let $(i) = (i_1, \ldots, i_k)$ and $(j) = (j_1, \ldots, j_k)$ be in Ω_k. We determine the coefficient of $\boldsymbol{v}_{(i)}$ in $\wedge^k(S)(\boldsymbol{v}_{(j)})$:

$$\begin{aligned}
\wedge^k(S)(\boldsymbol{v}_{(j)}) &= \wedge^k(S)(\boldsymbol{v}_{j_1} \wedge \cdots \wedge \boldsymbol{v}_{j_k}) \\
&= (\boldsymbol{v}_{j_1}) \wedge \cdots \wedge S(\boldsymbol{v}_{j_k}) \\
&= \left(\sum_{i=1}^{n} a_{ij_1}\boldsymbol{v}_i\right) \wedge \cdots \wedge \left(\sum_{i=1}^{n} a_{ij_k}\boldsymbol{v}_i\right).
\end{aligned}$$

Since we want to compute the coefficient of $\boldsymbol{v}_{(i)} = \boldsymbol{v}_{i_1} \wedge \cdots \wedge \boldsymbol{v}_{i_k}$ in the sums we need only take the sums over those $i \in \{i_1, \ldots, i_k\}$. Thus, we need to compute

$$\left(\sum_{t=1}^{k} a_{i_t,j_1}\boldsymbol{v}_{i_t}\right) \wedge \cdots \wedge \left(\sum_{t=1}^{k} a_{i_t,j_k}\boldsymbol{v}_{i_t}\right).$$

A typical term of this sum is

$$a_{i_{t_1},j_1} \ldots a_{i_{t_k},j_k}\boldsymbol{v}_{i_{t_1}} \wedge \cdots \wedge \boldsymbol{v}_{i_{t_k}}.$$

If any of the indices $i_{t_1}, \ldots, i_{t_k}$ are identical, then the term is zero. Therefore, in order to get a non-zero term, it must be the case that $i_{t_1}, \ldots, i_{t_k}$ is a permutation of $i_1, \ldots, i_k$. So, let π be a permutation of $\{1, 2, \ldots, k\}$. Then we can write the typical non-zero term as

$$a_{i_{\pi(1)},j_1} \ldots a_{i_{\pi(k)},j_k}\boldsymbol{v}_{i_{\pi(1)}} \wedge \cdots \wedge \boldsymbol{v}_{i_{\pi(k)},j_k}.$$

Now $\boldsymbol{v}_{i_{\pi(1)},j_1} \wedge \cdots \wedge \boldsymbol{v}_{i_{\pi(k)},j_k}$ will be ± 1 times $\boldsymbol{v}_{i_1} \wedge \cdots \wedge \boldsymbol{v}_{i_k}$ and the coefficient is determined by the sign of the permutation π. This should look familiar (go back and look at the formula for determinant of a matrix). What we get is the determinant of the $k \times k$ matrix

$$\begin{pmatrix}
a_{i_1,j_1} & \cdots & a_{i_1,j_k} \\
a_{i_2,j_1} & \cdots & a_{i_2,j_k} \\
\vdots & \cdots & \vdots \\
a_{i_k,j_1} & \cdots & a_{i_k,j_k}
\end{pmatrix}.$$

This is just the $k \times k$ matrix obtained from the matrix A by taking the intersection of rows $i_1, \ldots, i_k$ with columns $j_1, \ldots, j_k$. We represent this matrix by the expression $A_{(i),(j)}$ and the coefficient by $a_{(i),(j)}$. Thus,

$$a_{(i),(j)} = det(A_{(i),(j)}).$$

Putting this together we get

$$\wedge^k(\boldsymbol{v}_{(j)}) = \sum_{(i)\in\Omega_k} a_{(i),(j)}\boldsymbol{v}_{(i)}$$

$$= \sum_{(i)\in\Omega_k} det(A_{(i),(j)})\boldsymbol{v}_{(i)}.$$

We complete our exposition with one final definition:

Definition 10.13 *Let V be an n-dimensional vector space, $\mathcal{B} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ a basis for V, and $S : V \to V$ a linear operator. Assume that the matrix of S with respect to $\mathcal{B}$ is A. Let $(i), (j) \in \Omega_n^k$. Then the numbers $det(A_{(i),(j)})$ are the* **Plucker coordinates** *for $S(\boldsymbol{v}_{(j)})$.*

Exercises

1. Let V be a vector space of dimension n, k a natural number with $2 \leq k \leq n$ and π a permutation of $\{1, \dots, k\}$. Prove that $\mathcal{J}_k$ contains all vectors of the form

$$\boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{w}_k - sgn(\pi)(\boldsymbol{w}_{\pi(1)} \otimes \cdots \otimes \boldsymbol{w}_{\pi(k)}).$$

2. Let V be a vector space of dimension n over the field $\mathbb{F}$ with a basis $\mathcal{B} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ and let k be a natural number such that $2 \leq k \leq n$. Prove $\mathcal{J}_k$ is spanned by all vectors of the form $\boldsymbol{w}_1 \otimes \cdots \otimes \boldsymbol{w}_k - sgn(\pi)(\boldsymbol{w}_{\pi(1)} \otimes \cdots \otimes \boldsymbol{w}_{\pi(k)})$, where $(\boldsymbol{w}_1, \dots, \boldsymbol{w}_k) \in \mathcal{B}^k$.

3. Continue with the assumptions of Exercise 2. Prove that $\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_n$ is not contained in $\mathcal{J}_n$. Use this to prove the existence of a unique alternating n-linear form on V, which takes the value 1 on $\mathcal{B}$.

4. Prove Lemma (10.14).

5. Prove part ii) of Lemma (10.13).

6. Let V be a finite-dimensional vector space and $S : V \to V$ a nilpotent operator. Prove that $\wedge(S) : \wedge(V) \to \wedge(V)$ is nilpotent.

7. Let V be an n-dimensional vector space and $S : V \to V$ a diagonalizable operator with eigenvalues $\alpha_1, \dots, \alpha_n$ (not necessarily distinct). Prove that $\wedge^k(S) : \wedge^k(V) \to \wedge^k(V)$ is diagonalizable and determine the eigenvalues of this operator.

8. If S is an operator on the n-dimensional vector space V, express $det(\wedge^k(S))$ in terms of $det(S)$.

9. Give an example of an operator S on $\mathbb{R}^4$, which has no real eigenvalues such that $\wedge^2(S)$ has 2 real eigenvalues.

10. Let V be a space of dimension at least 4 and assume the characteristic of the underlying field is not 2. Prove that there exists a vector $\boldsymbol{x}$ in $\wedge(V)$ such that $\boldsymbol{x} \wedge \boldsymbol{x} \neq 0$.

11. Let V be a vector space of dimension $4k$ and let $\mathcal{B} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_{4k})$ be a basis for V. Set $W = \wedge^{2k}(V)$ and define the map $\delta : W \times W \to \mathbb{F}$ by

$$\boldsymbol{v} \wedge \boldsymbol{w} = \delta(\boldsymbol{v}, \boldsymbol{w})(\boldsymbol{v}_1 \wedge \cdots \wedge \boldsymbol{v}_{4k}).$$

Prove that δ is a non-degenerate symmetric bilinear form.

12. Continue with Exercise 10. In the specific case that $n = 4$, prove that this form is hyperbolic.

13. Let V be a vector space of dimension $2k$ with k odd and let $\mathcal{B} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{2k})$ be a basis for V. Set $W = \wedge^k(V)$ and define the map $\delta : W \times W \to \mathbb{F}$ by

$$\boldsymbol{v} \wedge \boldsymbol{w} = \delta(\boldsymbol{v}, \boldsymbol{w})(\boldsymbol{v}_1 \wedge \cdots \wedge \boldsymbol{v}_{2k}).$$

Prove that γ is a non-degenerate alternating bilinear form.

14. Let V be a four-dimensional real vector space and S an operator on V with characteristic polynomial $x^4 - 8x^3 + 12x - 2$. Determine the characteristic polynomial of $\wedge^2(S)$.

15. Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of the polynomial $x^3 - 6x + 3$. Compute the polynomial of degree 3, which has roots $\alpha_1\alpha_2, \alpha_1\alpha_3, \alpha_2\alpha_3$.

16. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be the roots of the polynomial $x^4 - 3x^3 + 3$. Compute the polynomial of degree 6, which has roots $\alpha_1\alpha_2, \alpha_1\alpha_3, \alpha_1\alpha_4, \alpha_2\alpha_3, \alpha_2\alpha_4, \alpha_3\alpha_4$.

10.6 Clifford Algebras, char $\mathbb{F} \neq 2$

In this section we define the notion of a Clifford algebra of an orthogonal space (V, ϕ) and show that it exists making use of the tensor algebra of V.

What You Need to Know

To be successful in understanding the material of this section, you should have already gained mastery of the following concepts: vector space, direct sum of a family of vector spaces, basis of a vector space, dimension of a vector space, finite-dimensional vector space, linear transformation, coordinate vector with respect to a basis, matrix of a linear transformation, an associative algebra over a field, ideal in an algebra, the tensor product of vector spaces, the tensor product of operators, the tensor algebra, a homomorphism from one algebra to another, and a $\mathbb{Z}$-graded algebra. You will also need to be familiar with the concept of a quadratic form on a vector space, a symmetric bilinear form on a vector space, and an orthogonal space as well as concepts from ring theory, specifically what it means for an ideal in a ring to be generated by a set of elements of the ring, and the quotient ring of a ring modulo an ideal.

Throughout this section, (V, ϕ) is an orthogonal space over a field $\mathbb{F}$ with associated symmetric bilinear form $\langle \ , \ \rangle$. We will momentarily define its Clifford algebra as an application of the tensor algebra of a vector space. The Clifford algebra of an orthogonal space has many important applications, in particular to differential geometry, physics, and digital image processing. Subsequently, we will generally assume that the characteristic of $\mathbb{F}$ is not two and that ϕ is non-degenerate and uncover some of the more fundamental properties of the Clifford algebra (in particular, we will compute its dimension).

We begin by recalling some particularly important definitions. Throughout this section when we refer to an algebra A over a field $\mathbb{F}$ we will mean an associative algebra. When A has a multiplicative identity 1_A, then the center of A (those elements of A which commute with every element of A) contains a copy of $\mathbb{F}$ consisting of all those elements of the form $b \cdot 1_A$ where $b \in \mathbb{F}$. We will identify $\mathbb{F}$ and $\{b \cdot 1_A | b \in \mathbb{F}\}$ and thereby treat $\mathbb{F}$ as a subalgebra of A.

Let $\mathbb{F}$ be a field and A and B two associative algebras over $\mathbb{F}$ with multiplicative identities 1_A and 1_B, respectively. By an algebra homomorphism from A to B we mean a linear map $T : A \to B$ such that $T(1_A) = 1_B$ and $T(xy) = T(x)T(y)$ for $x, y \in A$.

Recall, for a vector space V over $\mathbb{F}$ we defined $\mathcal{T}_0(V) = \mathbb{F}, \mathcal{T}_1(V) = V$ and for $k \in \mathbb{N}, k \geq 2, \mathcal{T}_k(V) = V \otimes \cdots \otimes V$ (where there are k factors). The tensor algebra of V is $\mathcal{T}(V) = \oplus_{k=0}^{\infty} \mathcal{T}_k(V)$, the direct sum of $\{\mathcal{T}_k(V) | k \in \mathbb{Z}_{\geq 0}\}$. We remind the reader that formally, this direct sum consists of infinite sequences $(a_0, a_1, \dots)$ such that $a_k \in \mathcal{T}_k(V)$ and for some $N, a_n = \mathbf{0}_{\mathcal{T}_n(V)}$ for all $n > N$.

However, for convenience and purposes of exposition we are identifying $\mathcal{T}_k(V)$ with those elements $(a_0, a_1, \dots)$ such that $a_j = \mathbf{0}_{\mathcal{T}_j(V)}$ for $j \neq k$ and in this way think of each of the $\mathcal{T}_k(V)$ as a subspace of $\mathcal{T}(V)$.

Definition 10.14 *Let (V, ϕ) be an orthogonal space over the field $\mathbb{F}$ with associated symmetric form $\langle\ ,\ \rangle$. By a* **algebraic realization** *of (V, ϕ) we shall mean a pair (A, d) consisting of an associative algebra A with multiplicative identity 1_A and a linear map $d : V \to A$ such that for all $\boldsymbol{v} \in V, d(\boldsymbol{v})^2 = d(\boldsymbol{v})d(\boldsymbol{v}) = \phi(\boldsymbol{v})$.*

Before proceeding to the definition and construction of the Clifford algebra of an orthogonal space (V, ϕ), we prove some useful properties shared by all algebraic realizations.

Lemma 10.15 *Assume (A, d) is an algebraic realization of (V, ϕ). Then for any $\boldsymbol{u}, \boldsymbol{v} \in V, \langle \boldsymbol{u}, \boldsymbol{v} \rangle = d(\boldsymbol{u})d(\boldsymbol{v}) + d(\boldsymbol{v})d(\boldsymbol{u})$.*

Proof *For vectors $\boldsymbol{u}, \boldsymbol{v}$ we have*

$$\begin{aligned}
\langle \boldsymbol{u}, \boldsymbol{v} \rangle &= \phi(\boldsymbol{u} + \boldsymbol{v}) - \phi(\boldsymbol{u}) - \phi(\boldsymbol{v}) \\
&= d(\boldsymbol{u} + \boldsymbol{v})^2 - d(\boldsymbol{u})^2 - d(\boldsymbol{v})^2 \\
&= [d(\boldsymbol{u}) + d(\boldsymbol{v})]^2 - d(\boldsymbol{u})^2 - d(\boldsymbol{v})^2 \\
&= d(\boldsymbol{u})^2 + d(\boldsymbol{u})d(\boldsymbol{v}) + d(\boldsymbol{v})d(\boldsymbol{u}) + d(\boldsymbol{v})^2 - d(\boldsymbol{u})^2 - d(\boldsymbol{v})^2 \\
&= d(\boldsymbol{u})d(\boldsymbol{v}) + d(\boldsymbol{v})d(\boldsymbol{u}).
\end{aligned}$$

As an immediate corollary we have:

Corollary 10.3 *Let $\boldsymbol{u}, \boldsymbol{v} \in V$. Assume (A, d) is an algebraic realization of (V, ϕ). Then $\boldsymbol{u} \perp \boldsymbol{v}$ if and only if $d(\boldsymbol{v})d(\boldsymbol{u}) = -d(\boldsymbol{u})d(\boldsymbol{v})$.*

Proof *First assume that $\boldsymbol{u} \perp \boldsymbol{v}$. By Lemma (10.15), $0 = \langle \boldsymbol{u}, \boldsymbol{v} \rangle = d(\boldsymbol{u})d(\boldsymbol{v}) + d(\boldsymbol{v})d(\boldsymbol{u})$.*

Conversely, assume $d(\boldsymbol{u})d(\boldsymbol{v}) + d(\boldsymbol{v})d(\boldsymbol{u}) = 0$. Then $\phi(\boldsymbol{u} + \boldsymbol{v}) = d(\boldsymbol{u} + \boldsymbol{v})^2 = [d(\boldsymbol{u}) + d(\boldsymbol{v})]^2 = d(\boldsymbol{u})^2 + d(\boldsymbol{u})d(\boldsymbol{v}) + d(\boldsymbol{v})d(\boldsymbol{u}) + d(\boldsymbol{v})^2 = d(\boldsymbol{u})^2 + d(\boldsymbol{v})^2 = \phi(\boldsymbol{u}) + \phi(\boldsymbol{v})$. Consequently, $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = \phi(\boldsymbol{u} + \boldsymbol{v}) - \phi(\boldsymbol{u}) - \phi(\boldsymbol{v}) = 0$.

Let (A, d) be a realization of the orthogonal space (V, ϕ). In our next result we determine when an element in *Range*(d) is invertible.

Lemma 10.16 *Let (A, d) be an algebraic realization of the orthogonal space (V, ϕ). Let $\boldsymbol{v} \in V$. Then $d(\boldsymbol{v})$ is invertible in A if and only if $\phi(\boldsymbol{v}) \neq 0$.*

Proof *Assume that $\phi(\boldsymbol{v}) \neq 0$. Set $\boldsymbol{x} = \frac{1}{\phi(\boldsymbol{v})} d(\boldsymbol{v})$. Then $\boldsymbol{x} d(\boldsymbol{v}) = \frac{1}{\phi(\boldsymbol{v})} d(\boldsymbol{v})^2 = 1$. Therefore, $\boldsymbol{x} = d(\boldsymbol{v})^{-1}$ and $d(\boldsymbol{v})$ is invertible. Conversely, assume that $d(\boldsymbol{v})$ is invertible, say $\boldsymbol{x} d(\boldsymbol{v}) = 1$. Then $\phi(\boldsymbol{v})\boldsymbol{x}^2 = d(\boldsymbol{v})^2 \boldsymbol{x}^2 = [d(\boldsymbol{v})\boldsymbol{x}]^2 = 1$ and so $\phi(\boldsymbol{v}) \neq 0$.*

Let (V, ϕ) be an orthogonal space. We define the Clifford algebra of (V, ϕ) below. It will be an algebraic realization of (V, ϕ) which is universal amongst all such realizations.

Definition 10.15 *Let (V, ϕ) be an orthogonal space over a field $\mathbb{F}$. A* **Clifford algebra** *of (V, ϕ) is an algebraic realization (C, γ) of (V, ϕ) such that if (A, d) is an algebra realization then there exists a unique algebra homomorphism $\delta : C \to A$ such that $\delta \circ \gamma = d$.*

The definition above refers to "a" Clifford algebra. As is usually the case, the Clifford algebra is unique up to a unique algebra homomorphism. We make this explicit in the following theorem.

Theorem 10.21 *Let (V, ϕ) be an orthogonal space and assume that (C, γ) and (C_1, γ_1) are Clifford algebras of (V, ϕ). Then C and C_1 are isomorphic by a unique algebra isomorphism $\delta : C \to C_1$ such that $\delta \circ \gamma = \gamma_1$.*

Proof *We first remark that since C is a Clifford algebra of (V, ϕ) there is a unique algebra homomorphism $\zeta : C \to C$ such that $\zeta \circ \gamma = \gamma$. Since $I_C \circ \gamma = \gamma$ it follows that $\zeta = I_C$. Similarly, if $\zeta_1 : C_1 \to C_1$ is an algebra homomorphism and $\zeta_1 \circ \gamma_1 = \gamma_1$ then $\zeta_1 = I_{C_1}$.*

Since (C_1, γ_1) is an algebra realization of (V, ϕ) and (C, γ) is a Clifford algebra of (V, ϕ), there exists a unique algebra homomorphism $\delta : C \to C_1$ such that $\delta \circ \gamma = \gamma_1$. Reversing the roles of (C, γ) and (C_1, γ_1) we get a unique algebra homomorphism $\delta_1 : C_1 \to C$ such that $\delta_1 \circ \gamma_1 = \gamma$. It is then the case that $\delta_1 \circ \delta : C \to C$ is an algebra homomorphism and $(\delta_1 \circ \delta) \circ \gamma = \delta_1 \circ (\delta \circ \gamma) = \delta_1 \circ \gamma_1 = \gamma$. Consequently, from the argument of the first paragraph, $\delta_1 \circ \delta = I_C$. In exactly the same way, $\delta \circ \delta_1 = I_{C_1}$.

Definition 10.16 *Assume (V, ϕ) is an orthogonal space. Let $\mathcal{T}(V)$ be the tensor algebra of V and denote by $\mathcal{I}_\phi$ the ideal of $\mathcal{T}(V)$ generated by all elements of the form $\boldsymbol{v} \otimes \boldsymbol{v} - \phi(\boldsymbol{v}) \cdot 1_{\mathbb{F}}$. Set $C(V, \phi) = C(V)$ equal to the quotient $\mathcal{T}(V)/\mathcal{I}_\phi$ and let π be the quotient map from $\mathcal{T}(V)$ to $C(V)$ so that for $\boldsymbol{t} \in \mathcal{T}(V), \pi(\boldsymbol{t}) = \boldsymbol{t} + \mathcal{I}_\phi$. Let j denote the composition of $\iota : V \to \mathcal{T}(V)$ with π so that $j = \pi \circ \iota$ where $\iota : V \to \mathcal{T}(V)$ is the map which takes $\boldsymbol{v} \in V$ to $(\boldsymbol{0}_{\mathbb{F}}, \boldsymbol{v}, \boldsymbol{0}_{\mathcal{T}_2(V)}, \dots)$.*

Before we proceed, a word on convention. We have been treating V as a subspace of $\mathcal{T}(V)$ by identifying an element $\boldsymbol{v} \in V$ with $(\mathbf{0}_{\mathbb{F}}, \boldsymbol{v}, \mathbf{0}_{\mathcal{T}^2(V)}, \ldots)$. Since $\mathcal{T}_1(V)$ intersects $\mathcal{I}_\phi$ trivially, the map j is an injection so that we can then identify V with its image in $C(V)$.

Notation. If $\boldsymbol{a} = \boldsymbol{s} + \mathcal{I}_\phi$ and $\boldsymbol{b} = \boldsymbol{t} + \mathcal{I}_\phi$ are two elements of $C(V)$ then we represent the product $(\boldsymbol{s} + \mathcal{I}_\phi)(\boldsymbol{t} + \mathcal{I}_\phi) = (\boldsymbol{s} \otimes \boldsymbol{t}) + \mathcal{I}_\phi$ by $\boldsymbol{a} \cdot \boldsymbol{b}$ or simply $\boldsymbol{ab}$.

Theorem 10.22 *Let (V, ϕ) be an orthogonal space over a field $\mathbb{F}$ and let $C(V)$ be its Clifford algebra. Then (V, f) is realized by $C(V)$.*

Proof *Let $\boldsymbol{v}$ be a vector in V. Since $\boldsymbol{v} \otimes \boldsymbol{v} - \phi(\boldsymbol{v})1_{\mathbb{F}} \in \mathcal{I}_\phi$ it then follows that $\pi(\boldsymbol{v} \otimes \boldsymbol{v} - \phi(\boldsymbol{v})1_{\mathbb{F}}) = \mathbf{0}_{C(V)}$. However,*

$$\begin{aligned}\pi(\boldsymbol{v} \otimes \boldsymbol{v} - \phi(\boldsymbol{v})1_{\mathbb{F}}) &= \pi(\boldsymbol{v} \otimes \boldsymbol{v}) - \phi(\boldsymbol{v})1_A \\ &= \pi(\boldsymbol{v})^2 - \phi(\boldsymbol{v})1_A \\ &= j(\boldsymbol{v})^2 - \phi(\boldsymbol{v})1_A.\end{aligned}$$

Theorem 10.23 *Let (V, ϕ) be an orthogonal space over a field $\mathbb{F}$. Assume A is an associative algebra with multiplicative identity which realizes (V, ϕ), that is, there exists a linear map $d : V \to A$ such that $d(\boldsymbol{v})^2 = \phi(\boldsymbol{v})1_A$ for every $\boldsymbol{v} \in V$. Then there exists a unique homomorphism of $\mathbb{F}$-algebras $D : C(V) \to A$ such that $d = D \circ j$.*

Proof *Since the tensor algebra is universal, there exists a unique homomorphism τ of $\mathbb{F}$-algebras $\tau : \mathcal{T}(V) \to A$ such that $d = \tau \circ \iota$. We claim that $\mathcal{I}_\phi$ is contained in the kernel of τ. Let $\boldsymbol{u} \in V$. Then $\tau(\boldsymbol{u} \otimes \boldsymbol{u} - \phi(\boldsymbol{u})) = \tau(\boldsymbol{u} \otimes \boldsymbol{u}) - \phi(\boldsymbol{u}) \cdot 1_A = \tau(\boldsymbol{u})^2 - \phi(\boldsymbol{u}) \cdot 1_A = d(\boldsymbol{u})^2 - \phi(\boldsymbol{u}) \cdot 1_A = 0$. Consequently, there exists a unique linear transformation $D : C(V) = \mathcal{T}(V)/\mathcal{I}_\phi \to A$ such that $D(\boldsymbol{a} + \mathcal{I}_\phi)) = \tau(\boldsymbol{a})$. For $\boldsymbol{u} \in V, D(\boldsymbol{u} + \mathcal{I}_\phi) = \tau(\boldsymbol{u}) = d(\boldsymbol{u})$ and therefore $D \circ j = d$. Finally, D is unique since $C(V)$ is generated as an algebra by the subspace V.*

Example 10.5 *Let (V, ϕ) be a non-singular orthogonal space of dimension one over the field $\mathbb{F}$. Assume $\boldsymbol{v} \neq \mathbf{0}$ and $\phi(\boldsymbol{v}) = c$. Then $C(V)$ is spanned by 1 and $\boldsymbol{v}$. Moreover, $\boldsymbol{v}$ satisfies $\boldsymbol{v}^2 - c = 0$. If c is a square in $\mathbb{F}$, say $c = a^2$ then $C(V)$ is isomorphic to $\mathbb{F}[x]/(x^2 - a^2)$ which, in turn, is isomorphic to $\mathbb{F}[x]/(x - a) \oplus \mathbb{F}[x]/(x + a)$. Finally, the latter algebra is isomorphic to $\mathbb{F} \oplus \mathbb{F}$. On the other hand, if c is not a square in $\mathbb{F}$, then $x^2 - c$ is irreducible in $\mathbb{F}[x]$ and $C(V)$ is isomorphic to the field $\mathbb{F}[x]/(x^2 - c)$.*

Now assume that the characteristic of $\mathbb{F}$ is not two and (V, ϕ) is an orthogonal space. Then there exists an orthogonal basis $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ for V. By Corollary (10.3), for $i \neq j, \boldsymbol{v}_i\boldsymbol{v}_j = -\boldsymbol{v}_j\boldsymbol{v}_i$. Set $\boldsymbol{v}_\emptyset = 1$ and for $\alpha = \{i_1 < i_2 < \dots < i_k\}$, a non-empty subset of $[1, n] = \{1, 2, \dots, n\}$, denote by $\boldsymbol{v}_\alpha$ the element $\boldsymbol{v}_{i_1} \dots \boldsymbol{v}_{i_k}$ of $C(V)$.

Lemma 10.17 *Let α be a subset of $[1, n]$ and $j \in [1, n]$.*

i) If $j \notin \alpha$ then $\boldsymbol{v}_\alpha\boldsymbol{v}_j = \pm\boldsymbol{v}_{\alpha\cup\{j\}}$.

ii) If $j \in \alpha$ then $\boldsymbol{v}_\alpha\boldsymbol{v}_j = \pm\phi(\boldsymbol{v}_j)\boldsymbol{v}_{\alpha\setminus\{j\}}$.

We leave this as an exercise.

Remark 10.4 *Assume α is a subset of $[1, n]$ with cardinality k and $j \in [1, n]$. If $j \notin \alpha$ then $\boldsymbol{v}_\alpha\boldsymbol{v}_j = (-1)^k\boldsymbol{v}_j\boldsymbol{v}_\alpha$. If $j \in \alpha$ then $\boldsymbol{v}_\alpha\boldsymbol{v}_j = (-1)^{k-1}\boldsymbol{v}_j\boldsymbol{v}_\alpha$.*

Lemma 10.18 *Let $k \in \mathbb{N}$ and $(i_1, \dots, i_k)$ be a sequence of natural numbers. Then $\boldsymbol{v}_{i_1} \dots \boldsymbol{v}_{i_k}$ is a multiple of $\boldsymbol{v}_\alpha$ for some $\alpha \in [1, n]$.*

Proof *The proof is by induction on k. If $k = 1$ there is nothing to prove. Assume the result has been established for $k \geq 1$ and that $(i_1, \dots, i_{k+1})$ is a sequence of natural numbers. We must show that $\boldsymbol{v}_{i_1} \dots \boldsymbol{v}_{i_k}\boldsymbol{v}_{i_{k+1}}$ is multiple of $\boldsymbol{v}_\alpha$ for some subset α of $[1, n]$. By induction, $\boldsymbol{v}_{i_1} \dots \boldsymbol{v}_{i_k} = c\boldsymbol{v}_\beta$ for some subset β of $[1, n]$ and scalar c. Then by Lemma (10.17) it follows that $\boldsymbol{v}_{i_1} \dots \boldsymbol{v}_{i_k}\boldsymbol{v}_{i_{k+1}} = c\boldsymbol{v}_\beta\boldsymbol{v}_{i_{k+1}}$ is a multiple of $\boldsymbol{v}_\alpha$ where $\alpha = \beta\cup\{i_{k+1}\}$ if $i_{k+1} \notin \beta$ or $\alpha = \beta\setminus\{i_{k+1}\}$ if $i_{k+1} \in \beta$.*

Lemma 10.19 *Fix a basis $\mathcal{B} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ of V. Let S be the set of all $\boldsymbol{v}_\alpha$ such that α is a subset of $[1, n]$. Then S is a spanning set of $C(V)$.*

Proof *First note that $\mathcal{T}_k(V)$ is spanned by all elements of the form $\boldsymbol{u}_1 \otimes \dots \otimes \boldsymbol{u}_k$ where $\boldsymbol{u}_i \in V$ and therefore $C(V)$ is spanned by 1 together with all elements of the form $\boldsymbol{u}_1 \dots \boldsymbol{u}_k$ where $k \in \mathbb{N}$ and $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k \in V$. Assume $\boldsymbol{u}_j = \sum_{i=1}^n a_{ij}\boldsymbol{v}_i$. Then $\boldsymbol{u}_1 \dots \boldsymbol{u}_k$ is a sum of monomials of the form $a_{i_1,1}a_{i_2,2} \dots a_{i_k,k}\boldsymbol{v}_{i_1} \dots \boldsymbol{v}_{i_k}$. Note that $i_1, \dots, i_k$ are not necessarily distinct. By Lemma (10.18), any product $\boldsymbol{v}_{i_1} \dots \boldsymbol{v}_{i_k}$ is a multiple of $\boldsymbol{v}_\alpha$ for some subset α of $[1, n]$.*

We will show below that S is linearly independent and therefore a basis for $C(V)$. Toward that purpose, we introduce the concept of a $\mathbb{Z}_2$-grading and how a $\mathbb{Z}$-grading can be used to obtain a $\mathbb{Z}_2$-grading.

Definition 10.17 *An algebra A is said to be $\mathbb{Z}_2$-graded if there is a direct sum decomposition $A = A^0 \oplus A^1$ such that $A^iA^j \subset A^{i+j}$ where the addition is taken modulo two.*

When an algebra A has a $\mathbb{Z}$-grading, $A = \oplus_{k\in\mathbb{Z}}A_k$, a $\mathbb{Z}_2$-grading can be obtained by setting $A^0 = \oplus_{k\equiv 0\ (2)}A_k, A^1 = \oplus_{k\equiv 1\ (2)}A_k$. In particular, we can obtain a $\mathbb{Z}_2$-grading of $\mathcal{T}(V)$ in this way.

The notion of a homogenous ideal can be extended to algebras with a $\mathbb{Z}_2$-grading:

Definition 10.18 *Assume $A = A^0 \oplus A^1$ is a $\mathbb{Z}_2$-grading of the algebra A. An ideal $\mathcal{I}$ is homogeneous (relative to this grading) if whenever $\boldsymbol{x} = \boldsymbol{x}_0 + \boldsymbol{x}_1 \in \mathcal{I}$ with $\boldsymbol{x}_i \in A^i$, then $\boldsymbol{x}_i \in \mathcal{I}$.*

When $\mathcal{I}$ is a homogenous ideal of the $\mathbb{Z}_2$-graded algebra A, then the quotient $A/\mathcal{I}$ inherits the grading since $A/\mathcal{I} = (A^0 + \mathcal{I})/\mathcal{I} \oplus (A^1 + \mathcal{I})/\mathcal{I}$ is isomorphic to $A^0/(A^0 \cap \mathcal{I}) \oplus A^1/(A^1 \cap \mathcal{I})$.

The next result gives a characterization of homogenous ideals in a $\mathbb{Z}_2$-graded algebra. It is proved just like Lemma (10.7) and we leave its proof as an exercise.

Lemma 10.20 *Assume $A = A^0 \oplus A^1$ is a $\mathbb{Z}_2$-graded algebra and $\mathcal{I}$ is an ideal of A. Then $\mathcal{I}$ is homogenous if and only if $\mathcal{I}$ is generated (as an ideal) by homogenous elements.*

We now apply the above to $\mathcal{T}(V)$. Denote by $\mathcal{T}^0(V) = \oplus_{k\equiv 0\ (2)}\mathcal{T}_k(V)$ and $\mathcal{T}^1(V) = \oplus_{k\equiv 1\ (2)}\mathcal{T}_k(V)$. Recall, the ideal $\mathcal{I}_\phi$ is generated by all elements of the form $\boldsymbol{v}\otimes\boldsymbol{v} - \phi(\boldsymbol{v})$ where $\boldsymbol{v} \in V$. All such elements belong to $\mathcal{T}^0(V)$ and are homogenous with respect to the $\mathbb{Z}_2$-grading. Consequently, $\mathcal{T}(V)/\mathcal{I}_\phi = [\mathcal{T}^0(V)+\mathcal{T}^1(V)]/\mathcal{I}_\phi$ is isomorphic to $\mathcal{T}^0(V)/[\mathcal{T}^0(V)\cap\mathcal{I}_\phi]\oplus\mathcal{T}^1(V)/[\mathcal{T}^1(V\cap\mathcal{I}_\phi]$. Set

$$C_0 = C_0(V) = \pi(\mathcal{T}^0(V)) = [\mathcal{T}^0(V) + \mathcal{I}_\phi]/\mathcal{I}_\phi \cong \mathcal{T}^0(V)/[\mathcal{T}^0(V) \cap \mathcal{I}_\phi]$$

$$C_1 = C_1(C) = \pi(\mathcal{T}^1(V)) = [\mathcal{T}^1(V) + \mathcal{I}_\phi]/\mathcal{I}_\phi \cong \mathcal{T}^1(V)/[\mathcal{T}^1(V) \cap \mathcal{I}_\phi].$$

Since $C(V) = C_0(V) \oplus C_1(V)$ we have a $\mathbb{Z}_2$-grading on $C(V)$. We will momentarily use this to show that $dim(C(V)) = 2^n$ where $dim(V) = n$. First we introduce the notion of a $\mathbb{Z}_2$-graded (twisted) tensor product.

Definition 10.19 *Assume $A = A^0 \oplus A^1$ and $B = B^0 \oplus B^1$ are $\mathbb{Z}_2$-graded algebras over the field $\mathbb{F}$. The $\mathbb{Z}_2$-graded tensor product of A and B, $A\widehat{\otimes}B$, has as its underlying set the vector space*

$$\begin{aligned} A \otimes B &= [A^0 \oplus A^1] \otimes [B^0 \otimes B^1] \\ &= [(A^0 \otimes B^0) \oplus (A^1 \otimes B^1)] \oplus [(A^0 \otimes B^1) \oplus (A^1 \otimes B^0)]. \end{aligned}$$

The multiplication in $A\widehat{\otimes}B$ is as follows: Assume $\boldsymbol{a}_1, \boldsymbol{a}_2 \in A$ are homogeneous and $\boldsymbol{b}_1, \boldsymbol{b}_2 \in B$ are homogeneous. Then $(\boldsymbol{a}_1 \otimes \boldsymbol{b}_1)(\boldsymbol{a}_2 \otimes \boldsymbol{b}_2) = (-1)^{(deg(\boldsymbol{a}_2)deg(\boldsymbol{b}_1)}\boldsymbol{a}_1\boldsymbol{a}_2 \otimes \boldsymbol{b}_1\boldsymbol{b}_2$. The multiplication is extended to all of $A \otimes B$ by bilinearity.

Set $(A\widehat{\otimes}B)^0 = (A^0 \otimes B^0) \oplus (A^1 \otimes B^1)$ and $(A\widehat{\otimes}B)^1 = (A^0 \otimes B^1) \oplus (A^1 \otimes B^0)$.

Theorem 10.24 *If $A = A^0 \oplus A^1$ and $B = B^0 \oplus B^1$ are two $\mathbb{Z}_2$-graded (associative) algebras then $A\widehat{\otimes}B$ is an associative $\mathbb{Z}_2$-graded (associative) algebra.*

Proof *That the multiplication is well-defined follows from the universal properties of the tensor product $A \otimes B$. Since the multiplication, by definition, is bilinear, associativity reduces to the case where $\boldsymbol{x}_i = \boldsymbol{a}_i \otimes \boldsymbol{b}_i, i = 1, 2, 3$ where $\boldsymbol{a}_i \in A$ and $\boldsymbol{b}_i \in B$ are homogenous. Set $d_i = deg(\boldsymbol{a}_i), e_i = deg(\boldsymbol{b}_i)$. Then*

$$\begin{aligned} \boldsymbol{x}_1[\boldsymbol{x}_2\boldsymbol{x}_3] &= (\boldsymbol{a}_1 \otimes \boldsymbol{b}_1)[(\boldsymbol{a}_2 \otimes \boldsymbol{b}_2)(\boldsymbol{a}_3 \otimes \boldsymbol{b}_3)] \\ &= (\boldsymbol{a}_1 \otimes \boldsymbol{b}_1)[(-1)^{d_3e_2}(\boldsymbol{a}_2\boldsymbol{a}_3) \otimes (\boldsymbol{b}_2\boldsymbol{b}_3)] \\ &= (-1)^{(d_2+d_3)e_1}(-1)^{d_3e_2}[\boldsymbol{a}_1(\boldsymbol{a}_2\boldsymbol{a}_3) \otimes [\boldsymbol{b}_1(\boldsymbol{b}_2\boldsymbol{b}_3)] \end{aligned}$$

$$\begin{aligned} [\boldsymbol{x}_1\boldsymbol{x}_2]\boldsymbol{x}_3 &= [(\boldsymbol{a}_1 \otimes \boldsymbol{b}_1)(\boldsymbol{a}_2 \otimes \boldsymbol{b}_2)](\boldsymbol{a}_3 \otimes \boldsymbol{b}_3) \\ &= (-1)^{d_2e_1}[(\boldsymbol{a}_1\boldsymbol{a}_2) \otimes (\boldsymbol{b}_1\boldsymbol{b}_2)(\boldsymbol{a}_3 \otimes \boldsymbol{b}_3) \\ &= (-1)^{d_2e_1}(-1)^{d_3(e_1+e_2}[(\boldsymbol{a}_1\boldsymbol{a}_2)\boldsymbol{a}_3] \otimes [(\boldsymbol{b}_1\boldsymbol{b}_2)\boldsymbol{b}_3]. \end{aligned}$$

Since the multiplication in A is associative, and the multiplication in B is associative, it follows that $[(\boldsymbol{a}_1\boldsymbol{a}_2)\boldsymbol{a}_3] \otimes [(\boldsymbol{b}_1\boldsymbol{b}_2)]\boldsymbol{b}_3 = [\boldsymbol{a}_1(\boldsymbol{a}_2\boldsymbol{a}_3)] \otimes [\boldsymbol{b}_1(\boldsymbol{b}_2\boldsymbol{b}_3)]$. Therefore, equality comes down to whether $d_3e_2+(d_2+d_3)e_1$ and $d_2e_1+d_3(e_1+e_2)$ have the same parity. However, in fact, they are identical.

Assume that A and B are $\mathbb{Z}_2$-graded algebras. The map which takes $\boldsymbol{a} \in A$ to $\boldsymbol{a} \otimes 1_B$ is an injection (and an algebra homomorphism). We will identify

$\boldsymbol{a} \otimes 1_B$ with $\boldsymbol{a}$ and treat A as if it is a subalgebra of $A\widehat{\otimes}B$. Similarly we treat B as a sub algebra of $A\widehat{\otimes}B$.

Let (V, ϕ) be an orthogonal space and assume that we have a decomposition $V = U \oplus W$ where $\langle \boldsymbol{u}, \boldsymbol{w}\rangle = 0$ for $\boldsymbol{u} \in U, \boldsymbol{w} \in W$. We will prove that $C(V)$ is isomorphic to $C(U)\widehat{\otimes}C(W)$. This will allow us to now determine the dimension of $C(V)$ from $dim(V)$.

Theorem 10.25 *Assume (V, ϕ) is an orthogonal space and $V = U \oplus W$ where $\langle \boldsymbol{u}, \boldsymbol{w}\rangle = 0$ for $\boldsymbol{u} \in U, \boldsymbol{w} \in W$. Then $C(V)$ is isomorphic to $C(U)\widehat{\otimes}C(W)$.*

Proof *Define $f : V \to C(U)\widehat{\otimes}C(W)$ as follows: If $\boldsymbol{v} \in V$, write $\boldsymbol{v} = \boldsymbol{u} + \boldsymbol{w}$ where $\boldsymbol{u} \in U, \boldsymbol{w} \in W$. Set $f(\boldsymbol{v}) = \boldsymbol{u} \otimes 1_{C(W)} + 1_{C(U)} \otimes \boldsymbol{w}$. Thus,*

$$\begin{aligned} f(\boldsymbol{v})^2 &= [\boldsymbol{u} \otimes 1_{C(W)} + 1_{C(U)} \otimes \boldsymbol{w}]^2 \\ &= \boldsymbol{u}^2 \otimes 1_{C(W)} - \boldsymbol{u} \otimes \boldsymbol{w} + \boldsymbol{u} \otimes \boldsymbol{w} + 1_{C(U)} \otimes \boldsymbol{w}^2 \\ &= \phi(\boldsymbol{u}) + \phi(\boldsymbol{w}) \\ &= \phi(\boldsymbol{v}). \end{aligned}$$

We have therefore shown that $C(U)\widehat{\otimes}C(W)$ is a realization of (V, ϕ). We will show that if A is an algebra over $\mathbb{F}$ and $\epsilon : V \to A$ is a realization of (V, ϕ), then there is a unique algebra homomorphism $E : C(U)\widehat{\otimes}C(W) \to A$ such that $E \circ f = \epsilon$ which will establish that $C(U)\widehat{\otimes}C(W)$ is isomorphic to $C(V)$. Denote by j_U the injection of U into $C(U)$ and by j_W the injection of W into $C(W)$. Further, let ϵ_U be the restriction of ϵ to U and ϵ_W the restriction of ϵ to W. Then (A, ϵ_U) is a realization of $(U, \phi_{|U})$ and (A, ϵ_W) is a realization of $(W, \phi_{|W})$. By the universality of $C(U)$ there is an algebra homomorphism $\sigma_U : C(U) \to A$ such that $\sigma_U \circ j_U = \epsilon_U$ and, similarly, by the universality of $C(W)$ there is an algebra homomorphism $\sigma_W : C(W) \to A$ such that $\sigma_W \circ j_W = \epsilon_W$. Define $\sigma : C(U) \times C(W) \to A$ by $\sigma(\boldsymbol{x}, \boldsymbol{y}) = \sigma_U(\boldsymbol{x})\sigma_W(\boldsymbol{y})$. Since the multiplication in A is bilinear and each of σ_U, σ_W is linear, it follows that σ is bilinear. By the universality of the tensor product, there is a linear map $E : C(U) \otimes C(W) \to A$ such that $E(\boldsymbol{u} \otimes \boldsymbol{v}) = \sigma_U(\boldsymbol{u})\sigma_W(\boldsymbol{w})$ for $\boldsymbol{u} \in U$ and $\boldsymbol{w} \in W$.

We next claim that E is an algebra homomorphism. Let $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$ be a basis for U and $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_l)$ be a basis for W. For a subset $\alpha = \{i_1 < \cdots < i_s\}$ of $[1, k]$ denote by $\boldsymbol{u}_\alpha$ the element $\boldsymbol{u}_{i_1} \ldots \boldsymbol{u}_{i_s}$ of $C(U)$. Likewise for a subset $\beta = \{j_1 < \cdots < j_t\}$ of $[1, l]$, denote by $\boldsymbol{w}_\beta$ the element $\boldsymbol{w}_{j_1} \ldots \boldsymbol{w}_{j_t}$ of $C(W)$. Since E is linear and the multiplication in each of $C(U), C(W)$, and A is bilinear, it suffices to show that for $\boldsymbol{y}_1, \boldsymbol{y}_2$ homogenous in $C(U)$ and $\boldsymbol{z}_1, \boldsymbol{z}_2$ homogenous in $C(W)$ that $E((\boldsymbol{y}_1 \otimes \boldsymbol{z}_1)(\boldsymbol{y}_2 \otimes \boldsymbol{z}_2)) = E(\boldsymbol{y}_1 \otimes \boldsymbol{z}_1)E(\boldsymbol{y}_2 \otimes \boldsymbol{z}_2))$.

Again, by the bilinearity of multiplication in $C(U), C(W)$, and A and the linearity of E, we can assume that $\boldsymbol{y}_i = \boldsymbol{u}_{\alpha_i}, \boldsymbol{z}_i = \boldsymbol{z}_{\beta_i}$ for $i = 1, 2$.

$$\begin{aligned}
E((\boldsymbol{u}_{\alpha_1} \otimes \boldsymbol{w}_{\beta_1})(\boldsymbol{u}_{\alpha_2} \otimes \boldsymbol{w}_{\beta_2}) &= (-1)^{|\beta_1|\cdot|\alpha_2|} E(\boldsymbol{u}_{\alpha_1}\boldsymbol{u}_{\alpha_2} \otimes \boldsymbol{w}_{\beta_1}\boldsymbol{w}_{\beta_2}) \\
&= (-1)^{|\beta_1|\cdot|\alpha_2|} \sigma(\boldsymbol{u}_{\alpha_1}\boldsymbol{u}_{\alpha_2} \otimes \boldsymbol{w}_{\beta_1}\boldsymbol{w}_{\beta_2})) \\
&= (-1)^{|\beta_1|\cdot|\alpha_2|} \sigma_U(\boldsymbol{u}_{\alpha_1}\boldsymbol{u}_{\alpha_2})\sigma_W(\boldsymbol{w}_{\beta_1}\boldsymbol{w}_{\beta_2}) \\
&= (-1)^{|\beta_1|\cdot|\alpha_2|} \sigma_U(\boldsymbol{u}_{\alpha_1})\sigma_U(\boldsymbol{u}_{\alpha_2})\sigma_W(\boldsymbol{w}_{\beta_1})\sigma_W(\boldsymbol{w}_{\beta_2})
\end{aligned}$$

On the other hand,

$$E(\boldsymbol{u}_{\alpha_1} \otimes \boldsymbol{w}_{\beta_1})E(\boldsymbol{u}_{\alpha_2} \otimes \boldsymbol{w}_{\beta_2}) = \sigma_U(\boldsymbol{u}_{\alpha_1})\sigma_W(\boldsymbol{w}_{\beta_1})\sigma_U(\boldsymbol{u}_{\alpha_2})\sigma_W(\boldsymbol{w}_{\beta_2}).$$

So we must show that

$$\sigma_W(\boldsymbol{w}_{\beta_1})\sigma_U(\boldsymbol{u}_{\alpha_2}) = (-1)^{|\beta_1|\cdot|\alpha_2|}\sigma_U(\boldsymbol{u}_{\alpha_2})\sigma(\boldsymbol{w}_{\beta_1}).$$

Assume that $\alpha_2 = \{i_1 < \cdots < i_s\} \subseteq [1, k]$ and $\beta_1 = \{j_1 < \cdots < j_t\} \subseteq [1, l]$. Then $\boldsymbol{u}_{\alpha_2} = \boldsymbol{u}_{i_1} \ldots \boldsymbol{u}_{i_s}$ and $\boldsymbol{w}_{\beta_1} = \boldsymbol{w}_{j_1} \ldots \boldsymbol{w}_{j_t}$. Thus,

$$\begin{aligned}
\sigma_U(\boldsymbol{u}_{\alpha_2}) &= \sigma_U(\boldsymbol{u}_{i_1} \ldots \boldsymbol{u}_{i_s}) \\
&= \sigma_U(\boldsymbol{u}_{i_1} \ldots \boldsymbol{u}_{i_s}) \\
&= \sigma_U(\boldsymbol{u}_{i_1}) \ldots \sigma_U(\boldsymbol{u}_{i_s}) \\
&= \epsilon_U(\boldsymbol{u}_{i_1}) \ldots \epsilon_U(\boldsymbol{u}_{i_s}) \\
&= \epsilon(\boldsymbol{u}_{i_1}) \ldots \epsilon(\boldsymbol{u}_{i_s}).
\end{aligned}$$

Similarly

$$\sigma_W(\boldsymbol{w}_{\beta_1}) = \epsilon(\boldsymbol{w}_{j_1}) \ldots \epsilon(\boldsymbol{w}_{j_t}).$$

Since for each pair (i, j) we have $\boldsymbol{u}_i \perp \boldsymbol{w}_j$, it follows by Corollary (10.3) that $\epsilon(\boldsymbol{w}_j)\epsilon(\boldsymbol{u}_i) = -\epsilon(\boldsymbol{u}_i)\epsilon(\boldsymbol{w}_j)$. It then follows that

$$\epsilon(\boldsymbol{w}_{j_1}) \ldots \epsilon(\boldsymbol{w}_{j_t})\epsilon(\boldsymbol{u}_{i_1}) \ldots \epsilon(\boldsymbol{u}_{i_s}) = (-1)^{ts}\epsilon(\boldsymbol{u}_{i_1}) \ldots \epsilon(\boldsymbol{u}_{i_s}\epsilon(\boldsymbol{w}_{j_1}) \ldots \epsilon(\boldsymbol{w}_{j_t}).$$

which is what we needed to prove.

We next show that $E \circ f = \epsilon$. Assume that $\boldsymbol{v} = \boldsymbol{u} + \boldsymbol{w}$ where $\boldsymbol{u} \in U, \boldsymbol{w} \in W$, so that $f(\boldsymbol{v}) = f(\boldsymbol{u} + \boldsymbol{w}) = \boldsymbol{u} \otimes 1_{C(W)} + 1_{C(U)} \otimes \boldsymbol{w}$. Thus,

$$\begin{aligned}
E(f(\boldsymbol{v})) &= E(\boldsymbol{u}\otimes 1_{C(W)}+1_{C(U)}\otimes \boldsymbol{w}) \\
&= E(\boldsymbol{u}\otimes 1_{C(W)})+E(1_{C(U)}\otimes \boldsymbol{w}) \\
&= \sigma(\boldsymbol{u},1_{C(W)})\sigma(1_{C(V)},\boldsymbol{w}) \\
&= \sigma_U(\boldsymbol{u})\sigma_W(1_{C(W)})+\sigma_U(1_{C(U)})\sigma_W(\boldsymbol{w}) \\
&= \epsilon(\boldsymbol{u})+\epsilon(\boldsymbol{w}) \\
&= \epsilon(\boldsymbol{u}+\boldsymbol{w}) \\
&= \epsilon(\boldsymbol{v}).
\end{aligned}$$

Finally, since $f(V)$ includes all elements of the form $\boldsymbol{u}\otimes 1_{C(W)}$ and $1_{C(U)}\otimes\boldsymbol{w}$ and $C(U)\widehat{\otimes}C(W)$ is generated as an algebra by these elements,l it follows that E is unique.

We can now determine the dimension of $C(V)$ given the dimension of V.

Theorem 10.26 *Assume (V,ϕ) is an orthogonal space of dimension n. Then $dim(C(V)) = 2^n$. Moreover, if $\mathcal{B} = (\boldsymbol{v}_1,\dots,\boldsymbol{v}_n)$ is a basis for V, then $S(\mathcal{B}) = \{\boldsymbol{v}_\alpha|\ \alpha\subset[1,n]\}$ is a basis for $C(V)$.*

Proof *The proof is by induction on $n = dim(V)$. If $n = 1$ then by Example (10.5) the dimension of $C(V) = 2$. Assume for orthogonal spaces (V,ϕ) of dimension $n-1$ that $dim(C(V)) = 2^{n-1}$ and let us suppose that (V,ϕ) is an orthogonal space of dimension n. Assume ϕ is non-trivial. Then choose any vector $\boldsymbol{w}$ such that $\phi(\boldsymbol{w})\neq 0$ and set $W = Span(\boldsymbol{w}), U = \boldsymbol{w}^\perp$ so that $V = U\oplus W$ where $\langle\boldsymbol{u},a\boldsymbol{w}\rangle = 0$ for all $\boldsymbol{u}\in U$, and $a\boldsymbol{w}\in W$. On the other hand, if ϕ is trivial, choose any decomposition of V as $U\oplus W$ where $dim(U) = n-1$ and the dimension of W is one. Since ϕ is trivial, we have $\langle\boldsymbol{u},\boldsymbol{w}\rangle = 0$ for all $\boldsymbol{u}\in U,\boldsymbol{w}\in W$. By the base case, $dim(C(W)) = 2$ and by the inductive hypothesis $dim(C(U)) = 2^{n-1}$. By Theorem (10.25) it follows that $C(V)$ is isomorphic to $C(U)\widehat{\otimes}C(W)$. As a vector space over $\mathbb{F}$, $C(U)\widehat{\otimes}C(W)$ is equal to $C(U)\otimes C(W)$. Then $dim(C(V)) = dim(C(U)\otimes C(W)) = dim(C(U))\cdot dim(C(W)) = 2^{n-1}\cdot 2 = 2^n$.*

Finally, since $S(\mathcal{B})$ is a spanning set with cardinality 2^n, it follows by Theorem (1.23) that $S(\mathcal{B})$ is a basis of $C(V)$.

Exercises

1. Assume (V,ϕ) is a real orthogonal space of dimension one and for every non-zero vector $\boldsymbol{v}$ assume that $\phi(\boldsymbol{v}) < 0$. Prove that $C(V)$ is isomorphic to the complex numbers.

2. Prove part a) of Lemma (10.17).

3. Prove part b) of Lemma (10.17).

4. Prove Lemma (10.20).

5. Assume (V, ϕ) is a real orthogonal space of dimension two and for all non-zero vectors $\boldsymbol{v}$ assume that $\phi(\boldsymbol{v}) < 0$. Prove that $C(V)$ is isomorphic to the division ring of quaternions.

6. Assume (V, ϕ) is a hyperbolic plane over the field $\mathbb{F}$. Prove that $C(V)$ is isomorphic to $M_{22}(\mathbb{F})$.

This page intentionally left blank

11

Linear Groups and Groups of Isometries

CONTENTS

In this chapter we study certain subgroups of the group of units $GL(V)$ in the algebra $\mathcal{L}(V,V)$ where V is an n-dimensional vector space over a field $\mathbb{F}$. In the first section we consider the normal group $SL(V)$ of $GL(V)$ consisting of those operators of determinant 1. We show that except when $(n,\mathbb{F}) = (2,\mathbb{F}_2)$ or $(3,\mathbb{F}_3)$, this group is perfect, and then prove that the quotient group of $SL(V)$ by its center is a simple group. In the second section we equip V with a non-degenerate alternating bilinear form f and study the group $I(V,f)$ of isometries f. Section three is devoted to isometries of a non-degenerate orthogonal space over a field $\mathbb{F}$ where the characteristic of $\mathbb{F}$ is not two. The final section is concerned with groups of isometries of a finite-dimensional, non-degenerate unitary space.

11.1 Linear Groups

In this section we define the subgroup $SL(V)$ of $GL(V)$ where V is an n-dimensional vector space over the field $\mathbb{F}$. We prove if either $n \geq 3$ or $n = 2$ and $|\mathbb{F}| > 3$ then $SL(V)$ is a perfect group. We also determine the center of the groups $GL(V)$ and $SL(V)$. Finally, we prove that when $SL(V)$ is perfect the quotient of $SL(V)$ by its center is a simple group.

What You Need to Know

To successfully navigate the material of this new section you should by now have mastered the following concepts: vector space over a field $\mathbb{F}$, basis of a vector space, dimension of a vector space, linear operator on a vector space V, matrix of a linear operator $T : V \to V$ with respect to a base $\mathcal{B}$ for V, eigenvalue and eigenvector of an operator T, the algebra $\mathcal{L}(V, V)$ of operators on a finite-dimensional vector space V, an invertible operator on a vector space V, and the group $GL(V)$ of invertible operators on a finite-dimensional vector space V. You must also be familiar with the following concepts from group theory: Abelian group, solvable group, normal subgroup of a group, quotient group of a group by a normal subgroup, the commutator of two elements in a group, the commutator subgroup of a group, a perfect group, the center of a group, a simple group, action of a group G on a set X, transitive action of a group G on a set X, primitive action of a group G on a set X, and a doubly transitive action of a group G on a set X. The latter can be found in Appendix B. We also recommend reviewing a textbook on abstract algebra such as ([2]) or ([3]).

Let V be an n-dimensional vector space over the field $\mathbb{F}$. Recall, by $GL(V)$ we mean the group of units in $\mathcal{L}(V, V)$. This is referred to as the **general linear group** on V. We also denote by $GL_n(\mathbb{F})$ the group of invertible $n \times n$ matrices, which is the group of units in the algebra $M_{nn}(\mathbb{F})$. The groups $GL(V)$ and $GL_n(\mathbb{F})$ are isomorphic as follows: Choose and fix a basis $\mathcal{B} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ for V. Then $T \to \mathcal{M}_T(\mathcal{B}, \mathcal{B})$ is a group isomorphism.

The map $det : GL(V) \to \mathbb{F}^* = \mathbb{F} \setminus \{0\}$ is a group homomorphism. We denote by $SL(V)$ the kernel of this map and refer to this as the **special linear group** on V. It consists of all the operators on V with determinant 1. This is isomorphic to $SL_n(\mathbb{F})$ which is the group of $n \times n$ matrices with determinant equal to one.

In our first lemma we determine the center of the groups $GL(V)$ and $SL(V)$.

Lemma 11.1 *Let V be an n-dimensional vector space. Then the following hold:*

i) The center of $GL(V), Z(GL(V))$ consists of all operators $\lambda I_V, \lambda \in \mathbb{F}^*$.

ii) The center of $SL(V), Z(SL(V))$ consists of all operator $\lambda I_V, \lambda \in \mathbb{F}^*$ such that $\lambda^n = 1$.

Proof *Assume $S \in GL(V)$ and $ST = TS$ for every $T \in SL(V)$. We prove that every non-zero vector of V is an eigenvector. Thus, let $\boldsymbol{v} \neq \mathbf{0}$. Let $\mathcal{B} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ be a basis such that $\boldsymbol{v}_n = \boldsymbol{v}$ and let T be the operator of V such that for $k < n, T(\boldsymbol{v}_k) = \boldsymbol{v}_k + \boldsymbol{v}_{k+1}$ and $T(\boldsymbol{v}_n) = \boldsymbol{v}_n$. Then T is an indecomposable cyclic operator with minimal polynomial $(x-1)^n$. Note that the determinant of T is $(-1)^n(-1)^n = 1$ and therefore $T \in SL(V)$. If $ST = TS$ then $S = f(T)$ for some polynomial $f(x) \in \mathbb{F}[x]$ by Exercise 12 of Section (4.2). In particular, if U is a T-invariant subspace then U is S-invariant. Note that $\boldsymbol{v} = \boldsymbol{v}_n$ is an eigenvector for T with eigenvalue 1 and therefore $Span(\boldsymbol{v})$ is T-invariant, hence S-invariant, and $\boldsymbol{v}$ is an eigenvector for S. Thus, for each vector $\boldsymbol{v} \in V$ there is a scalar $\lambda_{\boldsymbol{v}}$ such that $S(\boldsymbol{v}) = \lambda_{\boldsymbol{v}}\boldsymbol{v}$. We claim that for $(\boldsymbol{v}, \boldsymbol{w})$ linearly independent that $\lambda_{\boldsymbol{v}} = \lambda_{\boldsymbol{w}}$. This follows since , on the one hand, $S(\boldsymbol{v} + \boldsymbol{w}) = \lambda_{\boldsymbol{v}+\boldsymbol{w}}(\boldsymbol{v} + \boldsymbol{w}) = \lambda_{\boldsymbol{v}+\boldsymbol{w}}\boldsymbol{v} + \lambda_{\boldsymbol{v}+\boldsymbol{w}}\boldsymbol{w}$ and, on the other hand, $S(\boldsymbol{v}+\boldsymbol{w}) = S(\boldsymbol{v})+S(\boldsymbol{w}) = \lambda_{\boldsymbol{v}}\boldsymbol{v}+\lambda_{\boldsymbol{w}}\boldsymbol{w}$. Therefore $\lambda_{\boldsymbol{v}} = \lambda_{\boldsymbol{v}+\boldsymbol{w}} = \lambda_{\boldsymbol{w}}$. If $(\boldsymbol{v}, \boldsymbol{w})$ is linearly dependent then $\lambda_{\boldsymbol{v}} = \lambda_{\boldsymbol{w}}$. Now set $\lambda = \lambda_{\boldsymbol{v}}$. Then $S = \lambda I_V$. When $S \in GL(V)$ there are no conditions on λ (other than λ is not equal to zero). When $S \in SL(V), det(S) = \lambda^n = 1$.*

Remark 11.1 *If $\mathbb{F} = \mathbb{F}_2$, then $GL(V) = SL(V)$ and $Z(SL(V)) = \{I_V\}$.*

Definition 11.1 *Let V be an n-dimensional vector space over the field $\mathbb{F}$ and assume $1 \leq k < n$. We will denote by $L_k(V)$ the collection of all subspaces of V of dimension k.*

Define an action of the group $GL(V)$ on $L_k(V)$ by $T \cdot X = T(X) := \{T(\boldsymbol{x}) | \boldsymbol{x} \in X\}$ which has dimension k since T is invertible. Recall for an action of a group G on a set X the kernel of the action consists of all those elements $g \in G$ such that $g \cdot x = x$ for all $x \in X$. In the next lemma we prove that kernel of the action just defined by $GL(V)$ on $L_k(V)$ is $Z(GL(V))$.

Lemma 11.2 *Assume $T \in GL(V)$ and for every $U \in L_k(V)$ that $T(U) = U$. Then $T \in Z(GL(V))$.*

Proof *If $k = 1$, this is true by the proof of Lemma (11.1). We leave the case $k > 1$ as an exercise.*

Lemma 11.3 *Assume V is n-dimensional with $n \geq 2$. Then $SL(V)$ is doubly transitive on $L_1(V)$.*

Proof *Assume (X_1, X_2) and (Y_1, Y_2) two pairs of distinct one-dimensional subspaces of V. Let $\boldsymbol{x}_i \in X_i$ and $\boldsymbol{y}_i \in Y_i$. By Exercise 14 of Section (1.6) there is an $(n-2)$ dimensional subspace Z such that $Span(\boldsymbol{x}_1, \boldsymbol{x}_2) \oplus Z = V = Span(\boldsymbol{y}_1, \boldsymbol{y}_2) \oplus Z$. Let $\boldsymbol{z}_1, \ldots, \boldsymbol{z}_{n-2}$ be a basis of Z. Then $\mathcal{B} = (\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{z}_1, \ldots, \boldsymbol{z}_{n-2})$ and $\mathcal{B}' = (\boldsymbol{y}_1, \boldsymbol{y}_2, \boldsymbol{z}_1, \ldots, \boldsymbol{z}_{n-2})$ are bases of V. Let T be the operator on V such that $T(\boldsymbol{x}_i) = \boldsymbol{y}_i, i = 1, 2$; and $T(\boldsymbol{z}_j) = \boldsymbol{z}_j, 1 \leq j \leq n-2$. Since the image of the basis $\mathcal{B}$ is the basis $\mathcal{B}'$, $T \in GL(V)$. Set $a = det(T)$. Then define S such that $S(\boldsymbol{x}_1) = \frac{1}{a}\boldsymbol{y}_1, S(\boldsymbol{x}_2) = \boldsymbol{y}_2$ and $S(\boldsymbol{z}_j) = \boldsymbol{z}_j$ for $1 \leq j \leq n-2$. Then $S \in SL(V), S(X_i) = Y_i$ for $i = 1, 2$.*

Corollary 11.1 *The action of $SL(V)$ on $L_1(V)$ is primitive.*

Definition 11.2 *Let V be an n-dimensional vector space over a field $\mathbb{F}, H$ a hyperplane of V (i.e. a subspace of dimension $n-1$) and P a one-dimensional subspace of H. A non-identity operator τ of V is said to be a* **transvection with axis** *H* **and center** *P if $T(\boldsymbol{x}) = \boldsymbol{x}$ for $\boldsymbol{x} \in H$ and for arbitrary $\boldsymbol{v} \in V, T(\boldsymbol{v}) - \boldsymbol{v} \in P$. The collection of all transvections with axis H and center P along with the identity operator I_V, is denoted by $\chi(P, H)$. We denote by $\Omega(V)$ the subgroup of $SL(V)$ generated by all $\chi(P, H)$.*

Remark 11.2 *If T is a transvection then the minimal polynomial of T is $(x-1)^2$ and the characteristic polynomial is $(x-1)^n$. Thus, $det(T) = 1$ and $T \in SL(V)$.*

Lemma 11.4 *Let $\boldsymbol{u}, \boldsymbol{v}$ be non-zero vectors. Then there exists $S \in \Omega$ such that $S(\boldsymbol{u}) = \boldsymbol{v}$.*

Proof *First assume that $(\boldsymbol{x}, \boldsymbol{y})$ is linearly independent. Choose a hyperplane H of V such that $\boldsymbol{z} = \boldsymbol{y} - \boldsymbol{x} \in H, \boldsymbol{x} \notin H$ and set $Z = Span(\boldsymbol{z})$. Let S be the unique element of $\chi(Z, H)$ such that $S(\boldsymbol{x}) = \boldsymbol{x} + \boldsymbol{z} = \boldsymbol{y}$. Clearly $S \in \Omega$.*

On the other hand, suppose $\boldsymbol{y}$ is a multiple of $\boldsymbol{x}$. Chose $\boldsymbol{u} \in V \setminus Span(\boldsymbol{x})$. By what we have shown, there are transvections T_1 and T_2 such that $T(\boldsymbol{x}) = \boldsymbol{u}$ and $T_2(\boldsymbol{u}) = \boldsymbol{y}$. Set $S = T_2T_1$. Then $S \in \Omega$ and $S(\boldsymbol{x}) = \boldsymbol{y}$ as required.

Lemma 11.5 *Assume $dim(U) = n-2$ and X_1, X_2, X_3 are distinct hyperplanes containing U. Let P_1 be a one space contained in X_1 such that $X_1 = P_1 \oplus U$. Then there exists $S \in \chi(P_1, X_1)$ such that $\sigma(X_2) = X_3$.*

Proof *Let $\boldsymbol{x}_1$ be a non-zero vector in P_1 and choose any vector $\boldsymbol{x}_2 \in X_2 \setminus U$. The intersection $Span(\boldsymbol{x}_1, \boldsymbol{x}_2) \cap X_3$ is a one-dimensional subspace by the Grassmannian formula (see Exercise 8 of Section (1.6)). Let $\boldsymbol{x}_3 = a\boldsymbol{x}_1 + b\boldsymbol{x}_2$ be a non-zero element of $Span(\boldsymbol{x}_1, \boldsymbol{x}_2) \cap X_3$. Let S be the operator on V such that S restricted to X_1 is the identity and $S(\boldsymbol{x}_2) = \frac{a}{b}\boldsymbol{x}_1 + \boldsymbol{x}_2$. Then $S \in \chi(P_1, X_1)$ and $S(b\boldsymbol{x}_2) = b(\frac{a}{b}\boldsymbol{x}_1 + \boldsymbol{x}_2) = a\boldsymbol{x}_1 + b\boldsymbol{x}_2 = \boldsymbol{x}_3$ and therefore $S(X_2) = X_3$.*

Lemma 11.6 *Assume $n = 2$. Then $\Omega = SL(V)$.*

Proof *Let $T \in SL(V)$ and $\mathcal{B} = (\boldsymbol{u}_1, \boldsymbol{u}_2)$ a basis of V. Set $U = Span(\boldsymbol{u}_1)$, and $\boldsymbol{w}_i = T(\boldsymbol{u}_i), i = 1, 2$. Then also $(\boldsymbol{w}_1, \boldsymbol{w}_2)$ is a basis of V. By Lemma (11.4) there is an element $S \in \Omega$ such that $S(\boldsymbol{u}_1) = \boldsymbol{w}_1$. Set $\boldsymbol{w}_2' = S(\boldsymbol{u}_2)$. Then $(\boldsymbol{w}_1, \boldsymbol{w}_2')$ is a basis of V. Suppose $\boldsymbol{w}_2' = a\boldsymbol{w}_2$. Then $S^{-1}T(\boldsymbol{w}_1)$ has determinant one since $S, T \in SL(V)$. However, $S^{-1}T(\boldsymbol{v}_1) = \boldsymbol{v}_1$ and $S^{-1}T(\boldsymbol{v}_2) = \frac{1}{a}\boldsymbol{v}_2$. Therefore, $S^{-1}T$ has determinant $\frac{1}{a}$. Consequently, $a = 1$ and $S = T$. Thus we may assume that $(\boldsymbol{w}_2, \boldsymbol{w}_2')$ is linearly independent.*

Write $\boldsymbol{w}_2$ as a linear combination of $\boldsymbol{w}_1$ and $\boldsymbol{w}_2'$: $\boldsymbol{w}_2 = c\boldsymbol{w}_1 + d\boldsymbol{w}_2'$. Then $S^{-1}T(\boldsymbol{v}_1) = \boldsymbol{v}_1$ and $S^{-1}T(\boldsymbol{v}_2) = S^{-1}(\boldsymbol{w}_2) = S^{-1}(c\boldsymbol{w}_1 + d\boldsymbol{w}_2') = c\boldsymbol{v}_1 + d\boldsymbol{v}_2$. Then $det(S^{-1}T) = d$. However, $S^{-1}T \in SL(V)$ so $d = 1$. It now follows that that $S' = S^{-1}T$ is a transvection with center U, that is, $S' \in \chi(U, U)$. Now $T = S'S$ is a product of transvections.

Theorem 11.1 *If V is an n-dimensional vector space with $n \geq 2$ then $SL(V)$ is generated by its transvections, that is, $\Omega(V) = SL(V)$.*

Proof *The proof is by induction n. We have already proved this for the base case, $n = 2$, in Lemma (11.6). Assume the result is true for spaces of dimension n and that $dim(V) = n + 1$. We first prove if $T \in SL(V)$ and T has an eigenvector with eigenvalue 1, then $T \in \Omega$. So assume $T(\boldsymbol{x}) = \boldsymbol{x}$. Let Y be a hyperplane of V such that $\boldsymbol{x} \notin Y$. Set $Z = T(Y)$. If $Z = Y$ then $T_{|Y}$ has determinant 1 and we can apply the inductive hypothesis.*

So assume $Z \neq Y$ and set $U = Y \cap Z$ which has dimension $n-1$ and set $X = Span(\boldsymbol{x}) \oplus U$. By Lemma (11.5) there is an element $S \in \chi(Span(\boldsymbol{x}), X)$ such that $S(Y) = Z$. Set $T' = S^{-1}T$. Then $T'(\boldsymbol{x}) = \boldsymbol{x}$ and $T'(Y) = Y$; and so we are done by the first part of the proof.

Finally, we consider the general case. Let $T \in SL(V)$. Clearly we may assume $T \neq I_V$. Choose a vector $\boldsymbol{x}$ such that $T(\boldsymbol{x}) = \boldsymbol{y} \neq \boldsymbol{x}$. By Lemma (11.4) there is an element $S \in \Omega$ such that $S(\boldsymbol{x}) = \boldsymbol{y}$. Set $T' = S^{-1}T$. Then $T'(\boldsymbol{x}) = \boldsymbol{x}$; so we are done by the first case.

Our next goal is to prove that with the exceptions $(n, \mathbb{F}) = (2, \mathbb{F}_2)$ and $(2, \mathbb{F}_3)$ the group $SL(V)$ is perfect. Recall this means that $SL(V)$ is equal to its commutator subgroup: the subgroup, $SL(V)'$, generated by all elements of the form $[S, T] = S^{-1}T^{-1}ST$ as S and T range over $SL(V)$. The commutator subgroup is a characteristic subgroup, hence it is normal. We show directly below that $SL(V)$ is transitive on pairs (P, H) where $P \in L_1(V), H \in L_{n-1}(V)$, and $P \subset H$. This will imply that all the subgroups $\chi(P, H)$ are conjugate. We will then prove that, apart from the exceptions, the commutator subgroup contains one of the subgroups $\chi(P, H)$ and hence all of them. It will then follow that the commutator subgroup of $SL(V), SL(V)'$ is equal to $SL(V)$.

Lemma 11.7 *Let $P_i, i = 1, 2$ be one-dimensional subspaces, $H_i, i = 1, 2$ be hyperplanes, and assume $P_i \subset H_i$. Then there exists $S \in SL(V)$ such that $S(P_1) = P_2, S(H_1) = H_2$.*

Proof *Let $(\boldsymbol{x}_{1i}, \dots, \boldsymbol{x}_{n-1,i})$ be a basis for $H_i, i = 1, 2$ with $\boldsymbol{x}_{1i} \in P_i, i = 1, 2$. Let $\boldsymbol{x}_{ni} \in V \setminus H_i, i = 1, 2$. Then $(\boldsymbol{x}_{1i}, \dots, \boldsymbol{x}_{ni})$ is a basis for V for $i = 1, 2$. Let T be the operator such that $T(\boldsymbol{x}_{j1}) = \boldsymbol{x}_{j2}$. Then $T(P_1) = P_2, T(H_1) = H_2$. We are done if $det(T) = 1$. Suppose $det(T) = a \neq 1$. Define $S \in \mathcal{L}(V, V)$ such that S restricted to $H_1$is equal to T restricted to H_1 and such that $S(\boldsymbol{x}_{n1}) = \frac{1}{a}\boldsymbol{x}_{n2}$. Then $S(P_1) = P_2, S(H_1) = H_2$ and $det(S) = 1$.*

Corollary 11.2 *Let $P_i, i = 1, 2$ be one-dimensional subspaces, $H_i, i = 1, 2$ be hyperplanes, and assume $P_i \subset H_i$. Then there exists $S \in SL(V)$ such that $S\chi(P_1, H_1)S^{-1} = \chi(P_2, H_2)$.*

Proof *This follows from the fact that $S\chi(P, H)S^{-1} = \chi(S(P), S(H))$, which we leave as an exercise.*

Theorem 11.2 *Assume $(n, \mathbb{F}) \neq (2, \mathbb{F}_2), (2, \mathbb{F}_3)$. Then $SL(V)$ is perfect.*

Proof *First assume that $n \geq 3$. Let $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ be a basis of V. Let $a \in \mathbb{F}$ and let S_a be the operator defined on V such that $S_a(\boldsymbol{v}_i) = \boldsymbol{v}_i$ if $i \neq n$ and $S_a(\boldsymbol{v}_n) = a\boldsymbol{v}_{n-1} + \boldsymbol{v}_n$. This is a transvection with center Span$(\boldsymbol{v}_{n-1})$ and axis Span$(\boldsymbol{v}_1, \dots, \boldsymbol{v}_{n-1})$. Next let $b \in \mathbb{F}$ and T_b be the operator on V defined by $T_b(\boldsymbol{v}_i) = \boldsymbol{v}_i$ for $i \neq n-1$ and $T_b(\boldsymbol{v}_{n-1}) = b\boldsymbol{v}_1 + \boldsymbol{v}_{n-1}$. Then T_b is a transvection with center Span$(\boldsymbol{v}_1)$ and axis Span$(\boldsymbol{v}_1, \dots, \boldsymbol{v}_{n-2}, \boldsymbol{v}_n)$. Set $R = T_b^{-1} S_a^{-1} T_b S_a$. Then R is the transvection such that $R(\boldsymbol{v}_i) = \boldsymbol{v}_i$ for $i \neq n$ and $R(\boldsymbol{v}_n) = ab\boldsymbol{v}_1 + \boldsymbol{v}_n$. Thus, if $P =$ Span$(\boldsymbol{v}_1)$ and $H =$ Span$(\boldsymbol{v}_1, \dots, \boldsymbol{v}_{n-1})$ then $\chi(P, H)$ is contained in $SL(V)'$. Since $SL(V)'$ is normal in $SL(V)$ every conjugate, $S\chi(P, H)S^{-1}$ is contained in $SL(V)'$. By Corollary (11.2), $SL(V)'$ contains every transvection subgroup $\chi(P', H')$. Now by Theorem (11.1) it follows that $SL(V)' = SL(V)$.*

We may therefore assume that $n = 2$ and that $\mathbb{F}$ has at least four elements. Choose a basis $(\boldsymbol{v}_1, \boldsymbol{v}_2)$ for V and let $b \in \mathbb{F}, a \neq 0,$. Denote by T_b the transvection such that $T_b(\boldsymbol{v}_1) = \boldsymbol{v}_1$ and $T_b(\boldsymbol{v}_2) = b\boldsymbol{v}_1 + \boldsymbol{v}_2$. Next let $c \in \mathbb{F}, c \neq 0, \pm 1$ and denote by S_c the operator such that $S_c(\boldsymbol{v}_1) = c\boldsymbol{v}_1, S_c(\boldsymbol{v}_2) = \frac{1}{c}\boldsymbol{v}_2$. Note that $1 - c^2 \neq 0$. Set $R_{b,c} = S_c^{-1} T_b^{-1} S_c T_b$. Then $R_{b,c}(\boldsymbol{v}_1) = \boldsymbol{v}_1$ and $R_{b,c}(\boldsymbol{v}_2) = b(1-c^2)\boldsymbol{v}_1 + \boldsymbol{v}_2$. Thus, $R_{b,c}$ is a transvection with center and axis equal to Span$(\boldsymbol{v}_1)$. Note that as b ranges over $\mathbb{F}$ so does $b(1-c^2)$. Consequently, every transvection with axis Span$(\boldsymbol{v}_1)$ is contained in $SL(V)'$. Since $SL(V)'$ is normal in $SL(V)$ and transitive on one-dimensional subspaces it follows that $SL(V)'$ contains all transvections. Again by Theorem (11.1), it follows that $SL(V)' = SL(V)$.

Definition 11.3 *The* **projective general linear group** *is the quotient group $GL(V)/Z(GL(V))$ and is denoted by $PGL(V)$. The* **special linear group***, denoted by $PSL(V)$, is the quotient group $SL(V)/Z(SL(V))$.*

Remark 11.3 *Let $\overline{T} = Z(GL(V))T$ be an element of $PGL(V)$ and let U be a k-dimensional subspace of V. Define $\overline{T} \cdot U = T \cdot U = T(U)$. This is well defined and gives a* **faithful** *action of $PGL(V)$ on $L_k(V)$ (prove this).*

Lemma 11.8 *Let $P \in L_1(V), H_1, H_2 \in L_{n-1}(V)$ with $P \subset H_1 \cap H_2$. Then $\chi(P, H_1)$ and $\chi(P, H_2)$ commute.*

This is left as an exercise.

Definition 11.4 *Fix $P \in L_1(V)$. We denote the subgroup of $SL(V)$ generated by all $\chi(P, H)$ where $H \in L_{n-1}(V), P \subset H$ by $\chi(P)$ and refer to this as the* **group of transvections with center** *P.*

Corollary 11.3 *Let $P \in L_1(V)$. Then $\chi(P)$ is an Abelian group.*

Proof *This is immediate from Lemma (11.8).*

Let $P \in L_1(V)$. We denote by $SL(V)_P$ the set of all $T \in SL(V)$ such that $T(P) = P$.

Lemma 11.9 *Let $P \in L_1(V)$. Then $\chi(P)$ is a normal subgroup of $SL(V)_P$.*

Proof *Assume $S \in \chi(P, H)_P$ and $T \in SL(V)$. Set $H' = T(H)$. Then $H' \in L_{n-1}(V)$ and $P \subset H'$. It then follows that $STS^{-1} \in \chi(S(P), S(H)) = \chi(P, H')$, a subgroup of $\chi(P)$.*

Theorem 11.3 *Assume $(n, \mathbb{F})$ neither $(2, \mathbb{F}_2)$ nor $(2, \mathbb{F}_3)$ and that N is a normal subgroup of $SL(V)$ not contained in $Z(SL(V))$. Then $N = SL(V)$. In particular, $PSL(V)$ is a simple group.*

Proof *$SL(V)$ acts primitively on $L_1(V)$. For $P \in L_1(V), \chi(P)$ is an Abelian normal subgroup of $SL(V)_P$ and its conjugates generate $SL(V)$. Since $SL(V)$ is perfect, the conclusion follows from Iwasawa's theorem.*

Remark 11.4 *The groups $PSL_2(\mathbb{F}_2)$ and $PSL_2(\mathbb{F}_3)$ are truly exceptions: The order of $PSL_2(\mathbb{F}_2)$ is six and the group is isomorphic to the symmetric group of degree three, and is solvable. The group $PSL_2(\mathbb{F}_3)$ has order 12, is isomorphic to the alternating group of degree four, and is solvable.*

Exercises

1. Let V be an n-dimensional vector space over $\mathbb{F}_q$ where $q = p^k$ for a prime p. Determine the order of $GL(V)$ and $SL(V)$.

2. Assume that V is an n-dimensional vector space over a field $\mathbb{F}$ and k is a natural number, $2 \leq k \leq \frac{n}{2}$. Assume $U_1, U_2, W_1, W_2 \in L_k(V)$ and $dim(U_1 \cap U_2) = dim(W_1 \cap W_2)$. Prove that there exists $S \in SL(V)$ such that $S(U_i) = W_i, i = 1, 2$.

3. Let V be an n-dimensional vector space and k a natural number, $1 < k < n$. Assume $T \in GL(V)$ and $T(U) = U$ for every $U \in L_k(V)$. Prove $T \in Z(GL(V))$.

4. Assume $dim(V) = n, P \in L_1(V), H_1 \neq H_2 \in L_{n-1}(V)$ with $P \subset H_1 \cap H_2$. Prove that $\chi(P, H_1)$ and $\chi(P, H_2)$ commute.

5. Continue with the assumptions of Exercise 4. Set $U = H_1 \cap H_2$. Assume $S \in \chi(P, H_1)\chi(P, H_2)$. Prove that there is an element $H \in L_{n-1}(V)$ containing U such that $T \in \chi(P, H)$.

6. Assume $dim(V) = n, P_1, P_2 \in L_1(V), H \in L_{n-1}(V)$ and $P_1 + P_2 \subset H$. Prove that $\chi(P_1, H)$ and $\chi(P_2, H)$ commute.

7. Continue with the assumptions of Exercise 6. Let $T \in \chi(P_1, H)\chi(P_2, H)$. Prove there is a $P \in L_1(P_1 + P_2)$ such that $T \in \chi(P, H)$.

8. Assume P_1 is not contained in H_2 and P_2 is not contained in H_1. Prove that $\langle \chi(P_1, H_1), \chi(P_2, H_2) \rangle$ is isomorphic to $SL(W)$ where $dim(W) = 2$.

9. Assume $dim(V) = n, P_1 \neq P_2 \in L_1(V), H_1 \neq H_2 \in L_{n-1}(V)$ with $P_i \subset H_i, i = 1, 2$. Prove that $\chi(P_1, H_1)$ commutes with $\chi(P_2, H_2)$ if and only if $P_1 + P_2 \subset H_1 \cap H_2$.

10. Assume $dim(V) = n, P \in L_1(V), H \in L_{n-1}(V)$ with $P \subset H$. Let $S \in SL(V)$. Prove that $S\chi(P, H)S^{-1} = \chi(S(P), S(H))$.

11.2 Symplectic Groups

In this section we consider the symplectic group, $Sp(V)$, of isometries of a non-degenerate $2m$-dimensional symplectic space (V, f). We show the existence of transvections in $SP(V)$. We also prove, with just three exceptions, that the quotient of the group $Sp(V)$ by its center is a simple group.

What You Need to Know

To successfully navigate the material of this new section you should by now have mastered the following concepts: vector space over a field $\mathbb{F}$, basis of a vector space, dimension of a vector space, linear operator on a vector space V, matrix of a linear operator $T : V \to V$ with respect to a base $\mathcal{B}$ for V, eigenvalue and eigenvector of an operator T, the algebra $\mathcal{L}(V, V)$ of operators on a finite-dimensional vector space V, an invertible operator on a vector space V, the group $GL(V)$ of invertible operators on a finite-dimensional vector space V, bilinear form, reflexive bilinear form, alternating bilinear form, symplectic space, non-degenerate symplectic space, hyperbolic pair in a symplectic space, a hyperbolic basis in a symplectic space, an isometry of a symplectic space. You must also be familiar with the following concepts from group theory: Abelian group, solvable group, normal subgroup of a group, quotient group of a group by a normal subgroup, the commutator of two elements in a group, the commutator subgroup of a group, a perfect group, the center of a group, a simple group, action of a group G on a set X, transitive action of a group G on a set X, primitive action of a group G on a set X, and faithful action of a group G on a set X. The material on groups can be found in Appendix B.

We recall some definitions:

Let V be a vector space over a field $\mathbb{F}$. An alternating bilinear form is a map $f : V \times V \to \mathbb{F}$ such that

1) for every vector $\boldsymbol{v}$, the map $f_{\boldsymbol{v}} : V \to \mathbb{F}$ defined by $f_{\boldsymbol{v}}(\boldsymbol{u}) = f(\boldsymbol{u}, \boldsymbol{v})$ is linear;

2) for every vector $\boldsymbol{v}$, the map ${}_{\boldsymbol{v}}f : V \to \mathbb{F}$ defined by ${}_{\boldsymbol{v}}f(\boldsymbol{u}) = f(\boldsymbol{v}, \boldsymbol{u})$ is linear; and

3) for every vector $\boldsymbol{v}, f(\boldsymbol{v}, \boldsymbol{v}) = 0$.

It follows from 1)–3) that for any vectors $\boldsymbol{v}$ and $\boldsymbol{u}$, $f(\boldsymbol{u}, \boldsymbol{v}) = -f(\boldsymbol{v}, \boldsymbol{u})$.

A symplectic space is a pair (V, f) of a vector space V and an alternating bilinear form $f : V \times V \to \mathbb{F}$.

The radical of (V, f) consists of all those vectors $\boldsymbol{v}$ such that $f_{\boldsymbol{v}} = \mathbf{0}_{V \to \mathbb{F}}$. (V, f) is non-degenerate if $Rad(f) = \{\mathbf{0}\}$. If (V, f) is a non-degenerate symplectic space then Theorem (8.7) implies that the dimension of V is even and the existence of a basis $\mathcal{B} = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ for V such that $f(\boldsymbol{u}_i, \boldsymbol{u}_j) = f(\boldsymbol{v}_i, \boldsymbol{v}_j) = f(\boldsymbol{u}_i, \boldsymbol{v}_j) = 0$ if $i \neq j$ and $f(\boldsymbol{u}_j, \boldsymbol{v}_j) = 1$. Such a basis is called a hyperbolic basis.

An isometry of a symplectic space (V, f) is a linear operator $T : V \to V$ such that $f(T(\boldsymbol{u}), T(\boldsymbol{v})) = f(\boldsymbol{u}, \boldsymbol{v})$ for all vectors $\boldsymbol{u}, \boldsymbol{v}$. If (V, f) is non-degenerate then an isometry must be invertible since a vector $\boldsymbol{v} \in Ker(T)$ must lie in the radical and, consequently, $Ker(T) = \{\boldsymbol{0}_V\}$. When (V, f) is non-degenerate the composition of isometries is an isometry and the inverse of an isometry is an isometry. Therefore the collection of isometries is a subgroup of $GL(V)$.

Definition 11.5 *Let (V, f) be a non-degenerate symplectic space. The collection of isometries of (V, f) is referred to as the* **symplectic group** *on V and is denoted by $Sp(V)$.*

Recall for a bilinear form f on a vector space V with a basis $\mathcal{B} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$, the matrix of f with respect to $\mathcal{B}, \mathcal{M}_f(\mathcal{B}, \mathcal{B})$, is the matrix A whose (i, j)-entry is $a_{ij} = f(\boldsymbol{v}_i, \boldsymbol{v}_j)$. For vectors $\boldsymbol{u}, \boldsymbol{v} \in V$

$$f(\boldsymbol{u}, \boldsymbol{v}) = [\boldsymbol{u}]_{\mathcal{B}}^{tr} A [\boldsymbol{v}]_{\mathcal{B}}.$$

Lemma 11.10 *Let (V, f) be a non-degenerate symplectic space with hyperbolic basis $\mathcal{B} = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{v}_1, \dots, \boldsymbol{v}_n) = (\boldsymbol{z}_1, \dots, \boldsymbol{z}_{2n})$. Set $A = \mathcal{M}_f(\mathcal{B}, \mathcal{B}) = \begin{pmatrix} 0_n & I_n \\ -I_n & 0_n \end{pmatrix}$. Let $\sigma \in GL(V)$ and set $Q = \mathcal{M}_\sigma(\mathcal{B}, \mathcal{B})$. Then the operator $\sigma \in Sp(V)$ if and only if $Q^{tr} A Q = A$.*

Proof *Let the entries of $Q^{tr} A Q$ be b_{ij}. Then $\sigma \in Sp(V)$ if and only if $f(\boldsymbol{u}, \boldsymbol{v}) = f(\sigma(\boldsymbol{u}), \sigma(\boldsymbol{v}))$ for every pair of vectors $(\boldsymbol{u}, \boldsymbol{v})$ from $\mathcal{B}$. It then follows that*

$$(Q[\boldsymbol{u}]_{\mathcal{B}})^{tr} A (Q[\boldsymbol{v}]_{\mathcal{B}}) = [\boldsymbol{u}]_{\mathcal{B}}^{tr} Q^{tr} A Q [\boldsymbol{v}]_{\mathcal{B}} = [\boldsymbol{u}]_{\mathcal{B}}^{tr} A [\boldsymbol{v}]_{\mathcal{B}}.$$

Taking $(\boldsymbol{u}, \boldsymbol{v}) = (\boldsymbol{z}_i, \boldsymbol{z}_j)$ we get that $b_{ij} = a_{ij}$ for $1 \leq i, j \leq 2n$ and so $Q^{tr} A Q = A$. Conversely, if $Q^{tr} A Q = A$ then

$$\begin{aligned} f(\sigma(\boldsymbol{u}), \sigma(\boldsymbol{v})) &= (Q[\boldsymbol{u}]_{\mathcal{B}})^{tr} A (Q[\boldsymbol{v}]_{\mathcal{B}}) \\ &= [\boldsymbol{u}]_{\mathcal{B}}^{tr} Q^{tr} A Q [\boldsymbol{v}]_{\mathcal{B}} \\ &= [\boldsymbol{u}]_{\mathcal{B}}^{tr} A [\boldsymbol{v}]_{\mathcal{B}} \\ &= f(\boldsymbol{u}, \boldsymbol{v}). \end{aligned}$$

Definition 11.6 *Let (V, f) be a non-degenerate symplectic space with hyperbolic basis $\mathcal{B} = (\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) = (\boldsymbol{z}_1, \ldots, \boldsymbol{z}_{2n})$. Set $A = \mathcal{M}_f(\mathcal{B}, \mathcal{B})$. The collection of matrices such that $Q^{tr}AQ = A$ is denoted by $Sp_{2n}(\mathbb{F})$ and referred to the* **symplectic group of degree 2n** *over $\mathbb{F}$.*

Theorem 11.4 *Let (V, f) be a non-degenerate symplectic space of dimension two. Then $Sp(V)$ is isomorphic to $SL(V)$.*

Proof *Let $\mathcal{B} = (\boldsymbol{u}, \boldsymbol{v})$ be a hyperbolic basis for V and assume $\sigma \in GL(V)$. Set $\mathcal{M}_\sigma(\mathcal{B}, \mathcal{B}) = \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix}$. Then by Lemma (11.10) $\sigma \in Sp(V)$ if and only if*

$$\begin{pmatrix} s_{11} & s_{21} \\ s_{12} & s_{22} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix} = \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix}.$$

This implies that

$$\begin{pmatrix} 0 & s_{11}s_{22} - s_{12}s_{21} \\ s_{12}s_{21} - s_{11}s_{22} & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Thus, $\sigma \in Sp(V)$ if and only if $s_{11}s_{22} - s_{12}s_{21} = 1$.

Let $\boldsymbol{x}$ be a non-zero vector in the non-degenerate symplectic space (V, f) and let $c \in \mathbb{F}$. Set $X = Span(\boldsymbol{x})$. Define a map $T_{\boldsymbol{x},c}$ on V as follows: for a vector $\boldsymbol{u} \in V, T_{\boldsymbol{x},c}(\boldsymbol{u}) = \boldsymbol{u} - cf(\boldsymbol{u}, \boldsymbol{x})\boldsymbol{x}$.

Lemma 11.11 *Let $\boldsymbol{x}$ be a non-zero vector in the non-degenerate symplectic space (V, f) and let $c \in \mathbb{F}$. Then the following hold:*

i) $T_{\boldsymbol{x},c}$ is a transvection with center $X = Span(\boldsymbol{x})$ and axis $\boldsymbol{x}^\perp$.

ii) $T_{\boldsymbol{x},c}$ is an isometry of f.

Proof *i. We leave this as an exercise.*

ii) This is Exercise 7 of Section (8.2).

Definition 11.7 *The map $T_{\boldsymbol{x},c}$ is referred to as a* **symplectic transvection centered at** *X. We denote by $\chi(X)$ the set of all $T_{\boldsymbol{x},c}$ with $c \in \mathbb{F}$ along with I_V. When $X = Span(\boldsymbol{x})$ we will often write $\chi(\boldsymbol{x})$ for $\chi(X)$.*

Lemma 11.12 *Assume (V, f) is a non-degenerate symplectic space. Then the following hold:*

i) If $\boldsymbol{x} \neq \mathbf{0}, c, d \in \mathbb{F}$ then $T_{\boldsymbol{x},c}T_{\boldsymbol{x},d} = T_{\boldsymbol{x},c+d}$.

ii) If $\boldsymbol{x} \neq \mathbf{0}, b, c \in \mathbb{F}$ then $T_{b\boldsymbol{x},c} = T_{\boldsymbol{x},b^2c}$.

iii) If $\boldsymbol{x}, \boldsymbol{y}$ are non-zero vectors, $c, d \in \mathbb{F}$ and $f(\boldsymbol{x}, \boldsymbol{y}) = 0$ then $T_{\boldsymbol{x},c}$ and $T_{\boldsymbol{y},d}$ commute.

iv) If $\boldsymbol{x}, \boldsymbol{y}$ are non-orthogonal vectors, then the group generated by $\chi(Span(\boldsymbol{x}))$ and $\chi(Span(\boldsymbol{y}))$ is isomorphic to $SL_2(\mathbb{F})$.

Proof *We leave i)–iii) as exercises and prove iv). Set $X = Span(\boldsymbol{x}), Y = Span(\boldsymbol{y})$. Since $Y = Span(c\boldsymbol{y})$ for any non-zero c, we may assume that $f(\boldsymbol{x}, \boldsymbol{y}) = 1$. Set $U = Span(\boldsymbol{x}, \boldsymbol{y})$, a non-degenerate subspace of V and set $W = U^{\perp}$. Let Σ be the group generated by $\chi(X)$ and $\chi(Y)$. Both U and W are Σ-invariant and Σ restricted to W is $\{I_Y\}$. Consequently, the map $T \to T_{|X}$ is an injection since the only transformation which fixes every vector in V is I_V. Therefore, we may assume that $V = U$. Set $\mathcal{B} = (\boldsymbol{x}, \boldsymbol{y})$. The matrix of $T_{\boldsymbol{x},c}$ with respect to $\mathcal{B}$ is $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$ and the matrix of $T_{\boldsymbol{y},c}$ is $\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$. We proved in Theorem (11.1) that these matrices generate $SL_2(\mathbb{F})$.*

Lemma 11.13 *Let $X = Span(\boldsymbol{x})$ for a non-zero vector $\boldsymbol{x}$ and $S \in Sp(V)$. Then $S\chi(X)S^{-1} = \chi(S(X))$.*

We leave this as an exercise.

Definition 11.8 *Let $X = Span(\boldsymbol{x})$ be a one-dimensional subspace of V. Let $\Psi(X)$ consist of all those operators T in $Sp(V)$ such that*

1. $T(\boldsymbol{x}) = \boldsymbol{x}$;

2. $T(\boldsymbol{u}) - \boldsymbol{u} \in X$ for $\boldsymbol{u} \in \boldsymbol{x}^{\perp}$; and

3. $T(\boldsymbol{w}) - \boldsymbol{w} \in \boldsymbol{x}^{\perp}$ for $\boldsymbol{w} \in V \setminus \boldsymbol{x}^{\perp}$.

In the next lemma we give criteria for a transformation to belong to $\Psi(X)$.

Lemma 11.14 *Let $(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n, \boldsymbol{y}_1, \dots, \boldsymbol{y}_n)$ be a hyperbolic basis of V such that $\boldsymbol{x}_1 = \boldsymbol{x}$ and set $X = Span(\boldsymbol{x})$. Assume the operator T satisfies the following:*

1. $T(\boldsymbol{x}_1) = \boldsymbol{x}_1$;

2. $T(\boldsymbol{y}_1) = \boldsymbol{y}_1 + \sum_{k=2}^{n}(a_k\boldsymbol{x}_k + b_k\boldsymbol{y}_k) + \gamma\boldsymbol{x}_1$;

3. $T(\boldsymbol{x}_j) = \boldsymbol{x}_j + c_j\boldsymbol{x}_1$ *for* $j \geq 2$*; and*

4. $T(\boldsymbol{y}_j) = \boldsymbol{y}_j + d_j\boldsymbol{x}_1$ *for* $j \geq 2$.

Then $T \in Sp(V)$ *if and only if* $c_j = -b_j$ *and* $d_j = a_j$ *for* $j \geq 2$.

Proof *Assume* T *satisfies 1)–4) and* $T \in Sp(V)$ *and* $j \geq 2$. *Then* $f(T(\boldsymbol{x}_j), T(\boldsymbol{y}_1)) = f(\boldsymbol{x}_j, \boldsymbol{y}_1) = 0$. *However,*

$$\begin{aligned} f(T(\boldsymbol{x}_j), T(\boldsymbol{y}_1)) &= f(\boldsymbol{x}_j + c_j\boldsymbol{x}_1, \boldsymbol{y}_1 + \sum_{k=2}^{n}(a_k\boldsymbol{x}_k + b_k\boldsymbol{y}_k)) \\ &= b_j + c_j. \end{aligned}$$

Thus, $b_j + c_j = 0$ *and* $c_j = -b_j$ *for* $j \geq 2$.

It is also the case that $f(T(\boldsymbol{y}_j), T(\boldsymbol{y}_1)) = f(\boldsymbol{y}_j, \boldsymbol{y}_1) = 0$. *However,*

$$\begin{aligned} f(T(\boldsymbol{y}_j), T(\boldsymbol{y}_1)) &= f(\boldsymbol{y}_j + d_j\boldsymbol{x}_1, \boldsymbol{y}_1 + \sum_{k=2}(a_j\boldsymbol{x}_k + b_j\boldsymbol{y}_k)) \\ &= -a_j + d_j, \end{aligned}$$

and therefore $d_j = a_j$.

Conversely, assume that $c_j = -b_j$ *and* $d_j = a_j$. *By Theorem (8.8) we need to prove that* $(T(\boldsymbol{x}_1), \ldots, T(\boldsymbol{x}_n), T(\boldsymbol{y}_1), \ldots, T(\boldsymbol{y}_n))$ *is a hyperbolic basis, and for this we need to show that* $f(T(\boldsymbol{x}_i), T(\boldsymbol{x}_j)) = f(T(\boldsymbol{y}_i), T(\boldsymbol{y}_j)) = f(T(\boldsymbol{x}_i), T(\boldsymbol{y}_j)) = 0$ *for* $i \neq j$ *and* $f(T(\boldsymbol{x}_i), T(\boldsymbol{y}_i)) = 1$. *The only non-trivial cases are* $f(T(\boldsymbol{x}_i), T(\boldsymbol{y}_1)) = f(T(\boldsymbol{y}_j), T(\boldsymbol{y}_1)) = 0$ *and these follow from the conditions* $c_j = -b_j$ *and* $d_j = a_j$.

Lemma 11.15 *Let* $X = Span(\boldsymbol{x}) \in L_1(V)$. *Then the following hold:*

i) If $S \in Sp(V)$ *then* $S\Psi(X)S^{-1} = \Psi(S(X))$.

ii) The subgroup $\Psi(X)$ *is normal in* $Sp(V)_X = \{T \in Sp(V) | \ T(X) = X\}$.

iii) $\Psi(X)$ *is solvable.*

We leave these as exercises.

It is our goal to prove that $Sp(V)$ is generated by its transvections. Toward that goal, we let $\Omega(V)$ be the subgroup of $Sp(V)$ generated by all $\chi(P), P \in L_1(V)$. We prove in a series of lemmas that $\Omega(V) = Sp(V)$. Our first lemma is a kind of extension result.

Lemma 11.16 *Assume W is a non-degenerate subspace of V, $X \in L_1(W)$ and σ is an isometry of W which is a transvection with center X. Define S on V as follows: if $\boldsymbol{v} \in V$ write $\boldsymbol{v} = \boldsymbol{w} + \boldsymbol{u}$ with $\boldsymbol{w} \in W, \boldsymbol{u} \in W^{\perp}$. Then $S(\boldsymbol{v}) = \sigma(\boldsymbol{w}) + \boldsymbol{u}$. Then S is a transvection on V with center X.*

Proof *We know from Exercise 7 of Section (8.15) that S is an isometry of V. Clearly S restricted to $X^{\perp} = W^{\perp} \oplus (W \cap X^{\perp})$ is the identity and Range$(S - I_V) =$ Range$(\sigma - I_W) = X$, it follows that S is a transvection.*

The following is an immediate consequence of Lemma (11.16):

Corollary 11.4 *Let (V, f) be a non-degenerate symplectic space and W a non-degenerate subspace of V. Assume $S \in Sp(V), S_{|W} \in \Omega(W)$ and $S_{|W^{\perp}} = I_{W^{\perp}}$. Then $S \in \Omega(V)$.*

Lemma 11.17 *Let (V, f) be a non-degenerate symplectic space and $\boldsymbol{u}, \boldsymbol{v}$ non-zero vectors. Then there exists $\sigma \in \Omega(V)$ such that $\sigma(\boldsymbol{u}) = \boldsymbol{v}$.*

Proof *Assume first that $f(\boldsymbol{u}, \boldsymbol{v}) \neq 0$. Then $W =$ Span$(\boldsymbol{u}, \boldsymbol{w})$ is non-degenerate. Let γ be defined by $\gamma(\boldsymbol{u}) = \boldsymbol{u} + \boldsymbol{v}, \gamma(\boldsymbol{v}) = \boldsymbol{v}$ and $\gamma(\boldsymbol{x}) = \boldsymbol{x}$ for $\boldsymbol{x} \in W^{\perp}$. Then γ is a transvection. Let δ be defined by $\delta(\boldsymbol{u}) = \boldsymbol{u}, \delta(\boldsymbol{v}) = -\boldsymbol{u} + \boldsymbol{v}$, and $\delta(\boldsymbol{x}) = \boldsymbol{x}$ for $\boldsymbol{x} \in W^{\perp}$. Then δ is also a transvection. Set $\sigma = \delta\gamma$. Then $\sigma(\boldsymbol{u}) = \delta\gamma(\boldsymbol{u}) = \delta(\boldsymbol{u} + \boldsymbol{v}) = \delta(\boldsymbol{u}) + \delta(\boldsymbol{v}) = \boldsymbol{u} + (-\boldsymbol{u} + \boldsymbol{v}) = \boldsymbol{v}$.*

Assume now that $f(\boldsymbol{u}, \boldsymbol{v}) = 0$. Then there exists $\boldsymbol{w}$ such that $f(\boldsymbol{u}, \boldsymbol{w}) \neq 0 \neq f(\boldsymbol{w}, \boldsymbol{v})$. By the first part of the proof there exist elements $\sigma_1, \sigma_2 \in \Omega(V)$ such that $\sigma_1(\boldsymbol{u}) = \boldsymbol{w}, \sigma_2(\boldsymbol{w}) = \boldsymbol{v}$. Set $\sigma = \sigma_2\sigma_1$.

We next prove that $\Omega(V)$ is transitive on hyperbolic pairs.

Lemma 11.18 *Assume $(\boldsymbol{x}_i, \boldsymbol{y}_i)$ are hyperbolic pairs for $i = 1, 2$. Then there exists $\sigma \in \Omega(V)$ such that $\sigma(\boldsymbol{x}_1) = \boldsymbol{x}_2, \sigma(\boldsymbol{y}_1) = \boldsymbol{y}_2$.*

Proof *We first treat the case where $\boldsymbol{x}_1 = \boldsymbol{x}_2 = \boldsymbol{x}$. Suppose $f(\boldsymbol{y}_1, \boldsymbol{y}_2) = a \neq 0$. Set $\boldsymbol{z} = \boldsymbol{y}_2 - \boldsymbol{y}_1$. Note that $f(\boldsymbol{x}, \boldsymbol{z}) = f(\boldsymbol{x}, \boldsymbol{y}_2 - \boldsymbol{y}_1) = f(\boldsymbol{x}, \boldsymbol{y}_2) - f(\boldsymbol{x}, \boldsymbol{y}_1) = 0$. Set $\sigma = T_{\boldsymbol{z}, \frac{1}{a}}$. Note that $\sigma(\boldsymbol{x}) = \boldsymbol{x}$ since $\boldsymbol{x} \perp \boldsymbol{z}$. Moreover, $\sigma(\boldsymbol{y}_1) = \boldsymbol{y}_1 + \frac{1}{a} f(\boldsymbol{y}_1, \boldsymbol{z})\boldsymbol{z} = \boldsymbol{y}_1 + \frac{1}{a} f(\boldsymbol{y}_1, \boldsymbol{y}_2 - \boldsymbol{y}_1)(\boldsymbol{y}_2 - \boldsymbol{y}_1) = \boldsymbol{y}_1 + (\boldsymbol{y}_2 - \boldsymbol{y}_1) = \boldsymbol{y}_2$.*

Now assume that $f(\boldsymbol{y}_1, \boldsymbol{y}_2) = 0$. Note that $(\boldsymbol{x}, \boldsymbol{y}_1)$ and $(\boldsymbol{x}, \boldsymbol{y}_1 + \boldsymbol{x})$ are hyperbolic pairs and $f(\boldsymbol{y}_1, \boldsymbol{y}_1 + \boldsymbol{x}) = -1 \neq 0$ so by what we have shown there is a transvection σ_1 such that $\sigma_1(\boldsymbol{x}) = \boldsymbol{x}$ and $\sigma_1(\boldsymbol{y}_1) = \boldsymbol{y}_1 + \boldsymbol{x}$. Next note that

$f(\boldsymbol{y}_1+\boldsymbol{x},\boldsymbol{y}_2)=f(\boldsymbol{x},\boldsymbol{y}_2)=1\neq 0$. Consequently, there is a transvection σ_2 such that $\sigma_2(\boldsymbol{x})=\boldsymbol{x}$ and $\sigma_2(\boldsymbol{y}_1+\boldsymbol{x})=\boldsymbol{y}_2$. Set $\sigma=\sigma_2\sigma_1$.

Finally, assume $\boldsymbol{x}_1\neq\boldsymbol{x}_2$. By Lemma (11.17) there is an element $\tau\in\Omega(V)$ such that $\tau(\boldsymbol{x}_1)=\boldsymbol{x}_2$. Set $\boldsymbol{y}_2'=\tau(\boldsymbol{y}_1)$. By the first case there exists $\gamma\in\Omega(V)$ such that $\gamma(\boldsymbol{x}_2)=\boldsymbol{x}_2$ and $\gamma(\boldsymbol{y}_2')=\boldsymbol{y}_2$. Set $\sigma=\gamma\tau$.

We are now able to prove:

Theorem 11.5 *Assume (V,f) is a non-degenerate symplectic space. Then $Sp(V)$ is generated by transvections.*

Proof *The proof is by induction on n where $dim(V)=2n$. When $n=1$ we have already shown that $Sp(V)=SL(V)$ and $SL(V)$ is generated by transvections. So assume the result has been proved for spaces of dimension $2n$ and that $dim(V)=2n+2$. Let $T\in Sp(V)$ and let $(\boldsymbol{x}_1,\boldsymbol{y}_1)$ be a hyperbolic pair and set $T(\boldsymbol{x}_1)=\boldsymbol{x}_2, T(\boldsymbol{y}_1)=\boldsymbol{y}_2$. Then $(\boldsymbol{x}_2,\boldsymbol{y}_2)$ is a hyperbolic pair. By Lemma (11.18) there is a $\sigma\in\Omega(V)$ such $\sigma(\boldsymbol{x}_1)=\boldsymbol{x}_2,\sigma(\boldsymbol{y}_1)=\boldsymbol{y}_2$. Set $S=\sigma^{-1}T$. Then $S(\boldsymbol{x}_1)=\boldsymbol{x}_1, S(\boldsymbol{y}_1)=\boldsymbol{y}_1$. Set $W=Span(\boldsymbol{x}_1,\boldsymbol{y}_1)$ and $U=W^{\perp}$. It follows that S restricted to W is the identity, I_W, that U is S-invariant, and S restricted to U is in the isometry group of $(U,f_{|U\times U})$ which is isomorphic to $Sp(U)$. By the induction hypothesis $S_{|U}\in\Omega(U)$ and by Corollary (11.4), $S\in\Omega(V)$. From $\sigma^{-1}T=S\in\Omega(V)$ we obtain $T=\sigma S\in\Omega(V)$.*

It is our next goal to prove that with three exceptions the group $Sp(V)$ is perfect. Since the commutator subgroup of a group is normal, since all the transvection groups $\chi(X)$ are conjugate in $Sp(V)$, and since $Sp(V)$ is generated by transvections, $Sp(V)$ will be perfect precisely when the transvection groups $\chi(X)$ are contained in $Sp(V)'$. We proceed to determine when this is so.

Lemma 11.19 *Assume $|\mathbb{F}|\geq 4$ and (V,f) is a non-degenerate symplectic space. Then $Sp(V)$ is perfect.*

Proof *Let $(\boldsymbol{x},\boldsymbol{y})$ be a hyperbolic pair and set $X=Span(\boldsymbol{x}), W=Span(\boldsymbol{x},\boldsymbol{y})$ and $U=W^{\perp}$. Let $\sigma(\boldsymbol{x})=c\boldsymbol{x},\sigma(\boldsymbol{y})=\frac{1}{c}\boldsymbol{y}$ and $\sigma(\boldsymbol{u})=\boldsymbol{u}$ for $\boldsymbol{u}\in U$. Let $\tau_d(\boldsymbol{x})=\boldsymbol{x},\tau_d(\boldsymbol{y})=d\boldsymbol{x}+\boldsymbol{y}$, and $\tau_d(\boldsymbol{u})=\boldsymbol{u}$ for $\boldsymbol{u}\in U$. Let $\gamma=\tau\sigma\tau^{-1}\sigma^{-1}$. Then $\gamma(\boldsymbol{u})=\boldsymbol{u}$ for $\boldsymbol{u}\in U$. Also, $\gamma(\boldsymbol{x})=\boldsymbol{x}$ and $\gamma(\boldsymbol{y})=d(c^2-1)\boldsymbol{x}+\boldsymbol{y}$. We can choose $c\neq 0$ such that $c^2-1\neq 0$. Then $d(c^2-1)$ ranges over all of $\mathbb{F}$ as d does. Therefore γ ranges over all of $\chi(X)$ and $\chi(Span(\boldsymbol{x}))$ is contained in $Sp(V)'$ and $Sp(V)$ is perfect.*

Lemma 11.20 *Assume $\mathbb{F} = \mathbb{F}_3$ and (V, f) is a non-degenerate symplectic space over $\mathbb{F}$ of dimension $2n$ with $n \geq 2$. Then $Sp(V)$ is perfect.*

Proof *As noted above it suffices to prove that the commutator subgroup of $Sp(V)$ contains a transvection group $\chi(X)$ for some $X \in L_1(V)$. Since $\chi(X)$ is cyclic of order 3, in fact, it suffices to prove that $Sp(V)$ contains at least one transvection. Assume we have proved the result in the case that $dim(V) = 4$. Let W be a non-degenerate subspace of dimension four. Set $S(W) = \{T \in Sp(V)|\ T(W) = W, T_{|W^\perp} = I_{W^\perp}\}$. By Witt's theorem for symplectic spaces, Theorem (8.10), $S(W)$ is isomorphic to $Sp(W)$. By our assumption there exists a $T \in S(W)$ which induces a transvection on W. However, since T restricted to $W^\perp$ is the identity, T is a transvection on V. Consequently, the commutator subgroup of $Sp(V)$ contains a transvection and is perfect. Thus, it remains to show that the commutator subgroup of $Sp(V)$ contains a transvection when $dim(V) = 4$.*

Let $\mathcal{B} = (\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{v}_2, \boldsymbol{v}_1)$ be a basis for V such that

$$f(\boldsymbol{u}_1, \boldsymbol{u}_2) = f(\boldsymbol{u}_1, \boldsymbol{v}_2) = f(\boldsymbol{u}_2, \boldsymbol{v}_1) = f(\boldsymbol{v}_2, \boldsymbol{v}_1) = 0$$

$$f(\boldsymbol{u}_1, \boldsymbol{v}_1) = f(\boldsymbol{u}_2, \boldsymbol{v}_2) = 1.$$

We define operators σ, τ_a, γ_b and δ_c, ϵ_d such that

$$\mathcal{M}_\sigma(\mathcal{B}, \mathcal{B}) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\mathcal{M}_{\tau_a}(\mathcal{B}, \mathcal{B}) = \begin{pmatrix} 1 & a & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -a \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\mathcal{M}_{\gamma_b}(\mathcal{B}, \mathcal{B}) = \begin{pmatrix} 1 & 0 & b & 0 \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\mathcal{M}_{\delta_c}(\mathcal{B}, \mathcal{B}) = \begin{pmatrix} 1 & 0 & 0 & c \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\mathcal{M}_{\epsilon_d}(\mathcal{B},\mathcal{B}) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & d & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Each of these operators is in $Sp(V)$ as can be checked by showing that each takes $\mathcal{B}$ to a hyperbolic basis. Also, δ_c is a transvection.

The commutator $[\sigma^{-1}, \gamma_b^{-1}]$ has matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & b & 0 \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -b & 0 \\ 0 & 1 & 0 & -b \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 0 & b & 0 \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

This proves that γ_b is in $Sp(V)'$.

The commutator $[\tau_a^{-1}, \epsilon_d^{-1}]$ has matrix

$$\begin{pmatrix} 1 & a & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -a \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & d & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & a \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -d & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 0 & ad & a^2d \\ 0 & 1 & 0 & ad \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

It therefore follows that $\gamma_{ad}\delta_{a^2d}$ is an element of $Sp(V)'$. Since γ_{ad} is in $Sp(V)'$ it follows that $\delta_{a^2d} \in Sp(V)'$.

One case remains:

Lemma 11.21 *Assume $\mathbb{F} = \mathbb{F}_2$ and (V, f) is a non-degenerate symplectic space. If $dim(V) = 2n \geq 6$, then $Sp(V)$ is perfect.*

Proof *By arguing as we did in Lemma (11.20), it suffices to prove that* $Sp(V)$ *is perfect when* $dim(V) = 6$. *To prove that* $Sp(V)$ *is perfect when* $dim(V) = 6$ *and* $\mathbb{F} = \mathbb{F}_2$, *it is enough to show that the commutator subgroup* $Sp(V)'$ *contains a transvection.*

We first note that the order of $Sp(V)$ *is equal to the number of hyperbolic bases which can be computed inductively in general for* $Sp_{2n}(\mathbb{F}_q)$. *In the present case,* $|Sp_6(\mathbb{F}_2)| = 2^9(2^6-1)(2^4-1)(2^2-1) = 2^9 \cdot 3^4 \cdot 7$. *It therefore suffices to show that a 2-Sylow subgroup of* $Sp(V)$ *is contained in the commutator subgroup.*

Let $\mathcal{B} = (\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3)$ *be a hyperbolic basis satisfying*

$$f(\boldsymbol{u}_i, \boldsymbol{u}_j) = f(\boldsymbol{v}_i, \boldsymbol{v}_j) = f(\boldsymbol{u}_i, \boldsymbol{v}_j) = 0 \text{ for all } i \neq j \text{ and}$$

$$f(\boldsymbol{u}_1, \boldsymbol{v}_1) = f(\boldsymbol{u}_2, \boldsymbol{v}_2) = f(\boldsymbol{u}_3, \boldsymbol{v}_3) = 1.$$

Then the matrix of f *with respect to* $\mathcal{B}$ *is* $A = \begin{pmatrix} 0_3 & I_3 \\ I_3 & 0_3 \end{pmatrix}$. *We note that if* $T \in \mathcal{L}(V,V)$ *with* $\mathcal{M}_T(\mathcal{B},\mathcal{B}) = Q$, *then* $T \in Sp(V)$ *if and only if* $Q^{tr}AQ = A$.

Set $U = Span(\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3)$, *a maximal totally isotropic subspace of* V. *Let* $S(U)$ *be the subgroup of* $Sp(V)$ *of all operators such that* $T(U) = U$. *This contains the subgroup* $Q(U)$ *consisting of all those operators* T *such that* U *is contained in* $Ker(T - I_V)$ *and* $Range(T - I_V)$ *is contained in* U. *An operator in* $GL(V)$ *satisfying these properties will have matrix*

$$\mathcal{M}_T(\mathcal{B},\mathcal{B}) = \begin{pmatrix} I_3 & M \\ 0_3 & I_3 \end{pmatrix}$$

with M *a* 3×3 *matrix. From our comment above it follows that* T *is in* $Sp(V)$ *and therefore* $Q(U)$ *if and only if* M *is symmetric.*

Operators T *such that* $\mathcal{M}_T(\mathcal{B},\mathcal{B}) = \begin{pmatrix} B & 0_3 \\ 0_3 & C \end{pmatrix}$ *with* B, C *invertible* 3×3 *matrices are in* $GL(V)$ *and satisfy* $T(U) = U$. *However, to be in* $Sp(V)$ *it must be the case that* $C = (B^{tr})^{-1}$. *We denote the collection of such operators by* $L(U)$. *Note that* $L(U)$ *is isomorphic to* $SL_3(\mathbb{F}_2)$, *a simple group, and consequently, perfect. Assume now that* $S \in Q(U), T \in L(U)$ *with*

$$\mathcal{M}_S(\mathcal{B},\mathcal{B}) = \begin{pmatrix} I_3 & M \\ 0_3 & I_3 \end{pmatrix} \text{ and } \mathcal{M}_T(\mathcal{B},\mathcal{B}) = \begin{pmatrix} B & 0_3 \\ 0_3 & (B^{tr})^{-1} \end{pmatrix}.$$

Then the matrix of TST^{-1} *is* $\mathcal{M}_{TST^{-1}}(\mathcal{B},\mathcal{B}) = \begin{pmatrix} I_3 & BMB^{tr} \\ 0_3 & I_3 \end{pmatrix}$. *Thus,* $L(U)$ *normalizes* $Q(U)$ *and* $L(U)Q(U)$ *is a subgroup of* $Sp(V)$. *Moreover, from the above computation it follows that* $Q(U)$ *is contained in* $S(U)'$. *Since* $L(U)$ *is simple,* $L(U)$ *is contained in* $S(U)'$. *However, the order of* $L(U)Q(U)$ *is* $2^9 \cdot 7 \cdot 3$ *and so contains a 2-Sylow of* $Sp(V)$ *and therefore transvections. This completes the proof.*

Let (V, f) be a non-degenerate symplectic space and $X \in L_1(V)$. We will denote by $\Delta(X)$ the set of all $Y \in L_1(V)$ such that $X \perp Y$ and by $\Gamma(X)$ those Y in $L_1(V)$ such that $X \not\perp Y$. In the following results we prove that $Sp(V)_X = \{T \in Sp(V)| \ T(X) = X\}$ is transitive on both $\Delta(X)$ and $\Gamma(X)$.

Theorem 11.6 *Let (V, f) be a non-degenerate symplectic space and $X \in L_1(V)$. Let $Y_1, Y_2 \in \Delta(X)$. Then there exists $T \in Sp(V)$ such that $T(X) = X, T(Y_1) = Y_2$.*

Proof *Assume first that Y_2 is contained in $X + Y_1$. Let $\boldsymbol{x} \in X, \boldsymbol{y}_i \in Y_i$ be non-zero vectors. There are scalars a, b such that $\boldsymbol{y}_2 = a\boldsymbol{x} + b\boldsymbol{y}_1$. Replacing $\boldsymbol{y}_2$ by $\frac{1}{b}\boldsymbol{y}_2$, if necessary, we may assume that $b = 1$. Set $\boldsymbol{u}_1 = \boldsymbol{x}, \boldsymbol{u}_2 = \boldsymbol{y}_1$ and extend to a hyperbolic basis $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ of V. Define $T \in \mathcal{L}(V, V)$ by $T(\boldsymbol{u}_i) = \boldsymbol{u}_i$ for $i \neq 2, T(\boldsymbol{v}_j) = \boldsymbol{v}_j$ for $j \neq 1, T(\boldsymbol{u}_2) = a\boldsymbol{u}_1 + \boldsymbol{u}_2, T(\boldsymbol{v}_1) = -a\boldsymbol{v}_2 + \boldsymbol{v}_1$. By Lemma (11.14) $T \in \Psi(X)$. Moreover, $T(\boldsymbol{y}_1) = T(\boldsymbol{u}_2) = a\boldsymbol{u}_1 + \boldsymbol{u}_2 = a\boldsymbol{x}_1 + \boldsymbol{y}_1 = \boldsymbol{y}_2$. Thus, $T(Y_1) = Y_2$ as required.*

Now assume that $X + Y_1 \neq X + Y_2$. Let $\boldsymbol{w}$ be a vector such that $X \not\perp \boldsymbol{w}$ and set $W = Span(\boldsymbol{x}, \boldsymbol{w})$. Also, set $Y_i' = (X + Y_i) \cap \boldsymbol{w}^{\perp} \in L_1(W^{\perp})$. $Sp(W^{\perp})$ is transitive on $L_1(W^{\perp})$ by Lemma (11.17). Consequently, there exists $\sigma \in Sp(V)$ such that $\sigma_{|W} = I_W$ and $\sigma(Y_1') = Y_2'$. Then $\sigma(X + Y_1) = \sigma(X + Y_1') = \sigma(X) + \sigma(Y_1') = X + Y_2' = X + Y_2$. Now by the first part there exists $\tau \in \Psi(X)$ such that $\tau(Y_2') = Y_2$. Set $T = \tau\sigma$. This is the required operator.

Theorem 11.7 *Let (V, f) be a non-degenerate symplectic space, $\boldsymbol{x}$ a non-zero vector, and $\boldsymbol{y}, \boldsymbol{z}$ vectors satisfying $f(\boldsymbol{x}, \boldsymbol{y}) = f(\boldsymbol{x}, \boldsymbol{z}) = 1$. Then there exists a unique $T \in \Psi(Span(\boldsymbol{x}))$ such that $T(\boldsymbol{y}) = \boldsymbol{z}$.*

Proof *Since $f(\boldsymbol{x}, \boldsymbol{y}) = f(\boldsymbol{x}, \boldsymbol{z}) = 1$ it follows that $\boldsymbol{x} \perp (\boldsymbol{z} - \boldsymbol{y})$ so that $\boldsymbol{z} - \boldsymbol{y} \in \boldsymbol{x}^{\perp}$. Set $\boldsymbol{x}_1 = \boldsymbol{x}$ and extend the hyperbolic pair $(\boldsymbol{x}_1, \boldsymbol{y}_1)$ to a hyperbolic basis, $(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n, \boldsymbol{y}_1, \dots, \boldsymbol{y}_n)$. Then $\boldsymbol{x}^{\perp} = Span(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n, \boldsymbol{y}_2, \dots, \boldsymbol{y}_n)$. Let $\boldsymbol{z} - \boldsymbol{y} = c\boldsymbol{x}_1 + \sum_{j=2}^{n}(a_j\boldsymbol{x}_j + b_j\boldsymbol{y}_j)$. Let T be the operator such that $T(\boldsymbol{x}_1) = \boldsymbol{x}_1, T(\boldsymbol{x}_j) = -b_j\boldsymbol{x}_1 + \boldsymbol{x}_j$ for $j \geq 2, T(\boldsymbol{y}_j) = a_j\boldsymbol{x}_1 + \boldsymbol{y}_j$ for $j \geq 2$, and $T(\boldsymbol{y}_1) = \boldsymbol{z} = c\boldsymbol{x}_1 + \sum_{j=2}^{n}(a_j\boldsymbol{x}_j + b_j\boldsymbol{y}_j) + \boldsymbol{y}_1$. Then $T \in \Psi(Span(\boldsymbol{x}))$ and $T(\boldsymbol{y}) = \boldsymbol{z}$. Moreover, by Lemma (11.14), T is the unique operator in $\Psi(Span(\boldsymbol{x}))$ such that $T(\boldsymbol{y}) = \boldsymbol{z}$.*

As an immediate corollary of Theorem (11.7) we have:

Corollary 11.5 *Let (V, f) be a non-degenerate symplectic space, $X \in L_1(V)$ and $Y_1, Y_2 \in \Gamma(X)$. Then there exists a unique $T \in \Psi(X)$ such that $T(Y_1) = Y_2$.*

We leave this as an exercise.

Theorem 11.8 *Let (V, f) be a non-degenerate symplectic space. The action of $Sp(V)$ on $L_1(V)$ is primitive.*

Proof *Assume $B \subset L_1(V)$ has at least two elements and for any $T \in Sp(V), T(B) = B$ or $T(B) \cap B = \emptyset$. We show that $B = L_1(V)$. Let $X, Y \in B$. Assume first that $Y \in \Delta(X)$. Let $T \in Sp(V)_X$. Then $X \in B \cap T(B)$ and therefore $T(B) = B$. Thus, $T(Y) \in B$. It follows from Theorem (11.6) that $\Delta(X)$ is contained in B. Suppose $B \neq \{X\} \cap \Delta(X)$. If $Z \in B$ but $X \not\perp Z$, then by Theorem (11.7), $\Gamma(X) \subset B$ and $B = L_1(V)$. Thus it must be the case that $B = \{X\} \cup \Delta(X)$. Reversing the roles of X and Y we also get that $B = \{Y\} \cup \Delta(Y)$. However, if $\boldsymbol{u}_1 = \boldsymbol{x}, \boldsymbol{u}_2 = \boldsymbol{y}$ then $(\boldsymbol{x}_1, \boldsymbol{x}_2)$ can be extended to a hyperbolic basis $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ Then $Span(\boldsymbol{v}_2) \in \Delta(X) \cap \Gamma(Y)$ and we have a contradiction. We can argue similarly if $Y \in \Gamma(X)$. Thus, $B = L_1(V)$.*

As in the case of $SL(V)$ we have an action of $Sp(V)$ on $L_1(V)$ given by $T \cdot X = T(X)$. The kernel of this action consists of the scalar operators $cI_V, c \in \mathbb{F}^*$ which are isometries. Since a hyperbolic pair must go to a hyperbolic pair, it follows that $c = \pm 1$. Clearly this is contained in $Z(Sp(V))$ but we require equality, the subject of the next lemma.

Lemma 11.22 *If (V, f) is a non-degenerate symplectic space, then $Z(Sp(V)) = \{I_V, -I_V\}$.*

Proof *Let $S \in Z(Sp(V))$. We claim that $S(U) = U$ for every maximal totally isotropic subspace of V. Thus, let $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ be a basis for U. Extend this to a hyperbolic basis of $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ for V. Let T be the operator defined by $T(\boldsymbol{u}_i) = \boldsymbol{u}_i, T(\boldsymbol{v}_i) = \boldsymbol{u}_i + \boldsymbol{v}_i$. Then U is the eigenspace for the eigenvalue 1 of T. Since $S \in Sp(V)$ and commutes with T, we must have $S(U) = U$. Now every one-dimensional space in V is the intersection of $n - 1$ totally isotropic subspaces which contain it. Consequently, every one-dimensional subspace of V is fixed by S. As shown in Section (11.1), this implies that S is a scalar operator.*

Definition 11.9 *We will refer to the quotient of $Sp(V)$ by its center as the* **projective symplectic group** *and denote this by $PSp(V)$. We will also denote by $PSp_{2n}(\mathbb{F})$ the isomorphic matrix group.*

Theorem 11.9 *Let (V, f) be a non-degenerate symplectic space of dimension $2n$ over the field $\mathbb{F}$. Then $Sp(V)$ is simple if $(n, \mathbb{F})$ is not one of $(1, \mathbb{F}_2), (1, \mathbb{F}_3)$, or $(2, \mathbb{F}_2)$.*

Proof *The group $PSp(V)$ acts transitively and primitively on $L_1(V)$. Apart from the exceptions, $PSp(V)$ is perfect. For $X \in L_1(V)$ the stabilizer, $PSp(V)_X$ contains the solvable subgroup $\Psi(X)$ which is normal in $PSp(V)_X$. Moreover, since $\Psi(X)$ contains $\chi(X)$ the conjugates of $\Psi(X)$ generate $PSp(V)$. We can therefore invoke Iwasawa's theorem and conclude that $PSp(V)$ is simple.*

Remark 11.5 *The exceptions are really exceptions: $|PSp_2(\mathbb{F}_2)| = 6$ and the group is isomorphic to S_3. $|PSp_2(\mathbb{F}_3)| = 12$ and is isomorphic to A_4. $|PSp_4(\mathbb{F}_2)| = 720$ and is isomorphic to S_6. This is more difficult to show. We outline an approach to proving this in the exercises.*

Exercises

1. Prove part i. of Lemma (11.11).

2. Prove part i. of Lemma (11.12).

3. Prove part ii. of Lemma (11.12).

4. Prove part iii. of Lemma (11.12).

5. Prove Lemma (11.13).

6. Prove part i. of Lemma (11.15).

7. Prove part ii. of Lemma (11.15).

8. Prove part iii. of Lemma (11.15).

9. Prove Corollary (11.5).

10. Let (V, f) be a non-degenerate symplectic space of dimension $2n$ and let $X \in L_1(V)$. Prove that X is the intersection of n maximal totally isotropic subspaces of V.

11. Let (V, f) be a non-degenerate symplectic space over the finite field $\mathbb{F}_q$. Compute the number of hyperbolic bases and, therefore, the order of $Sp(V)$.

12. Let $[1, 6] = \{1, 2, 3, 4, 5, 6\}$ and denote by $[1, 6]^{\{2\}}$ the collection of pairs of $[1, 6]$. Let 0 be a symbol and set $V = \{0\} \cup [1, 6]^{\{2\}}$. Then $|V| = 16$. Define an addition on V as follows:

If $\boldsymbol{v} \in V$ then $0 + \boldsymbol{v} = \boldsymbol{v} + 0 = \boldsymbol{v}$.

If $\alpha \in [1, 6]^{\{2\}}$ then $\alpha + \alpha = 0$.

If $\alpha, \beta \in [1,6]^{\{2\}}$ and $\alpha \cap \beta = \emptyset$ then $\alpha + \beta = [1,6] \setminus (\alpha \cup \beta)$.

If $\alpha \cap \beta \neq \emptyset$ then $\alpha + \beta = (\alpha \cup \beta) \setminus (\alpha \cap \beta)$.

Prove that V is an Abelian group with identity 0 and every non-zero element has order two. Note this means that V is a vector space of dimension four over $\mathbb{F}_2$.

13. Let V be as defined in Exercise 12. Define $f : V \times V \to \mathbb{F}_2$ as follows:

$f(\boldsymbol{v}, 0) = f(0, \boldsymbol{v}) = 0$;

$f(\alpha, \alpha) = 0$ for $\alpha \in [1,6]^{\{2\}}$; and

for $\alpha \neq \beta \in [1,6]^{\{2\}}, f(\alpha, \beta) = 0$ if and only if $\alpha \cap \beta = \emptyset$.

Prove that f is a non-degenerate alternating form on V.

14. Let S_6, the group of permutations of $[1,6]$, act on V as follows:

For $\pi \in S_6$, $\pi(0) = 0, \pi(\{i,j\}) = \{\pi(i), \pi(j)\}$. Prove that S_6 is a subgroup of $Sp(V, f)$, that is, each π is an isometry of (V, f). Use this to conclude that $Sp_4(\mathbb{F}_2)$ is isomorphic to S_6.

11.3 Orthogonal Groups, char $\mathbb{F} \neq 2$

This section follows the previously established pattern but with a slight deviation: We will define the general orthogonal group as the group of isometries of an orthogonal space and the special orthogonal group as the set of those isometries with determinant one. In contrast with the symplectic and special linear groups, the special orthogonal group is not generally perfect. However, we will define a particular subgroup, generated by so-called Siegel transformations, and prove that this group is both the commutator subgroup of the general (special) orthogonal group and perfect. We will prove the quotient of this group by its center is simple except for some specified exceptions.

What You Need to Know

To successfully navigate the material of this new section, you should by now have mastered the following concepts: vector space over a field $\mathbb{F}$, basis of a vector space, dimension of a vector space, linear operator on a vector space V, matrix of a linear operator $T : V \to V$ with respect to a base $\mathcal{B}$ for V, eigenvalue and eigenvector of an operator T, the algebra $\mathcal{L}(V, V)$ of operators on a finite-dimensional vector space V, an invertible operator on a vector space V, the group $GL(V)$ of invertible operators on a finite-dimensional vector space V, bilinear form, reflexive bilinear form, symmetric bilinear form, quadratic form, orthogonal space, non-degenerate orthogonal space, singular vector in an orthogonal space, totally singular subspace in an orthogonal space, hyperbolic pair in an orthogonal space, an isometry of an orthogonal space, and the reflection defined by a non-singular vector. You must also be familiar with the following concepts from group theory: Abelian group, solvable group, normal subgroup of a group, quotient group of a group by a normal subgroup, the commutator of two elements in a group, the commutator subgroup of a group, a perfect group, the center of a group, a simple group, action of a group G on a set X, transitive action of a group G on a set X, primitive action of a group G on a set X, and a faithful action of a group G on a set X. This latter material can be found in Appendix B

We begin by recalling some definitions.

Let V be a vector space over a field $\mathbb{F}$. By a **quadratic form** on V we mean a function $\phi : V \to \mathbb{F}$ which satisfies

1) for $\boldsymbol{v} \in V, a \in \mathbb{F}, \phi(a\boldsymbol{v}) = a^2\phi(\boldsymbol{v})$; and

2) if we define $\langle\ ,\ \rangle_\phi : V \times V \to \mathbb{F}$ by $\langle \boldsymbol{v}, \boldsymbol{w}\rangle_\phi = \phi(\boldsymbol{v}+\boldsymbol{w}) - \phi(\boldsymbol{v}) - \phi)(\boldsymbol{w})$ then $\langle\ ,\ \rangle_\phi$ is a symmetric bilinear form, referred to as the form associated to ϕ.

An **orthogonal space** is a pair (V, ϕ) consisting of a vector space V and a quadratic form $\phi : V \to \mathbb{F}$. The space is non-degenerate if the associated bilinear form $\langle\ ,\ \rangle_\phi$ is **non-degenerate**, that is, for all $\boldsymbol{v} \in V$ there exists $\boldsymbol{w} \in V$ such that $\langle \boldsymbol{v}, \boldsymbol{w}\rangle_\phi \neq 0$.

A non-zero vector $\boldsymbol{v}$ is **singular** if $\phi(\boldsymbol{v}) = 0$ and non-singular otherwise. The orthogonal space (V, ϕ) is said to be **singular** if it contains singular vectors. Two vectors $\boldsymbol{v}$ and $\boldsymbol{w}$ are **orthogonal**, and we write $\boldsymbol{v} \perp \boldsymbol{w}$, if $\langle \boldsymbol{v}, \boldsymbol{w}\rangle_\phi = 0$. A subspace W of V is **totally singular** if $\phi(\boldsymbol{v}) = 0$ for all $\boldsymbol{v} \in W$.

An **isometry** of an orthogonal space (V, ϕ) is an operator $T : V \to V$ such that $\phi(T(\boldsymbol{v})) = \phi(\boldsymbol{v})$ for all $\boldsymbol{v} \in V$. An isometry is invertible and the composition of isometries is an isometry. Consequently, the collection of all isometries is a subgroup of $GL(V)$. We denote it by $O(V, \phi)$ or just $O(V)$. If T is an isometry of (V, ϕ), then it also satisfies $\langle T(\boldsymbol{v}), T(\boldsymbol{w})\rangle_\phi = \langle \boldsymbol{v}, \boldsymbol{w}\rangle_\phi$ for all $\boldsymbol{v}, \boldsymbol{w} \in V$. If the characteristic of $\mathbb{F}$ is not two then the converse holds as well since in this situation $\phi(\boldsymbol{v}) = \frac{1}{2}\langle \boldsymbol{v}, \boldsymbol{v}\rangle_\phi$. The **special orthogonal group** is the intersection $O(V, \phi) \cap SL(V)$ and is denoted $SO(V, \phi)$ or just $SO(V)$.

Throughout this section we will assume that (V, ϕ) is a finite-dimensional non-degenerate, singular orthogonal space over $\mathbb{F}$ and that the characteristic of $\mathbb{F}$ is not two. We will denote by $S_1(V)$ those $X = Span(\boldsymbol{x}) \in L_1(V)$ such that $\boldsymbol{x}$ is singular. If $X \in S_1(V)$ we set $\Gamma(X) = \{Y \in S_1(V) | Y \not\perp X\}$. Further, if the Witt index of V is at least two, then for $X \in S_1(V)$ we will set $\Delta(X) = S_1(X^\perp)$. In our first result we determine the structure of $O(V, \phi)$ and $SO(V, \phi)$ when $dim(V) = 2$. Before doing so recall that if $\boldsymbol{y}$ is a non-singular vector, the **reflection** through $\boldsymbol{y}, \rho_{\boldsymbol{y}}$ is defined by $\rho_{\boldsymbol{y}}(\boldsymbol{x}) = \boldsymbol{x} - 2\frac{\langle \boldsymbol{x}, \boldsymbol{y}\rangle}{\langle \boldsymbol{y}, \boldsymbol{y}\rangle}\boldsymbol{y}$. It fixes every vector $\boldsymbol{x} \in \boldsymbol{y}^\perp$ and takes $\boldsymbol{y}$ to $-\boldsymbol{y}$.

Hereafter, throughout this section we will drop the subscript ϕ and write $\langle\ ,\ \rangle$ instead of $\langle\ ,\ \rangle_\phi$.

Theorem 11.10 *Assume $dim(V) = 2$. Then $SO(V, \phi)$ is isomorphic to the multiplicative group of $\mathbb{F}$. Every element of $O(V, \phi) \setminus SO(V, \phi)$ is a reflection.*

Proof *Let $(\boldsymbol{u}, \boldsymbol{v})$ be a hyperbolic basis of V so that $\phi(\boldsymbol{u}) = \phi(\boldsymbol{v}) = 0$ and $\langle \boldsymbol{u}, \boldsymbol{v}\rangle = 1$. Note that $S_1(V) = \{Span(\boldsymbol{u}), Span(\boldsymbol{v})\}$. Let $T \in O(V, \phi)$ then either $(T(\boldsymbol{u}), T(\boldsymbol{v})) = (a\boldsymbol{u}, b\boldsymbol{v})$ or $(a\boldsymbol{v}, b\boldsymbol{u})$ for some non-zero scalars a, b. Since $1 = \langle \boldsymbol{u}, \boldsymbol{v}\rangle = \langle T(\boldsymbol{u}), T(\boldsymbol{v})\rangle = ab$ we must have $b = a^{-1}$. In the first case, $det(T) = 1$ and T is in $SO(V, \phi)$. The map that takes a to T_a where $T_a(\boldsymbol{u}) = a\boldsymbol{u}, T_a(\boldsymbol{v}) = a^{-1}\boldsymbol{v}$ is an isomorphism of $\mathbb{F}^*$ to $SO(V, \phi)$.*

On the other hand, suppose $a \in \mathbb{F}^*$ and $T(\boldsymbol{u}) = a\boldsymbol{v}, T(\boldsymbol{v}) = a^{-1}\boldsymbol{u}$. Set $\boldsymbol{x} = \boldsymbol{u} + a\boldsymbol{v}$ and $\boldsymbol{y} = \boldsymbol{u} - a\boldsymbol{v}$. Then $T(\boldsymbol{x}) = \boldsymbol{x}$ and $T(\boldsymbol{y}) = -\boldsymbol{y}$ so that $T = \rho_{\boldsymbol{y}}$, the reflection through $\boldsymbol{y}$.

We now prove an important result, the Cartan–Dieudonne theorem.

Theorem 11.11 *Assume $dim(V) = n$ and $T \in O(V, \phi), T \neq I_V$. Then T can be expressed as a product of at most n reflections.*

Proof *The proof is by induction on n. If $n = 1$ then $T = -I_V$ is a reflection. So assume the result is true for spaces of dimension less than n and that $dim(V) = n$. Let $T \in O(V, \phi), T \neq I_V$. Suppose first that there exists a non-singular vector $\boldsymbol{v}$ such that $T(\boldsymbol{v}) = \boldsymbol{v}$. Since $\boldsymbol{v}$ is non-singular, $\boldsymbol{v}^{\perp}$ is non-degenerate and T-invariant. Since $T \neq I_V, T_{|\boldsymbol{v}^{\perp}} \neq I_{\boldsymbol{v}^{\perp}}$ and by induction, $T_{|\boldsymbol{v}^{\perp}}$ is a product of at most $n-1$ reflections, thus T is the product of at most $n-1$ reflections. We may therefore assume that $ker(T - I_V) = \{\mathbf{0}\}$ or is totally singular.*

Suppose now that there exists $\boldsymbol{z}$ non-singular such that $\boldsymbol{w} = T(\boldsymbol{z}) - \boldsymbol{z}$ is non-singular. Set $\boldsymbol{u} = T(\boldsymbol{z}) + \boldsymbol{z}$, we claim that $\boldsymbol{w} \perp \boldsymbol{u}$. We compute

$$\begin{aligned}
\langle \boldsymbol{w}, \boldsymbol{u}\rangle &= \langle T(\boldsymbol{z}) - \boldsymbol{z}, T(\boldsymbol{z}) + \boldsymbol{z}\rangle \\
&= \langle T(\boldsymbol{z}), T(\boldsymbol{z})\rangle + \langle T(\boldsymbol{z}), \boldsymbol{z}\rangle - \langle \boldsymbol{z}, T(\boldsymbol{z})\rangle - \langle \boldsymbol{z}, \boldsymbol{z}\rangle \\
&= \langle \boldsymbol{z}, \boldsymbol{z}\rangle - \langle \boldsymbol{z}, \boldsymbol{z}\rangle \\
&= 0.
\end{aligned}$$

Now $\boldsymbol{z} = \frac{1}{2}(\boldsymbol{u} - \boldsymbol{w})$ and $T(\boldsymbol{z}) = \frac{1}{2}(\boldsymbol{u} + \boldsymbol{w})$. Then $\rho_{\boldsymbol{w}}(\boldsymbol{z}) = \rho_{\boldsymbol{w}}(\frac{\boldsymbol{u}-\boldsymbol{w}}{2}) = \frac{1}{2}[\rho_{\boldsymbol{w}}(\boldsymbol{u}) - \rho_{\boldsymbol{w}}(\boldsymbol{w})] = \frac{1}{2}[\boldsymbol{u} + \boldsymbol{w}] = T(\boldsymbol{z})$. It then follows that $\rho_{\boldsymbol{w}} T(\boldsymbol{z}) = \boldsymbol{z}$. Then by the above $\rho_{\boldsymbol{w}} T$ is a product of at most $n - 1$ reflections so that T is a product of at most n reflections.

Consequently, we may assume there does not exist a non-singular vector $\boldsymbol{z}$ such that $T(\boldsymbol{z}) - \boldsymbol{z}$ is non-singular. We claim that this implies that $Range(T - I_V)$ is totally singular. Assume to the contrary and let $\boldsymbol{x}$ be a singular vector such that $T(\boldsymbol{x}) - \boldsymbol{x}$ is non-singular. Then there exists a singular vector $\boldsymbol{y}$ such that $\langle \boldsymbol{x}, \boldsymbol{y}\rangle = 1$. Assume now that $\mathbb{F} \neq \mathbb{F}_3$ and let $a \in \mathbb{F}^*, a \neq \pm 1$. Then $\boldsymbol{x}+\boldsymbol{y}, \boldsymbol{x}-\boldsymbol{y}$ and $\boldsymbol{x} + a\boldsymbol{y}$ are all non-singular vectors. Then t

$$T(\boldsymbol{x} + \boldsymbol{y}) - (\boldsymbol{x} + \boldsymbol{y}) = [T(\boldsymbol{x}) - \boldsymbol{x}] + [T(\boldsymbol{y}) - \boldsymbol{y}],$$
$$T(\boldsymbol{x} - \boldsymbol{y}) = [T(\boldsymbol{x}) - \boldsymbol{x}] - [T(\boldsymbol{y}) - \boldsymbol{y}],$$

, and

$$T(\boldsymbol{x} + a\boldsymbol{y}) - (\boldsymbol{x} + a\boldsymbol{y}) = [T(\boldsymbol{x}) - \boldsymbol{x}] + a[T(\boldsymbol{y}) - \boldsymbol{y}]$$

are all singular. This implies that $T(\boldsymbol{x}) - \boldsymbol{x}$ and $T(\boldsymbol{y}) - \boldsymbol{y}$ are singular, a contradiction.

We may therefore assume that $\mathbb{F} = \mathbb{F}_3$. Suppose $n = 2$. Then $(T(\boldsymbol{x}), T(\boldsymbol{y})) = (-\boldsymbol{x}, -\boldsymbol{y}), (\boldsymbol{y}, \boldsymbol{x})$, or $(-\boldsymbol{y}, -\boldsymbol{x})$. In the first case, $T = \rho_{\boldsymbol{x}+\boldsymbol{y}}\rho_{\boldsymbol{x}-\boldsymbol{y}}$. In the second case, $T = \rho_{\boldsymbol{x}-\boldsymbol{y}}$ and in the third case $T = \rho_{\boldsymbol{x}+\boldsymbol{y}}$. We may therefore assume that $n \geq 3$.

Set $\boldsymbol{u} = \boldsymbol{x}+\boldsymbol{y}, \boldsymbol{v} = \boldsymbol{x}-\boldsymbol{y}$ and let $\boldsymbol{w} \in \boldsymbol{x}^\perp \cap \boldsymbol{y}^\perp = \boldsymbol{u}^\perp \cap \boldsymbol{v}^\perp$ with $\boldsymbol{w}$ non-singular. Then $\phi(\boldsymbol{w}) = \pm 1$. Suppose $\phi(\boldsymbol{w}) = 1$. Set $\boldsymbol{u}' = T(\boldsymbol{u}) - \boldsymbol{u}, \boldsymbol{v}' = T(\boldsymbol{v}) - \boldsymbol{v}, \boldsymbol{w}' = T(\boldsymbol{w}) - \boldsymbol{w}$ and $U' = Span(\boldsymbol{u}', \boldsymbol{v}', \boldsymbol{w}')$. Note that $\boldsymbol{u} + \boldsymbol{w}$ is non-singular and therefore $T(\boldsymbol{u}+\boldsymbol{w}) \neq \boldsymbol{u}+\boldsymbol{w}$ so, in particular, $\boldsymbol{u}' = T(\boldsymbol{u})-\boldsymbol{u} \neq T(\boldsymbol{w})-\boldsymbol{w} = \boldsymbol{w}'$. It follows that $Span(\boldsymbol{u}', \boldsymbol{w}')$ is a totally singular two-dimensional subspace. Since $T(\boldsymbol{x})-\boldsymbol{x} \in U'$ is non-singular it follows that $dim(U') = 3$ and the radical of U' is non-trivial and contained in $Span(\boldsymbol{u}', \boldsymbol{w}')$. Note that this implies that $(\boldsymbol{u}', \boldsymbol{v}', \boldsymbol{w}')$ is linearly independent. If $dim(Rad(U')) = 2$ then every singular vector of U' is contained in $Span(\boldsymbol{u}', \boldsymbol{w}')$, in particular, $\boldsymbol{v}' \in Span(\boldsymbol{u}', \boldsymbol{w}')$, a contradiction. Therefore $dim(Rad(U')) = 1$. It then follows that there are 14 singular vectors in U'. However, there are 18 non-singular vectors in U. By the pigeonhole principle there must be non-singular vectors $\boldsymbol{z}, \boldsymbol{z}' \in U$ such that $(T - I_V)(\boldsymbol{z}) = (T - I_V)(\boldsymbol{z}')$. However, this contradicts $(\boldsymbol{u}', \boldsymbol{v}', \boldsymbol{w}')$ linearly independent and we have a contradiction. Thus, $Range(T - I_V)$ is totally singular as claimed.

Since $Range(T - I_V)$ is totally singular, $Range(T-I_V) \subseteq Range(T-I_V)^\perp = ker(T - I_V)$. As shown above, $ker(T - I_V) = \{\boldsymbol{0}\}$ or $ker(T - I_V)$ is totally singular. Since $T \neq I_V, Range(T - I_V) \neq \{\boldsymbol{0}\}$ so, in fact, $ker(T - I_V)$ is totally singular. Then $ker(T - I_V) \subseteq ker(T - I_V)^\perp = Range(T - I_V)$. We therefore have $ker(T - I_V) = Range(T - I_V)$. If $m = dim(ker(T - I_V))$ then by the rank-nullity theorem, $n = dim(V) = 2m$. We can also conclude that the minimum polynomial of T is $(x-1)^2$ from which it follows that $det(T) = 1$ and $T \in SO(V, \phi)$. Let $\boldsymbol{u}$ be any non-singular vector. Then $det(\rho_{\boldsymbol{u}} T) = -1$ and therefore $\rho_{\boldsymbol{u}} T$ is the product of at most n reflections from which we conclude that T is a product of at most $n+1$ reflections. However, if T were a product of $n + 1 = 2m + 1$ reflections then $det(T) = -1$, a contradiction. Thus, T is a product of at most n reflections.

Corollary 11.6 *Assume $dim(V) = n$ and $T = \rho_{\boldsymbol{x}_1} \dots \rho_{\boldsymbol{x}_m}$ with $m < n$. Then $dim(Ker(T - I_V)) \geq n - m$.*

Proof *Set $X = Span(\boldsymbol{x}_1, \dots, \boldsymbol{x}_m)$. Then the kernel of $T - I_V$ contains $X^\perp$ and $dim(X^\perp) = n - dim(X) \geq n - m$.*

Corollary 11.7 *Assume $T = \rho_{\boldsymbol{x}_1} \dots \rho_{\boldsymbol{x}_m}$ and $ker(T - I_V) = \{\boldsymbol{0}\}$. Then $m \geq n$.*

We now revisit some isometries that were the subject of exercises in Section (8.3).

Theorem 11.12 *Let $\boldsymbol{u}$ be a singular vector and $\boldsymbol{v} \in \boldsymbol{u}^\perp$. Then there exists a unique isometry τ of V such that for $\boldsymbol{x} \in \boldsymbol{u}^\perp, \tau(\boldsymbol{x}) = \boldsymbol{x} + \langle \boldsymbol{x}, \boldsymbol{v} \rangle \boldsymbol{u}$.*

Proof *For $\boldsymbol{x} \in \boldsymbol{u}^\perp$ let $T(\boldsymbol{x}) = \boldsymbol{x} + \langle \boldsymbol{x}, \boldsymbol{v}\rangle \boldsymbol{u}$. We first show that T is an isometry of $\boldsymbol{u}^\perp$. Let $\boldsymbol{x}, \boldsymbol{y} \in \boldsymbol{u}^\perp$. Then*

$$\begin{aligned}
\langle T(\boldsymbol{x}), T(\boldsymbol{y})\rangle &= \langle \boldsymbol{x} + \langle \boldsymbol{x}, \boldsymbol{v}\rangle \boldsymbol{u}, \boldsymbol{y} + \langle \boldsymbol{y}, \boldsymbol{v}\rangle \boldsymbol{u}\rangle \\
&= \langle \boldsymbol{x}, \boldsymbol{y}\rangle + \langle \boldsymbol{y}, \boldsymbol{v}\rangle\langle \boldsymbol{x}, \boldsymbol{u}\rangle + \langle \boldsymbol{x}, \boldsymbol{v}\rangle\langle \boldsymbol{u}, \boldsymbol{y}\rangle + \langle \boldsymbol{x}, \boldsymbol{v}\rangle\langle \boldsymbol{y}, \boldsymbol{v}\rangle\langle \boldsymbol{u}, \boldsymbol{u}\rangle \\
&= \langle \boldsymbol{x}, \boldsymbol{y}\rangle.
\end{aligned}$$

By Witt's theorem, Theorem (8.12), there exists an extension τ to all of V. We show that τ is unique. We claim that there exists a singular vector $\boldsymbol{w} \in \boldsymbol{v}^\perp$ such that $\langle \boldsymbol{u}, \boldsymbol{w}\rangle \neq 0$. If $\boldsymbol{v}$ is singular, this follows from Lemma (8.28). If $\boldsymbol{v}$ is non-singular then $\boldsymbol{v}^\perp$ is non-degenerate and again the claim follows from Lemma (8.24). By replacing $\boldsymbol{w}$ by $\frac{1}{\langle \boldsymbol{u}, \boldsymbol{w}\rangle}\boldsymbol{w}$, if necessary, we can assume $\langle \boldsymbol{u}, \boldsymbol{w}\rangle = 1$. Assume $\tau(\boldsymbol{w}) = a\boldsymbol{u} + \boldsymbol{z} + b\boldsymbol{w}$ where $a, b \in \mathbb{F}$ and $\boldsymbol{z} \in \boldsymbol{u}^\perp \cap \boldsymbol{w}^\perp$. Now

$$\begin{aligned}
1 &= \langle \boldsymbol{u}, \boldsymbol{w}\rangle \\
&= \langle \tau(\boldsymbol{u}), \tau(\boldsymbol{w})\rangle \\
&= \langle \boldsymbol{u}, a\boldsymbol{u} + \boldsymbol{z} + b\boldsymbol{w}\rangle \\
&= b.
\end{aligned}$$

It therefore follows that $b = 1$. Next, let $\boldsymbol{x} \in \boldsymbol{u}^\perp \cap \boldsymbol{w}^\perp$. Then

$$\begin{aligned}
0 &= \langle \boldsymbol{x}, \boldsymbol{w}\rangle \\
&= \langle \tau(\boldsymbol{x}), \tau(\boldsymbol{w})\rangle \\
&= \langle \boldsymbol{x} + \langle \boldsymbol{x}, \boldsymbol{v}\rangle \boldsymbol{u}, a\boldsymbol{u} + \boldsymbol{z} + \boldsymbol{w}\rangle \\
&= \langle \boldsymbol{x}, \boldsymbol{z}\rangle + \langle \boldsymbol{x}, \boldsymbol{v}\rangle\langle \boldsymbol{u}, \boldsymbol{w}\rangle \\
&= \langle \boldsymbol{x}, \boldsymbol{z}\rangle + \langle \boldsymbol{x}, \boldsymbol{v}\rangle \\
&= \langle \boldsymbol{x}, \boldsymbol{z} + \boldsymbol{v}\rangle.
\end{aligned}$$

It follows that $\langle \boldsymbol{x}, \boldsymbol{z} + \boldsymbol{v}\rangle = 0$ for every $\boldsymbol{x} \in \boldsymbol{u}^\perp \cap \boldsymbol{w}^\perp$. However, $\boldsymbol{u}^\perp \cap \boldsymbol{w}^\perp$ is non-degenerate so that $\boldsymbol{z} + \boldsymbol{v} = 0$, hence $\boldsymbol{z} = -\boldsymbol{v}$.

Finally, $0 = \phi(\boldsymbol{w}) = \phi(\tau(\boldsymbol{w})) = \phi(a\boldsymbol{u} - \boldsymbol{v} + \boldsymbol{w}) = \phi(\boldsymbol{v}) + a$ and therefore $a = -\phi(\boldsymbol{v})$. This proves that τ is unique.

Definition 11.10 *Let $\boldsymbol{u}$ be a singular vector, $\boldsymbol{v} \in \boldsymbol{u}^\perp$. We will denote by $\tau_{\boldsymbol{u},\boldsymbol{v}}$ the unique isometry of V such that $\tau_{\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{x}) = \boldsymbol{x} + \langle \boldsymbol{x}, \boldsymbol{v}\rangle \boldsymbol{u}$ for $\boldsymbol{x} \in \boldsymbol{u}^\perp$. This is referred to as a Siegel transformation.*

These isometries will play a role in orthogonal groups similar to that of transvections in linear and symplectic groups. In the next couple of results we uncover some of their properties. These results should be compared to corresponding results for transvections.

Lemma 11.23 *Let $\boldsymbol{u}$ be a singular vector and $\boldsymbol{v} \in \boldsymbol{u}^\perp$. Then $\tau_{\boldsymbol{u},\boldsymbol{v}} = I_V$ if and only if $\boldsymbol{v} \in Span(\boldsymbol{u})$.*

We leave this as an exercise.

Lemma 11.24 *Let $\boldsymbol{u}$ be a singular vector and $\boldsymbol{v} \in \boldsymbol{u}^\perp$. Then $\tau_{\boldsymbol{u},\boldsymbol{v}} \in SO(V,\phi)$.*

Proof *If $\boldsymbol{v} \in Span(\boldsymbol{u})$, then $\tau_{\boldsymbol{u},\boldsymbol{v}} = I_V \in SO(V,\phi)$ by Lemma (11.23). Assume $\boldsymbol{v} \notin Span(\boldsymbol{u})$. Let $\boldsymbol{w}$ be a singular vector, $\boldsymbol{w} \notin \boldsymbol{u}^\perp$. Now $\boldsymbol{w}^\perp \cap Span(\boldsymbol{u},\boldsymbol{v}) \neq \{\boldsymbol{0}\}$. Suppose $a\boldsymbol{u}+\boldsymbol{v} \perp \boldsymbol{w}$. Then $\tau_{\boldsymbol{u},a\boldsymbol{u}+\boldsymbol{v}} = \tau_{\boldsymbol{u},\boldsymbol{v}}$. Thus, by replacing $\boldsymbol{v}$ with $a\boldsymbol{u}+\boldsymbol{v}$, if necessary, we may assume that $\boldsymbol{w} \perp \boldsymbol{v}$. It then follows that $\tau_{\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{w}) = -\phi(\boldsymbol{v})\boldsymbol{u}+\boldsymbol{v}+\boldsymbol{w}$ so that $(\tau_{\boldsymbol{u},\boldsymbol{v}} - I_V)(\boldsymbol{w}) = -\phi(\boldsymbol{v})\boldsymbol{u}+\boldsymbol{v} \in Span(\boldsymbol{u},\boldsymbol{v})$.*

By the definition of $\tau_{\boldsymbol{u},\boldsymbol{v}}$ it then follows that $(\tau_{\boldsymbol{u},\boldsymbol{v}} - I_V)(\boldsymbol{v}) \in Span(\boldsymbol{v})$ and is the zero vector if and only if $\boldsymbol{v}$ is singular. It therefore follows that the minimum polynomial of $\tau_{\boldsymbol{u},\boldsymbol{v}}$ is $(x-1)^2$ if $\boldsymbol{v}$ is singular and $(x-1)^3$ if $\boldsymbol{v}$ is non-singular. In either case, $det(\tau_{\boldsymbol{u},\boldsymbol{v}}) = 1$ and $\tau_{\boldsymbol{u},\boldsymbol{v}} \in SO(V,\phi)$.

Lemma 11.25 *Let $\boldsymbol{u}$ be a singular vector, and $\boldsymbol{v},\boldsymbol{w}$ vectors in $\boldsymbol{u}^\perp$. Then $\tau_{\boldsymbol{u},\boldsymbol{v}}\tau_{\boldsymbol{u},\boldsymbol{w}} = \tau_{\boldsymbol{u},\boldsymbol{v}+\boldsymbol{w}}$.*

Proof *By Theorem (11.12) it suffices to prove for $\boldsymbol{x} \in \boldsymbol{u}^\perp$ that $\tau_{\boldsymbol{u},\boldsymbol{v}}\tau_{\boldsymbol{u},\boldsymbol{w}}(\boldsymbol{x}) = \boldsymbol{x} + \langle \boldsymbol{x},\boldsymbol{v}+\boldsymbol{w}\rangle\boldsymbol{u}$. We compute:*

$$\begin{aligned}
\tau_{\boldsymbol{u},\boldsymbol{v}}\tau_{\boldsymbol{u},\boldsymbol{w}}(\boldsymbol{x}) &= \tau_{\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{x} + \langle \boldsymbol{x},\boldsymbol{w}\rangle\boldsymbol{u}) \\
&= \tau_{\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{x}) + \langle \boldsymbol{x},\boldsymbol{w}\rangle\tau_{\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{u}) \\
&= \boldsymbol{x} + \langle \boldsymbol{x},\boldsymbol{v}\rangle\boldsymbol{u} + \langle \boldsymbol{x},\boldsymbol{w}\rangle\boldsymbol{u} \\
&= \boldsymbol{x} + \langle \boldsymbol{x},\boldsymbol{v}+\boldsymbol{w}\rangle\boldsymbol{u}
\end{aligned}$$

as was to be shown.

Corollary 11.8 *Let $\boldsymbol{u}$ be a singular vector and $\boldsymbol{v} \in \boldsymbol{u}^\perp$. Then $\tau_{\boldsymbol{u},\boldsymbol{v}}^{-1} = \tau_{\boldsymbol{u},-\boldsymbol{v}}$.*

Proof *This follows immediately from Lemma (11.25).*

Corollary 11.9 *Let $\boldsymbol{u}$ be a singular vector and $\boldsymbol{v} \in \boldsymbol{u}^\perp$. Then $\tau_{\boldsymbol{u},\boldsymbol{u}+\boldsymbol{v}} = \tau_{\boldsymbol{u},\boldsymbol{v}}$.*

We leave this as an exercise.

Notation Let $\boldsymbol{u}$ be a singular vector. Denote by $T_{\boldsymbol{u}}$ the set of all $\tau_{\boldsymbol{u},\boldsymbol{v}}$ such that $\boldsymbol{v} \in \boldsymbol{u}^\perp$. Also, denote by $\Omega(V)$ the subgroup of $SO(V,\phi)$ generated by all $T_{\boldsymbol{u}}$ such that $\boldsymbol{u}$ is a singular vector. It follows from Lemma (11.25) and Corollary (11.8) that $T_{\boldsymbol{u}}$ is an Abelian subgroup of $O(V,\phi)$.

Lemma 11.26 *Let $(\boldsymbol{u},\boldsymbol{w})$ be a hyperbolic pair and set $X = \boldsymbol{u}^\perp \cap \boldsymbol{w}^\perp$. The map that sends $\boldsymbol{v} \in X$ to $\tau_{\boldsymbol{u},\boldsymbol{v}}$ is an isomorphism of Abelian groups.*

Proof *This follows immediately from Lemma (11.25) and Lemma (11.8).*

Lemma 11.27 *Let $\boldsymbol{u}$ be a singular vector, $\boldsymbol{v} \in \boldsymbol{u}^\perp$ and $\sigma \in O(V,\phi)$. Then $\sigma\tau_{\boldsymbol{u},\boldsymbol{v}}\sigma^{-1} = \tau_{\sigma(\boldsymbol{u}),\sigma(\boldsymbol{v})}$.*

Proof *It suffices to show for $\boldsymbol{y} \in \sigma(\boldsymbol{u})^\perp$ that $\sigma\tau_{\boldsymbol{u},\boldsymbol{v}}\sigma^{-1}(\boldsymbol{y}) = \boldsymbol{y} + \langle \boldsymbol{y}, \sigma(\boldsymbol{v})\rangle\sigma(\boldsymbol{u})$. Set $\boldsymbol{x} = \sigma^{-1}(\boldsymbol{y}) \in \boldsymbol{u}^\perp$. We compute:*

$$\begin{aligned}
\sigma\tau_{\boldsymbol{u},\boldsymbol{v}}\sigma^{-1}(\boldsymbol{y}) &= \sigma\tau_{\boldsymbol{u},\boldsymbol{v}}\sigma^{-1}(\sigma(\boldsymbol{x})) \\
&= \sigma\tau_{\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{x}) \\
&= \sigma(\boldsymbol{x} + \langle \boldsymbol{x}, \boldsymbol{v}\rangle \boldsymbol{u}) \\
&= \sigma(\boldsymbol{x}) + \langle \boldsymbol{x}, \boldsymbol{v}\rangle \sigma(\boldsymbol{u}) \\
&= \sigma(\boldsymbol{x}) + \langle \sigma(\boldsymbol{x}), \sigma(\boldsymbol{v})\rangle \sigma(\boldsymbol{u}) \\
&= \tau_{\sigma(\boldsymbol{u}),\sigma(\boldsymbol{v})}(\sigma(\boldsymbol{x})) \\
&= \tau_{\sigma(\boldsymbol{u}),\sigma(\boldsymbol{v})}(\boldsymbol{y}).
\end{aligned}$$

The following is an immediate consequence of Lemma (11.27):

Corollary 11.10 *Let $\boldsymbol{u}$ be a singular vector and $\sigma \in O(V,\phi)$, Then $\sigma T_{\boldsymbol{u}}\sigma^{-1} = T_{\sigma(\boldsymbol{u})}$. In particular, if $U = Span(\boldsymbol{u})$, then $T_{\boldsymbol{u}}$ is a normal subgroup of $O(V,\phi)_U = \{S \in O(V,\phi) | S(U) = U\}$.*

Corollary 11.11 *The subgroup $\Omega(V)$ is normal in $O(V,\phi)$.*

In our next result we prove that for $\boldsymbol{u}$ a singular vector the subgroup $T_{\boldsymbol{u}}$ is simply transitive on $\Gamma(Span(\boldsymbol{u}))$.

Lemma 11.28 *Let $\boldsymbol{u}$ be a singular vector and set $U = Span(\boldsymbol{u})$. Assume $\boldsymbol{w}$ and $\boldsymbol{x}$ are singular vectors satisfying $\langle \boldsymbol{u}, \boldsymbol{w}\rangle = \langle \boldsymbol{u}, \boldsymbol{x}\rangle = 1$. Then there exists a unique $\tau \in T_{\boldsymbol{u}}$ such that $\tau(\boldsymbol{w}) = \boldsymbol{x}$.*

Proof *Since $\langle \boldsymbol{u}, \boldsymbol{w}\rangle = \langle \boldsymbol{u}, \boldsymbol{x}\rangle = 1$, it follows that $\langle \boldsymbol{u}, \boldsymbol{x} - \boldsymbol{w}\rangle = 0$, that is. $\boldsymbol{v} = \boldsymbol{x} - \boldsymbol{w} \in \boldsymbol{u}^{\perp}$. Suppose $\phi(\boldsymbol{v}) = 0$. Then $\langle \boldsymbol{v}, \boldsymbol{w}\rangle = 0$ and from the proof of Theorem (11.12) we can conclude that $\tau_{\boldsymbol{u},-\boldsymbol{v}}(\boldsymbol{w}) = \boldsymbol{w} + \boldsymbol{v} = \boldsymbol{x}$. Assume then that $\langle \boldsymbol{v}, \boldsymbol{w}\rangle = \langle \boldsymbol{x} - \boldsymbol{w}, \boldsymbol{w}\rangle = a$. Then $\boldsymbol{v}' = \boldsymbol{v} + a\boldsymbol{u} \in \boldsymbol{u}^{\perp} \cap \boldsymbol{w}^{\perp}$. Moreover,*

$$\begin{aligned}
\phi(\boldsymbol{v}') &= \phi(\boldsymbol{v} + a\boldsymbol{u}) \\
&= \phi(\boldsymbol{v}) - a\langle \boldsymbol{v}, \boldsymbol{u}\rangle + a^2\langle \boldsymbol{u}, \boldsymbol{u}\rangle \\
&= \phi(\boldsymbol{v}) \\
&= \frac{1}{2}\langle \boldsymbol{x} - \boldsymbol{w}, \boldsymbol{x} - \boldsymbol{w}\rangle \\
&= -\frac{1}{2}\cdot 2\langle \boldsymbol{x}, \boldsymbol{w}\rangle \\
&= -a.
\end{aligned}$$

Again by the proof of Theorem (11.12) it follows that

$$\begin{aligned}
\tau_{\boldsymbol{u},-\boldsymbol{v}'}(\boldsymbol{w}) &= \boldsymbol{w} + \boldsymbol{v}' - \phi(\boldsymbol{v}')\boldsymbol{u} \\
&= \boldsymbol{w} + (\boldsymbol{x} - \boldsymbol{w} + a\boldsymbol{u}) - a\boldsymbol{u} \\
&= \boldsymbol{x}.
\end{aligned}$$

As for uniqueness, suppose $\boldsymbol{v}, \boldsymbol{y} \in \boldsymbol{u}^{\perp} \cap \boldsymbol{w}^{\perp}$ and $\tau_{\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{w}) = \tau_{\boldsymbol{u},\boldsymbol{y}}(\boldsymbol{w}) = \boldsymbol{x}$. Then $\tau_{\boldsymbol{u},-\boldsymbol{v}}\tau_{\boldsymbol{u},\boldsymbol{y}}(\boldsymbol{w}) = \tau_{\boldsymbol{u},\boldsymbol{y}-\boldsymbol{v}}(\boldsymbol{w}) = \boldsymbol{w}$. However, by the proof of Theorem (11.12) $\tau_{\boldsymbol{u},\boldsymbol{y}-\boldsymbol{v}}(\boldsymbol{w}) = \boldsymbol{w} + (\boldsymbol{y} - \boldsymbol{v}) - \phi(\boldsymbol{y} - \boldsymbol{v})\boldsymbol{u}$. It follows that $\boldsymbol{y} - \boldsymbol{v} = \boldsymbol{0}$ so that $\boldsymbol{y} = \boldsymbol{v}$.

Corollary 11.12 *Assume that $dim(V) \geq 3$ and that the Witt index of (V, ϕ) is one. Then $\Omega(V)$ is doubly transitive on $S_1(V)$. In particular, $\Omega(V)$ acts primitively on $S_1(V)$.*

Proof *Assume $X, Y \in S_1(V)$. Since $dim(V) \geq 3$ there exists $Z \in S_1(V)$ such that Z is equal to neither X nor Y. Let $\boldsymbol{z} \in Z$ and let $\boldsymbol{x} \in X, \boldsymbol{y} \in Y$ such that $\langle \boldsymbol{z}, \boldsymbol{x}\rangle = \langle \boldsymbol{z}, \boldsymbol{y}\rangle = 1$. By Lemma (11.28) there is a unique $\tau \in T_{\boldsymbol{z}}$ such that $\tau(\boldsymbol{x}) = \boldsymbol{y}$ and then $\tau(X) = Y$. This proves that $\Omega(V)$ is transitive on $S_1(V)$. Also, by Lemma (11.28) there exists a unique $\sigma \in T_{\boldsymbol{x}}$ such that $\sigma(\boldsymbol{y}) = \boldsymbol{z}$. Note that $\sigma(\boldsymbol{x}) = \boldsymbol{x}$ so that $\sigma(X) = X$. From $\sigma(\boldsymbol{y}) = \boldsymbol{z}$ it follows that $\sigma(Y) = Z$. This proves that $\Omega(V)$ is doubly transitive on $S_1(V)$.*

Remark 11.6 *It follows from Corollary (11.12), if* $n \geq 3$ *and the Witt index of* (V, ϕ) *is one, then for any pair of non-orthogonal singular vectors,* $(\boldsymbol{u}, \boldsymbol{v})$, $\Omega(V)$ *is generated by* $T_{\boldsymbol{u}} \cup T_{\boldsymbol{v}}$.

The next result will assist us in proving that $\Omega(V)$ is transitive and primitive on $S_1(V)$.

Theorem 11.13 *Assume the Witt index of* (V, ϕ) *is at least two. Then the following hold:*

i) If $X, Y \in S_1(V)$ *and* $X \perp Y$*, then there exists* $Z \in \Gamma(X) \cap \Gamma(Y)$.

ii) If $X, Y \in S_1(V)$ *and* $X \perp Y$*, then there exists* $Z \in \Delta(X) \cap \Gamma(Y)$.

iii) If $X, Y \in S_1(V)$ *and* $X \not\perp Y$*, then there exists* $Z \in \Gamma(X) \cap \Gamma(Y)$.

iv) If $X \in S_1(V), Y \not\perp X$*, then there exists* $Z \in \Delta(X) \cap \Gamma(Y)$.

Proof *i) Let* $\boldsymbol{x} \in X, \boldsymbol{y} \in Y$ *be non-zero vectors. By the proof of Lemma (8.28) there exists singular vectors* $\boldsymbol{x}', \boldsymbol{y}'$ *such that* $\langle \boldsymbol{x}, \boldsymbol{y}' \rangle = \langle \boldsymbol{y}, \boldsymbol{x}' \rangle = \langle \boldsymbol{x}', \boldsymbol{y}' \rangle = 0, \langle \boldsymbol{x}, \boldsymbol{x}' \rangle = \langle \boldsymbol{y}, \boldsymbol{y}' \rangle = 1$. *Set* $Z = Span(\boldsymbol{x}' + \boldsymbol{y}')$. *Then* $Z \in \Gamma(X) \cap \Gamma(Y)$*, as required.*

ii) If $\boldsymbol{x}, \boldsymbol{x}'\boldsymbol{y}, \boldsymbol{y}'$ *are as in part i) set* $Z = Span(\boldsymbol{x}') \in \Delta(Y) \cap \Gamma(X)$.

iii) Let $\boldsymbol{x} \in X, \boldsymbol{y} \in Y$ *be non-zero vectors. Since the Witt index is at least two,* $X^{\perp} \cap Y^{\perp}$ *is a non-degenerate, singular subspace. Let* $\boldsymbol{u}$ *be a singular vector in* $X^{\perp} \cap Y^{\perp}$. *Set* $\boldsymbol{w} = \boldsymbol{x} + \boldsymbol{u}$. *Then* $\boldsymbol{x} \perp \boldsymbol{w} \not\perp \boldsymbol{y}$. *By part ii) there exists a singular vector* $\boldsymbol{v}$ *such that* $\boldsymbol{x} \not\perp \boldsymbol{v} \perp \boldsymbol{w}$. *Replacing* $\boldsymbol{v}$ *by a vector in* $Span(\boldsymbol{w}, \boldsymbol{v}) \cap \boldsymbol{y}^{\perp}$ *we can assume that* $\boldsymbol{v} \perp \boldsymbol{y}$. *Set* $Z = Span(\boldsymbol{w} + \boldsymbol{v})$. *Then* $Z \in \Gamma(X) \cap \Gamma(Y)$.

iv) Let $\boldsymbol{x} \in X, \boldsymbol{y} \in Y$ *non-zero vectors. Let* $\boldsymbol{u}$ *be a singular vector in* $\boldsymbol{x}^{\perp} \cap \boldsymbol{y}^{\perp}$ *and set* $Z = Span(\boldsymbol{u} + \boldsymbol{y})$. *Then* $Z \in \Delta(Y) \cap \Gamma(X)$.

Lemma 11.29 *Let* $(\boldsymbol{x}, \boldsymbol{w})$ *be a hyperbolic pair,* $\boldsymbol{y} \in \boldsymbol{x}^{\perp} \cap \boldsymbol{w}^{\perp}$*, a singular vector, and* $b \in \mathbb{F}$. *Then there exists* $\tau \in T_{\boldsymbol{x}}$ *such that* $\tau(\boldsymbol{y}) = b\boldsymbol{x} + \boldsymbol{y}$.

Proof *Let* $\boldsymbol{u} \in \boldsymbol{x}^{\perp} \cap \boldsymbol{w}^{\perp}$ *such that* $\langle \boldsymbol{y}, \boldsymbol{u} \rangle = 1$. *Then* $\tau_{\boldsymbol{x}, b\boldsymbol{u}}(\boldsymbol{y}) = \boldsymbol{y} + \langle \boldsymbol{y}, b\boldsymbol{u} \rangle \boldsymbol{x} = \boldsymbol{y} + b\boldsymbol{x}$.

Lemma 11.30 *Assume* $n \geq 3$. *Then* $\Omega(V)$ *is transitive on* $S_1(V)$.

Proof *Let $X, Y \in S_1(V)$. Suppose $X \perp Y$. By part i) of Theorem (11.13) there exists $Z \in \Gamma(X) \cap \Gamma(Y)$. Let $\boldsymbol{z} \in Z$. Choose $\boldsymbol{x} \in X, \boldsymbol{y} \in Y$ such that $\langle \boldsymbol{z}, \boldsymbol{x} \rangle = \langle \boldsymbol{z}, \boldsymbol{y} \rangle = 1$. By Lemma (11.28) there exists $\tau \in T_{\boldsymbol{z}}$ such that $\tau(\boldsymbol{x}) = \boldsymbol{y}$. It follows that $\tau(X) = Y$. Now assume that $X \not\perp Y$. By part 3) of Theorem (11.13) there exists $Z \in \Gamma(X) \cap \Gamma(Y)$ and the proof proceeds in exactly the same as when $X \perp Y$. Thus, $\Omega(V)$ is transitive on $S_1(V)$.*

Theorem 11.14 *Assume the Witt index is at least two and that $n = dim(V) > 4$. Then $\Omega(V)$ is primitive on $S_1(V)$.*

Proof *We first show that if $X \in S_1(V)$ and $Y, Z \in \Delta(X)$, then there is a $\tau \in \Omega(V)$ such that $\tau(X) = X$ and $\tau(Y) = Z$. Choose $\boldsymbol{x} \in X$ and let $\boldsymbol{w}$ be a singular vector such that $\langle \boldsymbol{w}, \boldsymbol{x} \rangle = 1$. Let $\boldsymbol{y'} \in (X+Y) \cap \boldsymbol{w}^\perp$, $\boldsymbol{z'} \in (X+Z) \cap \boldsymbol{w}^\perp$, and set $Y' = Span(\boldsymbol{y'}), Z' = Span(\boldsymbol{z'})$. Then $Y', Z' \in S_1(\boldsymbol{x}^\perp \cap \boldsymbol{w}^\perp)$. The space $\boldsymbol{x}^\perp \cap \boldsymbol{w}^\perp$ is non-degenerate, singular, and $dim(\boldsymbol{x}^\perp \cap \boldsymbol{w}^\perp) \geq 3$. By Lemma (11.30) there is a $\sigma \in \Omega(\boldsymbol{x}^\perp \cap \boldsymbol{w}^\perp)$ such that $\sigma(Y') = Z'$. Extend σ to an isometry $\widehat{\sigma}$ of V so that $\widehat{\sigma}$ restricted to $Span(\boldsymbol{x}, \boldsymbol{w})$ is the identity. Then $\widehat{\sigma} \in \Omega(V), \widehat{\sigma}(X) = X$ and $\widehat{\sigma}(Y') = Z'$. By Lemma (11.29) there exists δ and γ in $T_{\boldsymbol{x}}$ such that $\delta(Y) = Y'$ and $\gamma(Z') = Z$. Set $\tau = \gamma\widehat{\sigma}\delta$. Then $\tau(X) = X$ and $\tau(Y) = \gamma\widehat{\sigma}\delta(Y) = \gamma\widehat{\sigma}(Y') = \gamma(Z') = Z$.*

Now assume that B is a subset of $S_1(V)$ with at least two elements and for any $\sigma \in \Omega(V)$ either $\sigma(B) = B$ or $\sigma(B) \cap B = \emptyset$. We prove that $V = S_1(V)$ from which it will follow that $\Omega(V)$ is primitive on $S_1(V)$. Let $X, Y \in B$. Suppose $Y \in \Delta(X)$. We claim that $\Delta(X)$ is contained in B. Let $Z \in \Delta(X)$. By what we have shown, there is a $\tau \in \Omega(V)$ such that $\tau(X) = X, \tau(Y) = Z$. Since $X \in B \cap \tau(B)$ it must be the case that $\tau(B) = B$. It then follows that $Z = \tau(Y) \in \tau(B) = B$ and our claim is proved. In a similar way, if $Y \in \Gamma(X)$ then $\Gamma(X) \subset B$. We return to the assumption that $Y \in \Delta(X)$. By switching the roles of X and Y we can also conclude that $\Delta(Y)$ is contained in B. By part ii) of Lemma (11.13) there is a $Z \in \Delta(Y) \cap \Gamma(X)$. But then, as argued above, $\Gamma(X) \subset B$, so that B contains $\{X\} \cup \Delta(X) \cup \Gamma(X) = S_1(V)$.

So we may assume that $Y \in \Gamma(X)$ and $\Gamma(X) \subset B$ and $\Gamma(Y) \subset B$. By part iv) of Theorem (11.13) there is a $Z \in \Delta(X) \cap \Gamma(Y)$. Then $Z \in B$, whence $\Delta(X)$ and we again have $B = S_1(V)$.

Remark 11.7 *The case when $dim(V) = 4$ and the Witt index is two is really an exception. Let $(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{y}_1, \boldsymbol{y}_2)$ be a hyperbolic basis. Let L_1 be the subgroup generated by $\tau_{\boldsymbol{x}_1, a\boldsymbol{y}_2}$ and $\tau_{\boldsymbol{x}_2, b\boldsymbol{y}_1}$ for a, b ranging over $\mathbb{F}$. Then L_1 is isomorphic to $SL_2(\mathbb{F})$. Let L_2 be the subgroup generated by $\tau_{\boldsymbol{y}_2, a\boldsymbol{y}_1}, \tau_{\boldsymbol{x}_1, b\boldsymbol{x}_2}$ where a, b range over $\mathbb{F}$. Then also L_2 is isomorphic to $SL_2(\mathbb{F})$. L_1 and L_2 commute and intersect in the center of $O(V, \phi)$. Moreover, $\Omega(V) = L_1 L_2$. The set $B = S_1(Span(\boldsymbol{x}_1, \boldsymbol{x}_2))$ is a block of imprimitivity of $S_1(V)$.*

In our next result we investigate the subgroup consisting of those isometries S which commute with every element of $\Omega(V)$. Subsequently we show that this is the kernel of the action on $S_1(V)$.

Theorem 11.15 *Assume dim*$(V) \geq 3$. *If* $S \in O(V,\phi)$ *commutes with every* $\tau \in \Omega(V)$, *then* $S = \pm I_V$. *In particular,* $Z(O(V,\phi)) = \{-I_V, I_V\}$.

Proof *Let* $\boldsymbol{u}$ *be a singular vector and* $\boldsymbol{v}$ *a non-singular vector in* $\boldsymbol{u}^\perp$. *Since* S *commutes with* $\tau_{\boldsymbol{u},\boldsymbol{v}}$, S *leaves invariant Range*$(\tau_{\boldsymbol{u},\boldsymbol{v}} - I_V) =$ *Span*$(\boldsymbol{u},\boldsymbol{v})$. *Then* S *also leaves invariant Rad*$($*Span*$(\boldsymbol{u},\boldsymbol{v})) =$ *Span*$(\boldsymbol{u})$. *Consequently, for each singular vector* $\boldsymbol{u}$ *there is a scalar* $\lambda_{\boldsymbol{u}}$ *such that* $S(\boldsymbol{u}) = \lambda_{\boldsymbol{u}}\boldsymbol{u}$. *We claim that* $\lambda_{\boldsymbol{u}}$ *is independent of* $\boldsymbol{u}$.

Suppose $\boldsymbol{u},\boldsymbol{v}$ *are singular,* $(\boldsymbol{u},\boldsymbol{v})$ *is linearly independent, and* $\boldsymbol{u} \perp \boldsymbol{v}$. *Then* $\boldsymbol{u}+\boldsymbol{v}$ *is a singular vector and we have* $\lambda_{\boldsymbol{u}+\boldsymbol{v}}(\boldsymbol{u}+\boldsymbol{v}) = S(\boldsymbol{u}+\boldsymbol{v}) = S(\boldsymbol{u}) + S(\boldsymbol{v}) = \lambda_{\boldsymbol{u}}\boldsymbol{u} + \lambda_{\boldsymbol{v}}\boldsymbol{v}$ *and we conclude that* $\lambda_{\boldsymbol{u}} = \lambda_{\boldsymbol{u}+\boldsymbol{v}} = \lambda_{\boldsymbol{v}}$. *We may therefore assume that* $\langle \boldsymbol{u},\boldsymbol{v}\rangle \neq 0$. *Since* S *is an isometry,* $\lambda_{\boldsymbol{u}}\lambda_{\boldsymbol{v}}\langle \boldsymbol{u},\boldsymbol{v}\rangle = \langle \lambda_{\boldsymbol{u}}\boldsymbol{u}, \lambda_{\boldsymbol{v}}\boldsymbol{v}\rangle = \langle S(\boldsymbol{u}), S(\boldsymbol{v})\rangle = \langle \boldsymbol{u},\boldsymbol{v}\rangle$. *Therefore* $\lambda_{\boldsymbol{v}} = \frac{1}{\lambda_{\boldsymbol{u}}}$. *Assume now that* U *is a non-degenerate subspace of* V *containing Span*$(\boldsymbol{u},\boldsymbol{v})$ *with dim*$(U) = 3$. *Let* $\boldsymbol{w}$ *be a singular vector of* U *such that* $(\boldsymbol{u},\boldsymbol{v},\boldsymbol{w})$ *is linearly independent. Then* $\frac{1}{\lambda_{\boldsymbol{u}}} = \lambda_{\boldsymbol{w}} = \frac{1}{\lambda_{\boldsymbol{v}}}$ *so that* $\lambda_{\boldsymbol{u}} = \lambda_{\boldsymbol{v}}$. *Switching the roles of* $\boldsymbol{u}$ *and* $\boldsymbol{w}$ *we also get* $\frac{1}{\lambda_{\boldsymbol{w}}} = \lambda_{\boldsymbol{u}} = \frac{1}{\lambda_{\boldsymbol{v}}}$. *It then follows that* $\lambda_{\boldsymbol{u}} = \lambda_{\boldsymbol{w}} = \lambda_{\boldsymbol{v}}$. *Set* $\lambda = \lambda_{\boldsymbol{u}}$. *Since* $\lambda = \frac{1}{\lambda}$ *it follows that* $\lambda \in \{-1, 1\}$.

As a corollary of the proof of Theorem (11.15) we have:

Corollary 11.13 *The kernel of the action of* $O(V,\phi)$ *on* $S_1(V)$ *is* $Z(O(V,\phi))$.

Theorem 11.16 *Let* $n \geq 3$. *Then the commutator subgroup of* $O(V,\phi)$ *is equal to the commutator subgroup of* $SO(V,\phi)$.

Proof *As we have done previously, if* G *is a group, we will denote by* G' *the commutator group of* G, *the subgroup of* G *generated by all commutators* $[g,h] = g^{-1}h^{-1}gh$. *Since* $SO(V,\phi)$ *is a subgroup of* $O(V,\phi)$, *it follows that* $SO(V,\phi)'$ *is contained in* $O(V,\phi)'$ *so we must prove that* $O(V,\phi)'$ *is a subgroup of* $SO(V,\phi)$. *Since* $O(V,\phi)$ *is generated by all reflections* $\rho_{\boldsymbol{x}}$ *where* $\boldsymbol{x}$ *is non-singular, it follows that* $O(V,\phi)'$ *is generated by all commutators* $[\rho_{\boldsymbol{x}}, \rho_{\boldsymbol{y}}] = \rho_{\boldsymbol{x}}^{-1}\rho_{\boldsymbol{y}}^{-1}\rho_{\boldsymbol{x}}\rho_{\boldsymbol{y}} = \rho_{\boldsymbol{x}}\rho_{\boldsymbol{y}}\rho_{\boldsymbol{x}}\rho_{\boldsymbol{y}}$ *since reflections have order two. Suppose first that* n *is odd. Then* $-I_V \notin SO(V,\phi)$ *but* $-\rho_{\boldsymbol{x}}, -\rho_{\boldsymbol{y}} \in SO(V,\phi)$ *and then* $[-\rho_{\boldsymbol{x}}, -\rho_{\boldsymbol{y}}] = [\rho_{\boldsymbol{x}}, \rho_{\boldsymbol{y}}] \in SO(V,\phi)$.

We may therefore assume that n *is even and* $n \geq 4$. *Suppose there exists a* *non-singular vector* $\boldsymbol{z} \in \boldsymbol{x}^{\perp} \cap \boldsymbol{y}^{\perp}$. *In this case,* $\rho_{\boldsymbol{x}}\rho_{\boldsymbol{z}}$ *and* $\rho_{\boldsymbol{y}}\rho_{\boldsymbol{z}}$ *are in* $SO(V, \phi)$ *and* $[\rho_{\boldsymbol{x}}, \rho_{\boldsymbol{y}}] = [\rho_{\boldsymbol{x}}\rho_{\boldsymbol{z}}, \rho_{\boldsymbol{y}}\rho_{\boldsymbol{z}}] \in SO(V, \phi)'$. *In the contrary case,* $n = 4$ *and* $X = Span(\boldsymbol{x}, \boldsymbol{y})$ *is degenerate with a radical of dimension one. In particular,* X *contains singular vectors. Let* U *be a three-dimensional non-degenerate subspace of* V *with* $X \subset U$ *and set* $W = U^{\perp}$. *Let* τ *be the isometry such that* τ *restricted to* U *is* $-I_U$ *and restricted to* W *is* I_W. *Then* $\tau \in O(V, \phi)$ *and* $\tau \notin SO(V, \phi)$ *and commutes with* $\rho_{\boldsymbol{x}}$ *and* $\rho_{\boldsymbol{y}}$. *Both* $\rho_{\boldsymbol{x}}\tau$ *and* $\rho_{\boldsymbol{y}}\tau \in SO(V, \phi)$ *so that* $[\rho_{\boldsymbol{x}}, \rho_{\boldsymbol{y}}] = [\rho_{\boldsymbol{x}}\tau, \rho_{\boldsymbol{y}}\tau] \in SO(V, \phi)'$ *and we have the desired equality.*

Let $(\boldsymbol{u}, \boldsymbol{v})$ be a hyperbolic pair and set $U = Span(\boldsymbol{u}, \boldsymbol{v})$ and $W = U^{\perp}$. Denote by $O(U)$ the collection of those isometries T such that $T(U) = U$ and $T_{|W} = I_W$. We claim for any $\sigma \in O(V, \phi)$ there exists $\gamma \in O(U)$ and $\tau \in \Omega(V)$ such that $\sigma = \tau\gamma$. Note that since $\Omega(V)$ is normal in $O(V, \phi)$ it suffices to prove this for a generating set of $O(V, \phi)$, in particular, for reflections. Toward that end let $\boldsymbol{x}$ be a non-singular vector and set $a = \phi(\boldsymbol{x})$. Let $\boldsymbol{y} = a\boldsymbol{u} + \boldsymbol{v}$ so that $\phi(\boldsymbol{y}) = a = \phi(\boldsymbol{x})$. By Witt's theorem (8.12) there is an isometry δ such that $\delta(\boldsymbol{y}) = \boldsymbol{x}$. Set $\boldsymbol{u}' = \delta(\boldsymbol{u})$ and $\boldsymbol{v}' = \delta(\boldsymbol{v})$, so that $(\boldsymbol{u}', \boldsymbol{v}')$ is a hyperbolic pair. By Lemma (11.30) and Lemma (11.28) there is a $\beta \in \Omega(V)$ such that $\beta(\boldsymbol{u}') \in Span(\boldsymbol{u})$ and $\beta(\boldsymbol{v}') \in Span(\boldsymbol{v})$. Then $\boldsymbol{z} = \beta(\boldsymbol{x}) \in U$. It then follows that $\beta\rho_{\boldsymbol{x}}\beta^{-1} = \rho_{\boldsymbol{z}}$ so that $\rho_{\boldsymbol{x}} = \beta^{-1}\rho_{\boldsymbol{z}}\beta$. Then $\rho_{\boldsymbol{x}} = \beta^{-1}\rho_{\boldsymbol{z}}\beta\rho_{\boldsymbol{z}}\rho_{\boldsymbol{z}} = [\beta^{-1}, \rho_{\boldsymbol{z}}]\rho_{\boldsymbol{z}}$. Set $\tau = [\beta^{-1}, \rho_{\boldsymbol{z}}]$. Since $\Omega(V)$ is normal in $O(V, \phi), \tau \in \Omega(V)$. Thus, $\rho_{\boldsymbol{x}} = \tau\rho_{\boldsymbol{z}}$ as desired. We have therefore proved most of following:

Lemma 11.31 *Let* $(\boldsymbol{u}, \boldsymbol{v})$ *be a hyperbolic pair and set* $U = Span(\boldsymbol{u}, \boldsymbol{v})$ *and* $W = U^{\perp}$. *Denote by* $O(U)$ *the collection of those isometries* T *such that* $T(U) = U$ *and* $T_{|W} = I_W$. *Then* $O(V, \phi) = \Omega(V)O(U)$ *and* $SO(V, \phi) = \Omega(V)[SO(V, \phi) \cap O(U)]$.

Proof *The only thing that requires any further explanation is the last statement. Suppose* $T \in SO(V, \phi)$. *Then there are* $\tau \in \Omega(V)$ *and* $\gamma \in O(U)$ *such that* $T = \tau\gamma$. *By Lemma (11.24),* $\tau \in SO(V, \phi)$ *from which it follows that* $\gamma \in SO(V, \phi)$.

With this result we can now state precisely what the commutator subgroup of $O(V, \phi)$ is:

Theorem 11.17 *Assume* $n \geq 3$. *Then the commutator subgroup of* $O(V, \phi)$ *is equal to* $\Omega(V)$.

Proof *We first prove that* $\Omega(V) \subseteq O(V, \phi)'$. *It suffices to prove that for each pair* $(\boldsymbol{u}, \boldsymbol{v})$ *where* $\boldsymbol{u}$ *is a singular vector and* $\boldsymbol{v} \in \boldsymbol{u}^{\perp}$ *is non-singular, that* $\tau = \tau_{\boldsymbol{u},\boldsymbol{v}} \in O(V, \phi)'$, *equivalently, that* $\tau[O'(V, \phi)] =$

$O(V,\phi)'$, the identity element of the quotient group $O(V,\phi)/O(V,\phi)'$. Let $\gamma = \tau_{\boldsymbol{u},\frac{1}{2}\boldsymbol{v}}$ so that $\gamma^2 = \tau_{\boldsymbol{u},\boldsymbol{v}}$. By the Cartan-Dieudonne theorem we can express γ as a product of reflections: $\gamma = \rho_{\boldsymbol{x}_1} \dots \rho_{\boldsymbol{x}_t}$. Now $\tau[O(V,\phi)'] = \gamma^2[O(V,\phi)'] = (\rho_{\boldsymbol{x}_1} \dots \rho_{\boldsymbol{x}_t})(\rho_{\boldsymbol{x}_1} \dots \rho_{\boldsymbol{x}_t})[O(V,\phi)']$. However, the quotient group $O(V,\phi)/O(V,\phi)'$ is Abelian. Therefore

$$(\rho_{\boldsymbol{x}_1} \cdots \rho_{\boldsymbol{x}_t})(\rho_{\boldsymbol{x}_1} \cdots \rho_{\boldsymbol{x}_t})[O(V,\phi)'] = \rho^2_{\boldsymbol{x}_1} \cdots \rho^2_{\boldsymbol{x}_t}[O(V,\phi)'] = O(V,\phi)'.$$

It remains to show that $O(V,\phi)' \subseteq \Omega(V)$. Let $(\boldsymbol{u},\boldsymbol{v})$ be a hyperbolic pair, and set

$$U = Span(\boldsymbol{u},\boldsymbol{v}), W = U^{\perp}, \text{ and } O(U) = \{T \in O(V,\phi)|\ T(U) = U, T_{|W} = I_W\}.$$

By Lemma (11.31), $SO(V,\phi) = \Omega(V)[O(U) \cap SO(V,\phi)]$. Then $SO(V,\phi)/\Omega(V)$ is isomorphic to $[O(U) \cap SO(V,\phi)]/[O(U) \cap \Omega(V)]$. However, $O(U) \cap SO(V,\phi)$ is isomorphic to $SO(U)$ which is an Abelian group (isomorphic to the multiplicative group of $\mathbb{F}$) and therefore the quotient group $[O(U) \cap SO(V,\phi)]/[O(U) \cap \Omega(V)]$ is Abelian. Thus, $SO(V,\phi)/\Omega(V)$ is Abelian which implies that $O(V,\phi)' = SO(V,\phi)' \subseteq \Omega(V)$ and we have equality.

In our next result we assume (V,ϕ) is a non-degenerate singular orthogonal space of dimension three over the field $\mathbb{F}$ (characteristic not two) and determine $\Omega(V)$.

Theorem 11.18 *Assume (V,ϕ) is a non-degenerate singular orthogonal space of dimension three over the field $\mathbb{F}$ and that the characteristic of $\mathbb{F}$ is not two. Then $\Omega(V)$ is isomorphic to $PSL_2(\mathbb{F})$.*

Proof *Let $(\boldsymbol{u},\boldsymbol{v})$ be a hyperbolic pair and let $\boldsymbol{z} \in \boldsymbol{u}^{\perp} \cap \boldsymbol{v}^{\perp}$. Set $\phi(\boldsymbol{z}) = c$. If we set $\phi' = \frac{1}{c}\phi$ then $O(V,\phi') = O(V,\phi)$ so we can, without loss of generality assume that $\phi(\boldsymbol{z}) = 1$. Note that $\Omega(V)$ is generated by $\tau_{\boldsymbol{u},a\boldsymbol{z}}, \tau_{\boldsymbol{v},b\boldsymbol{z}}$ where $a,b \in \mathbb{F}$. Because we will need it below we compute the matrix of $\tau_{\boldsymbol{u},a\boldsymbol{z}}$ and $\tau_{\boldsymbol{v},b\boldsymbol{z}}$ with respect to the basis $(\boldsymbol{u},\boldsymbol{z},\boldsymbol{v})$. Clearly, $\tau_{\boldsymbol{u},a\boldsymbol{z}}(\boldsymbol{u}) = \boldsymbol{u}$. We use the formula for computing $\tau_{\boldsymbol{u},a\boldsymbol{z}}(\boldsymbol{z})$:*

$$\tau_{\boldsymbol{u},a\boldsymbol{z}}(\boldsymbol{z}) = \boldsymbol{z} + \langle \boldsymbol{z}, a\boldsymbol{z}\rangle \boldsymbol{u} = \boldsymbol{z} + 2a\boldsymbol{u}.$$

It then follows from the proof of Theorem (11.12) that $\tau_{\boldsymbol{u},a\boldsymbol{z}}(\boldsymbol{v}) = \boldsymbol{v} - a\boldsymbol{z} - a^2\boldsymbol{u}$. Thus, the matrix of $\tau_{\boldsymbol{u},a\boldsymbol{z}}$ with respect to $(\boldsymbol{u},\boldsymbol{z},\boldsymbol{v})$ is $\begin{pmatrix} 1 & 2a & -a^2 \\ 0 & 1 & -a \\ 0 & 0 & 1 \end{pmatrix}$. Similarly, the matrix of $\tau_{\boldsymbol{v},b\boldsymbol{z}}$ with respect to the basis $(\boldsymbol{u},\boldsymbol{z},\boldsymbol{v})$ is $\begin{pmatrix} 1 & 0 & 0 \\ 2b & 1 & 0 \\ -b^2 & -b & 1 \end{pmatrix}$.

Now let X be a two-dimensional vector space over $\mathbb{F}$ with basis $(\boldsymbol{x}, \boldsymbol{y})$ and set $Y = Sym_2(X)$, the second symmetric power of X, which has basis $(\boldsymbol{x}^2, \boldsymbol{xy}, \boldsymbol{y}^2)$. Define $q : Y \to \mathbb{F}$ by $q(a\boldsymbol{x}^2 + b\boldsymbol{xy} + c\boldsymbol{y}^2) = b^2 - 4ac$. Set $\boldsymbol{u}' = \frac{1}{2}\boldsymbol{x}^2, \boldsymbol{z}' = \boldsymbol{xy}$, and $\boldsymbol{v}' = -\frac{1}{2}\boldsymbol{y}^2$. Then $(\boldsymbol{u}', \boldsymbol{v}')$ is a hyperbolic pair, $\boldsymbol{z}' \in (\boldsymbol{x}')^\perp \cap (\boldsymbol{y}')^\perp$, and $q(\boldsymbol{z}') = 1$. Consequently, the linear transformation that sends $(\boldsymbol{u}', \boldsymbol{z}', \boldsymbol{v}')$ to $(\boldsymbol{u}, \boldsymbol{z}, \boldsymbol{v})$ is an isometry.

For every operator $\sigma : X \to X$ there is an induced operator, $S_2(\sigma) : Sym_2(X) \to Sym_2(X)$. Moreover, the map S_2 is multiplicative: For $\sigma, \delta \in \mathcal{L}(X, X), S_2(\sigma\delta) = S_2(\sigma)S_2(\delta)$. Furthermore, if σ is invertible then so is $S_2(\sigma)$. Therefore S_2 restricted to $GL(X)$ is a group homomorphism to $GL(Sym_2(X)) = GL(Y)$.

We describe the map more explicitly: Suppose $\sigma(\boldsymbol{x}) = a\boldsymbol{x} + b\boldsymbol{y}$ and $\sigma(\boldsymbol{y}) = c\boldsymbol{x} + d\boldsymbol{y}$. Then

$$S_2(\sigma)(\boldsymbol{x}^2) = a^2\boldsymbol{x}^2 + 2ab\boldsymbol{xy} + b^2\boldsymbol{y}^2$$

$$S_2(\sigma)(\boldsymbol{xy}) = ac\boldsymbol{x}^2 + (ad + bc)\boldsymbol{xy} + bd\boldsymbol{y}^2$$

$$S_2(\sigma)(\boldsymbol{y}^2) = c^2\boldsymbol{x}^2 + 2cd\boldsymbol{xy} + d^2\boldsymbol{y}^2.$$

Let $\tau_{\boldsymbol{x},a}$ be the operator on X such that $\tau_{\boldsymbol{x},a} = \boldsymbol{x}$ and $\tau_{\boldsymbol{x},a}(\boldsymbol{y}) = a\boldsymbol{x} + \boldsymbol{y}$. Set $\sigma_a = S_2(\tau_{\boldsymbol{x},a})$. Then $\sigma_a(\boldsymbol{x}^2) = \boldsymbol{x}^2, \sigma_a(\boldsymbol{xy}) = a\boldsymbol{x}^2 + \boldsymbol{xy}$, and $\sigma_a(\boldsymbol{y}^2) = a^2\boldsymbol{x}^2 + 2a\boldsymbol{xy} + \boldsymbol{y}^2$. We determine the matrix of σ_a with respect to the basis $(\boldsymbol{u}', \boldsymbol{z}', \boldsymbol{v}')$.

$$\sigma_a(\boldsymbol{u}') = \sigma_a(\frac{1}{2}\boldsymbol{x}^2) = \frac{1}{2}\boldsymbol{x}^2 = \boldsymbol{u}'$$

$$\sigma_a(\boldsymbol{z}') = \sigma_a(\boldsymbol{xy}) = a\boldsymbol{x}^2 + \boldsymbol{xy} = 2a\boldsymbol{u}' + \boldsymbol{z}'$$

$$\sigma_a(\boldsymbol{v}') = \sigma_a(-\frac{1}{2}\boldsymbol{y}^2) = -\frac{1}{2}(a^2\boldsymbol{x}^2 + 2a\boldsymbol{xy} + \boldsymbol{y}^2) =$$

$$-\frac{1}{2}a^2\boldsymbol{x}^2 - a\boldsymbol{xy} - \frac{1}{2}\boldsymbol{y}^2 = -a^2\boldsymbol{u}' - a\boldsymbol{z}' + \boldsymbol{v}'$$

Consequently, the matrix of σ_a with respect to $(\boldsymbol{u}', \boldsymbol{z}', \boldsymbol{v}')$ is $\begin{pmatrix} 1 & 2a & -a^2 \\ 0 & 1 & -a \\ 0 & 0 & 1 \end{pmatrix}$. Note that this is the same as the matrix of $\tau_{\boldsymbol{u},\boldsymbol{z}}$ with respect to $(\boldsymbol{u}, \boldsymbol{z}, \boldsymbol{v})$. Therefore, σ_a is an isometry and, in fact, $\sigma_a = \tau_{\boldsymbol{u}',a\boldsymbol{z}'}$. A similar calculation shows that if $\tau_{\boldsymbol{y},b}$ is the operator of X such the $\tau_{\boldsymbol{y},b}(\boldsymbol{x}) = \boldsymbol{x} + b\boldsymbol{y}$ and $\tau_{\boldsymbol{y},b}(\boldsymbol{y}) = \boldsymbol{y}$, then $\sigma_b = S_2(\tau_{\boldsymbol{y},b}) = \tau_{\boldsymbol{v}',b\boldsymbol{z}}$. This shows that $\Omega(V)$ is isomorphic to the image of $SL_2(\mathbb{F})$ under the homomorphism $S_2 : SL(X) \to SL(Y) = SL(Sym_2(X))$.

Note that the kernel of this map is $\{I_X, -I_X\} = Z(SL(X))$ *and so the image is* $PSL(X)$ *which is isomorphic to* $PSL_2(\mathbb{F})$.

As a consequence of Theorem (11.18), we have the following result:

Theorem 11.19 *Assume* (V, ϕ) *is a non-degenerate, singular orthogonal space of dimension three over the field* $\mathbb{F}$*, the characteristic of* $\mathbb{F}$ *is not two, and* $\mathbb{F} \neq \mathbb{F}_3$*. Then* $\Omega(V)$ *is a non-Abelian simple group.*

We make use of Theorem (11.18) in proving the following result:

Theorem 11.20 *Assume* (V, ϕ) *is a non-degenerate orthogonal space of dimension* $n \geq 3$ *over the field* $\mathbb{F}$ *and that the Witt index of* (V, ϕ) *is positive. If* $\mathbb{F} \neq \mathbb{F}_3$ *then* $\Omega(V)$ *is perfect.*

Proof *Let* $\boldsymbol{u}$ *be a singular vector and* $\boldsymbol{z}$ *a non-singular vector in* $\boldsymbol{u}^{\perp}$*. We will show that* $\tau_{\boldsymbol{u},\boldsymbol{z}} \in \Omega(V)'$*, the commutator subgroup of* $\Omega(V)$*. Since any singular vector in* $\boldsymbol{u}^{\perp}$ *can be expressed as the sum of two non-singular vectors in* $\boldsymbol{u}^{\perp}$*, it will follow that* $T_{\boldsymbol{u}}$ *is contained in* $\Omega(V)'$*. Since* $\boldsymbol{u}$ *is arbitrary, we can conclude that* $T_{\boldsymbol{u}}$ *is contained in* $\Omega(V)'$ *for every singular vector* $\boldsymbol{u}$ *and consequently* $\Omega(V) \subseteq \Omega(V)'$*.*

Let $\boldsymbol{v}$ *be a singular vector in* $\boldsymbol{z}^{\perp}$ *such that* $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = 1$ *and set* $U = Span(\boldsymbol{u}, \boldsymbol{z}, \boldsymbol{v})$*, a non-degenerate subspace of* V *of dimension three and Witt index one. Let* $\Omega(U)$ *be the subgroup of* Ω *generated by* $T_{\boldsymbol{x}}$ *such that* $Span(\boldsymbol{x}) \in S_1(U)$*. By Theorem (11.19),* $\Omega(U)$ *is isomorphic to* $PSL_2(\mathbb{F})$ *and is simple. In particular,* $\tau_{\boldsymbol{u},\boldsymbol{z}}$ *is in* $\Omega(U)' \subseteq \Omega(V)'$*.*

We now turn our attention to orthogonal spaces over the field $\mathbb{F}_3$. We remark that since $\mathbb{F}_3$ is a finite field, if (V, ϕ) has dimension n then the Witt index is at least $\lfloor \frac{n-1}{2} \rfloor$. In particular, if $n \geq 5$, then the Witt index is at least two.

Lemma 11.32 *Assume* (V, ϕ) *is a non-degenerate orthogonal space over* $\mathbb{F}_3$ *of dimension four with Witt index 1. Then* $\Omega(V)$ *is isomorphic to* $PSL_2(\mathbb{F}_9)$*. In particular,* $\Omega(V)$ *is simple and, therefore, perfect.*

Proof *Let* M *be the subset of* $M_{22}(\mathbb{F}_9)$ *consisting of those matrices* m *such that* $\overline{m}^{tr} = m$*. Here, by* $\overline{m}$ *we mean the matrix obtained from* m *by applying the automorphism of* $\mathbb{F}_9$ *given by* $a = \overline{a} = a^3$ *to each entry of the matrix. Such a matrix has the form* $\begin{pmatrix} a & \alpha \\ \overline{\alpha} & b \end{pmatrix}$ *where* $a, b \in \mathbb{F}_3$ *and* $\alpha \in \mathbb{F}_9$*. As a vector space over* $\mathbb{F}_3$ *it has dimension four.*

For $m \in M$ *set* $q(m) = det(m) = ab - \alpha\overline{\alpha} \in \mathbb{F}_3$. *Then* q *is a non-degenerate quadratic form with Witt index one. We define an action of* $SL_2(\mathbb{F}_9)$ *as follows: For* $A \in SL_2(\mathbb{F}_9)$ *and* $m \in M$ *set* $A \cdot m = \overline{A}^{tr} mA$. *Then*

$$\begin{aligned}
\overline{A \cdot m}^{tr} &= \overline{\overline{A}^{tr} mA}^{tr} \\
&= A^{tr}\overline{m}\overline{A})^{tr} \\
&= \overline{A}^{tr}\overline{m}^{tr}A \\
&= \overline{A}^{tr}mA \\
&= A \cdot m.
\end{aligned}$$

Thus, $A \cdot m \in M$. *This is clearly a linear action and* $(AB) \cdot m = A \cdot (B \cdot m)$. *Thus we have a group homomorphism from* $SL_2(\mathbb{F}_9)$ *into* $GL(M)$. *We claim the image of* $A \in SL_2(\mathbb{F}_9)$ *acts as an isometry of* (M, q). *This follows since* $det(A) = det(\overline{A}^{tr}) = 1$. *So, in fact, we have a group homomorphism from* $SL_2(\mathbb{F}_9)$ *to* $O(M, q)$. *Clearly the center of* $SL_2(\mathbb{F}_9), \{-I_2, I_2\}$, *is in the kernel, and must be the kernel of the action since* $PSL_2(\mathbb{F}_9)$ *is a simple group). Because the image, isomorphic to* $PSL_2(\mathbb{F}_9)$, *is perfect it follows that the image is actually a subgroup of* $SO(M, q)$.

Set $\boldsymbol{u} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ *and* $\boldsymbol{v} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ *so that* $(\boldsymbol{u}, \boldsymbol{v})$ *is a hyperbolic pair. Note that if* $m_i = \begin{pmatrix} a_i & \alpha_i \\ \overline{\alpha_i} & b_i \end{pmatrix}$ *for* $i = 1, 2$, *then* $\langle m_1, m_2 \rangle_q = a_1b_2 + a_2b_1 - \alpha_1\overline{\alpha_2} - \alpha_2\overline{\alpha_1}$. *It then follows that* $\boldsymbol{u}^\perp \cap \boldsymbol{v}^\perp$ *consists of those matrices of the form* $\begin{pmatrix} 0 & \alpha \\ \overline{\alpha} & 0 \end{pmatrix}$ *where* $\alpha \in \mathbb{F}_9$. *For* $\alpha \in \mathbb{F}_9$, *denote by* $\boldsymbol{z}(\alpha)$ *the matrix* $\begin{pmatrix} 0 & \alpha \\ \overline{\alpha} & 0 \end{pmatrix}$.

We know from Remark (11.6) that $\Omega(M, q)$ *is generated by* $T_{\boldsymbol{u}}$ *and* $T_{\boldsymbol{v}}$. *Let* $\alpha \in \mathbb{F}_9$ *and let* $s(\alpha)$ *be the transvection* $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ *in* $SL_2(\mathbb{F}_9)$ *and by* $t(\alpha)$ *the transvection* $\begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}$. *We leave it as an exercise to show that the action on* M *induced by* $s(\alpha)$ *is the same as* $\tau_{\boldsymbol{u}, \boldsymbol{z}(\alpha)}$ *and the action induced by* $t(\alpha)$ *is the same as* $\tau_{\boldsymbol{v}, \boldsymbol{z}(\alpha)}$. *It follows from this that* $\Omega(M, q)$ *is isomorphic to* $PSL_2(\mathbb{F}_9)$.

We can now turn to the general case over the field $\mathbb{F}_3$.

Theorem 11.21 *Assume* (V, ϕ) *is a non-degenerate orthogonal space over* $\mathbb{F}_3$ *of dimension* $n \geq 5$. *Then* $\Omega(V)$ *is perfect.*

Proof *Let $\boldsymbol{u}$ be a singular vector and $\boldsymbol{z}$ a non-singular vector in $\boldsymbol{u}^{\perp}$. We will prove that $\tau_{\boldsymbol{u},\boldsymbol{z}} \in \Omega(V)'$. Since every singular vector in $\boldsymbol{u}^{\perp}$ can be expressed as the sum of two non-singular vectors from $\boldsymbol{u}^{\perp}$ it will then follow that $T_{\boldsymbol{u}}$ is contained in $\Omega(V)'$. Since $\boldsymbol{u}$ is arbitrary, we can then conclude that $\Omega(V)$ is contained in $\Omega(V)'$, hence we have equality.*

Let $\boldsymbol{v}$ be a singular vector in $\boldsymbol{z}^{\perp}$ such that $(\boldsymbol{u}, \boldsymbol{v})$ is a hyperbolic pair. Set $U = Span(\boldsymbol{u}, \boldsymbol{z}, \boldsymbol{v})$, a non-degenerate subspace of dimension three. Then $dim(U^{\perp}) \geq 2$ and $U^{\perp}$ is non-degenerate. Choose $\boldsymbol{w} \in U^{\perp}$ such that $\phi(\boldsymbol{w}) = \phi(\boldsymbol{z})$. Then $W = U + Span(\boldsymbol{w})$ is non-degenerate, dimension four, and has Witt index one. Denote by $\Omega(W)$ the subgroup of $\Omega(V)$ generated by all $\tau_{\boldsymbol{u},\boldsymbol{x}}$ and $\tau_{\boldsymbol{v},\boldsymbol{x}}$ where $\boldsymbol{x}$ is a vector in $Span(\boldsymbol{z}, \boldsymbol{w})$. By Lemma (11.32), $\Omega(W)$ is simple and isomorphic to $PSL_2(\mathbb{F}_9)$. In particular, $\tau_{\boldsymbol{u},\boldsymbol{z}}$ is contained in $\Omega(W)' \subseteq \Omega(V)'$.

We can now prove our main theorem:

Theorem 11.22 *Let $(V, \mathbb{F})$ be a non-degenerate orthogonal space of dimension $n \geq 3$ over the field $\mathbb{F}$ with Witt index $m > 0$. If $n = 3$, assume that $\mathbb{F} \neq \mathbb{F}_3$ and if $m = 2$, assume $n \geq 5$. Let $P\Omega(V)$ be the quotient of $\Omega(V)$ by $Z(\Omega(V))$. Then $P\Omega(V)$ is a simple group.*

Proof *$P\Omega(V)$ acts faithfully and primitively on $S_1(V)$. $P\Omega(V)$ is perfect. For $U = Span(\boldsymbol{u}) \in S_1(V)$ the subgroup $T_{\boldsymbol{u}}$ is Abelian and normal in $P\Omega(V)_U$, the stabilizer of U in $P\Omega(V)$. Finally, $P\Omega(V)$ is generated by the conjugates of $T_{\boldsymbol{u}}$. It follows by Iwasawa's theorem that $P\Omega(V)$ is a simple group.*

Exercises

1. Let $\boldsymbol{u}$ be a singular vector and $\boldsymbol{y}$ a non-singular vector in $\boldsymbol{u}^{\perp}$. Set $\boldsymbol{z} = \frac{\langle \boldsymbol{y}, \boldsymbol{y} \rangle_{\phi}}{2}\boldsymbol{u} + \boldsymbol{y}$. Prove that $\rho_{\boldsymbol{z}}\rho_{\boldsymbol{y}} = \tau_{\boldsymbol{u},\boldsymbol{y}}$.

2. Let $\boldsymbol{u}$ be a singular vector, $\boldsymbol{v}, \boldsymbol{w} \in \boldsymbol{u}^{\perp}$. Prove that $\tau_{\boldsymbol{u},\boldsymbol{v}} = \tau_{\boldsymbol{u},\boldsymbol{w}}$ if and only if $\boldsymbol{w} - \boldsymbol{v} \in Span(\boldsymbol{u})$. Conclude that $\tau_{\boldsymbol{u},\boldsymbol{z}} = I_V$ if and only if $\boldsymbol{z} \in Span(\boldsymbol{u})$.

3. Let $\boldsymbol{u}$ be a singular vector. Prove that $T_{\boldsymbol{u}}$ is generated by all $\tau_{\boldsymbol{u},\boldsymbol{z}}$ where $\boldsymbol{z} \in \boldsymbol{u}^{\perp}$ is non-singular.

4. Assume the Witt index of (V, ϕ) is one and that $(\boldsymbol{u}, \boldsymbol{v})$ is a hyperbolic pair. Prove that $\Omega(V)$ is generated by $T_{\boldsymbol{u}} \cup T_{\boldsymbol{v}}$.

In Exercises 5–8 assume (V, ϕ) has dimension four and Witt index two. If $l = Span(\boldsymbol{u}, \boldsymbol{v})$ is a totally singular two-dimensional space, let $\chi(l) = \{\tau_{\boldsymbol{u}',\boldsymbol{v}'} | Span(\boldsymbol{u}', \boldsymbol{v}') = Span(\boldsymbol{u}, \boldsymbol{v})\}$. Let $(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{y}_1, \boldsymbol{y}_2)$ be a basis of singular vectors such that $\langle \boldsymbol{x}_i, \boldsymbol{x}_j \rangle = \langle \boldsymbol{y}_i, \boldsymbol{y}_j \rangle = \langle \boldsymbol{x}_i, \boldsymbol{y}_j \rangle = 0$ for $\{i, j\} = \{1, 2\}$ and $\langle \boldsymbol{x}_1, \boldsymbol{y}_1 \rangle = \langle \boldsymbol{x}_2, \boldsymbol{y}_2 \rangle = 1$. Let $l_1 = Span(\boldsymbol{x}_1, \boldsymbol{x}_2), l_2 = Span(\boldsymbol{x}_2, \boldsymbol{y}_1), l_3 = Span(\boldsymbol{y}_1, \boldsymbol{y}_2), l_4 = Span(\boldsymbol{y}_2, \boldsymbol{x}_1)$.

5. Prove that $\Omega(V)$ is generated by $\chi(l_1) \cup \chi(l_2) \cup \chi(l_3) \cup \chi(l_4)$.

6. Let L_1 be the subgroup of $\Omega(V)$ generated by $\chi(l_4) \cup \chi(l_2)$ and L_2 the subgroup generated by $\chi(l_1) \cup \chi(l_3)$. Prove that L_1 and L_2 are isomorphic to $SL_2(\mathbb{F})$.

7. Prove that L_1 and L_2 commute.

8. Prove that the set $B = S_1(Span(\boldsymbol{x}_1, \boldsymbol{x}_2))$ is a block of imprimitivity of $\Omega(V)$.

In Exercises 9–13 assume (V, ϕ) is a non-degenerate orthogonal space of dimension four and Witt index one over the field $\mathbb{F}$. Let $(\boldsymbol{u}, \boldsymbol{v})$ be a hyperbolic pair and set $U = Span(\boldsymbol{u}, \boldsymbol{v})$ and $W = U^{\perp}$. Let $(\boldsymbol{x}, \boldsymbol{y})$ be an orthogonal basis of W and assume that $\phi(\boldsymbol{x}) = 1$ and $\phi(\boldsymbol{y}) = d$.

9. Prove that the quadratic polynomial $X^2 + d$ is irreducible in $\mathbb{F}[X]$.

10. Set $\mathbb{K} = \mathbb{F}[X]/(X^2 + d)$, the quotient ring of $\mathbb{F}[X]$ by the maximal ideal $(X^2 + d)$ generated by $X^2 + d$. Set $\omega = X + (X^2 + d)$ so that $\mathbb{K} = \mathbb{F}(\omega) = \{a + b\omega| \ , b \in \mathbb{F}\}$. For $\alpha = a + b\omega \in \mathbb{K}$ denote by $\overline{\alpha}$ its conjugate $a - b\omega$. Set $M = \{\begin{pmatrix} a & \alpha \\ \overline{\alpha} & b \end{pmatrix} |a, b \in \mathbb{F}, \alpha \in \mathbb{K}\}$. Note that $m \in M_{22}(\mathbb{K})$ is in M if and only if $\overline{m}^{tr} = m$.

Define $q : M \to \mathbb{F}$ by $q(m) = -det(m)$. Prove that (M, q) is isometric to (V, ϕ).

11. If $A \in SL_2(\mathbb{K})$ and $m \in M$ set $A \cdot m = \overline{A}^{tr} mA$. Prove that $A \cdot m \in M$.

12. For $A \in SL_2(\mathbb{K})$, let $T_A : M \to M$ given by $T_A(m) = A \cdot m$. Prove that T_A is a linear operator on M and an isometry of (M, q).

13. Prove that $Range(T)$ is isomorphic to $PSL_2(\mathbb{K})$ and equal to $\Omega(M, q)$ (which is isomorphic to $\Omega(V, \phi)$).

11.4 Unitary Groups

In this section we continue to study the unitary group and demonstrate that, with a small number of counterexamples, a projective special unitary group is simple.

What You Need to Know

To successfully navigate the material of this new section you should by now have mastered the following concepts: vector space over a field $\mathbb{F}$, basis of a vector space, dimension of a vector space, linear operator on a vector space V, matrix of a linear operator $T : V \to V$ with respect to a base $\mathcal{B}$ for V, eigenvalue and eigenvector of an operator T, the algebra $\mathcal{L}(V, V)$ of operators on a finite-dimensional vector space V, an invertible operator on a vector space V, the group $GL(V)$ of invertible operators on a finite-dimensional vector space V, sesquilinear form on a vector space, unitary space, non-degenerate unitary space, isotropic vector in a unitary space, hyperbolic pair in a unitary space, and an isometry of a unitary space. You must also be familiar with the following concepts from group theory: Abelian group, solvable group, normal subgroup of a group, quotient group of a group by a normal subgroup, the commutator of two elements in a group, the commutator subgroup of a group, a perfect group, the center of a group, a simple group, action of a group G on a set X, transitive action of a group G on a set X, primitive action of a group G on a set X, and a faithful action of a group G on a set X. This latter material can be found in Appendix B.

We begin by recalling some definitions:

Let V be a vector space over a field $\mathbb{F}$, σ a non-trivial automorphism of $\mathbb{F}$ with $\sigma^2 = I_{\mathbb{F}}$. Set $\mathbb{E} = \mathbb{F}^{\sigma} = \{a \in \mathbb{F} |\ \sigma(a) = a\}$. The norm from $\mathbb{F}$ to $\mathbb{E}$ is the function $N : \mathbb{F} \to \mathbb{E}$ such that $N(a) = a\sigma(a)$. The trace from $\mathbb{F}$ to $\mathbb{E}$ is the function $Tr : \mathbb{F} \to \mathbb{E}$ given by $Tr(a) = a + \sigma(a)$. We denote by Φ the kernel of $Tr, \Phi = \{a \in \mathbb{F} | a + \sigma(a) = 0\}$. We also denote by Λ the kernel of N restricted to $\mathbb{F}^*, \Lambda = \{a \in \mathbb{F}^* | a\sigma(a) = 1\}$. We will often times denote $\sigma(a)$ by $\overline{a}$.

A σ-Hermitian form (hereafter referred to as a Hermitian form) is a map $f : V \times V \to \mathbb{F}$ such that

1) for $\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{w} \in V, c_1, c_2 \in \mathbb{F}$, $f(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2, \boldsymbol{w}) = c_1 f(\boldsymbol{v}_1, \boldsymbol{w}) + c_2 f(\boldsymbol{v}_2, \boldsymbol{w})$; and

2) for $\boldsymbol{v}, \boldsymbol{w} \in V$, $f(\boldsymbol{w}, \boldsymbol{v}) = \sigma(f(\boldsymbol{v}, \boldsymbol{w}))$.

A unitary space is a pair (V, f) consisting of a vector space V and a Hermitian form $f : V \times V \to \mathbb{F}$. The radical of $(V, f), Rad(f)$, consists of all those vectors $\boldsymbol{v}$ such that $f(\boldsymbol{w}, \boldsymbol{v}) = 0$ for all $\boldsymbol{w} \in V$. The unitary space (V, f) is non-degenerate if $Rad(f) = \{\boldsymbol{0}\}$.

An isometry of a unitary space (V, f) is a linear operator $T : V \to V$ such that $f(T(\boldsymbol{u}), T(\boldsymbol{v})) = f(\boldsymbol{u}, \boldsymbol{v})$ for all vectors $\boldsymbol{u}, \boldsymbol{v}$. If (V, f) is non-degenerate, then an isometry must be invertible since a vector $\boldsymbol{v} \in Ker(T)$ must lie in the radical. When (V, f) is non-degenerate, the composition of isometries is an isometry and the inverse of an isometry is an isometry; therefore the collection of isometries is a subgroup of $GL(V)$ which we denote by $U(V, f)$ or simply $U(V)$ when the form f is understood.

A vector $\boldsymbol{v}$ in a unitary space (V, f) is ***isotropic*** if $f(\boldsymbol{v}, \boldsymbol{v}) = 0$ and ***anisotropic*** otherwise. The unitary space is said to be ***isotropic*** if there exist non-zero isotropic vectors and ***anisotropic*** otherwise. A pair $(\boldsymbol{u}, \boldsymbol{v})$ of isotropic vectors such that $f(\boldsymbol{u}, \boldsymbol{v}) = 1$ is said to be a **hyperbolic pair**. A subspace spanned by a hyperbolic pair is a **hyperbolic plane**.

Notation. Assume (V, f) is an isotropic unitary space. We will denote by $I_1(V)$ the set of all $X = Span(\boldsymbol{x})$ such that $\boldsymbol{x}$ is isotropic. We will refer to such X as **isotropic points**. For $X \in I_1(V)$ we will denote by $\Delta(X)$ those $Y \neq X$ in $I_1(V)$ such that $Y \perp X$ and by $\Gamma(X)$ the set of $Y \in I_1(V)$ such that $Y \not\perp X$.

Throughout this section we will generally use the bar notation to indicate images under σ. For example, we will write $\overline{a}$ for $\sigma(a)$. When $\boldsymbol{v} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{F}^n$ we will denote by $\overline{\boldsymbol{v}}$ the vector obtained from $\boldsymbol{v}$ by applying σ to each entry of $\boldsymbol{v}$ and similarly for a matrix $A, \overline{A} = \sigma(A)$, is the matrix obtained by applying σ to the entries of A.

Recall if $\mathcal{B} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ is a basis for V then the matrix of f with respect to $\mathcal{B}$, denoted by $\mathcal{M}_f(\mathcal{B}, \mathcal{B})$, is the matrix A whose (i, j)-entry is $a_{ij} = f(\boldsymbol{v}_i, \boldsymbol{v}_j)$. For vectors $\boldsymbol{u}, \boldsymbol{v} \in V$

$$f(\boldsymbol{u}, \boldsymbol{v}) = [\boldsymbol{u}]_{\mathcal{B}}^{tr} A \overline{[\boldsymbol{v}]}_{\mathcal{B}}.$$

The matrix A is a Hermitian matrix, that is, it satisfies $A^{tr} = \overline{A}$.

Theorem 11.23 *Let (V, f) be a finite-dimensional, non-degenerate unitary space and let $T \in U(V, f)$. Then $N(det(T)) = 1$. Moreover, if $a \in \mathbb{F}^*$ and $N(a) = 1$, then there exists $T \in U(V)$ with $det(T) = a$.*

Proof *Let $\mathcal{B} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ be a basis for V, and set $A = \mathcal{M}_f(\mathcal{B}, \mathcal{B})$ and $Q = \mathcal{M}_T(\mathcal{B}, \mathcal{B})$. It follows from the assumption that T is an isometry that $Q^{tr} A \overline{Q} = A$. Taking determinants and using the identity $det(Q^{tr}) = det(Q)$ we obtain that $det(Q)\det(\overline{Q})det(A) = det(A)$. Since f is non-degenerate, A is invertible and $det(A) \neq 0$ Consequently, $N(det(Q)) = det(Q)\overline{det(Q)} = det(Q)det(\overline{Q}) = 1$.*

For the second part, assume $N(a) = 1$*. Let* $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ *be an orthogonal basis of* V*. This exists by Exercise 11 of Section (11.4). The map* $T \in \mathcal{L}(V, F)$ *such that* $T(\boldsymbol{v}_i) = \boldsymbol{v}_i$ *for* $2 \le i \le n$ *and* $T(\boldsymbol{v}_1) = a\boldsymbol{v}_1$ *is an isometry and* $det(T) = a$*.*

Definition 11.11 *Let* (V, f) *be a finite-dimensional, non-degenerate unitary space. The* **special unitary group** *consists of those isometries* T *such that* $det(T) = 1$*. It is denoted by* $SU(V, f)$ *or simply* $SU(V)$ *when the form* f *is understood. Note that* $SU(V)$ *is the kernel of the map* $det : U(V, f) \to \mathbb{F}^*$ *and therefore* $SU(V)$ *is a normal subgroup of* $U(V)$*.*

In the next theorem we classify isometries T of (V, f) such that the kernel of $T - I_V$ contains a hyperplane.

Theorem 11.24 *Let* $T \in U(V)$ *and assume* $ker(T - I_V) = H$ *is a hyperplane of* V*. Then one of the following holds:*

1) $X = Range(T - I_V)$ *is anisotropic,* $H = X^\perp$*, and there is a scalar* $c \in \mathbb{F}$ *with* $N(c) = 1$ *such that* $T(\boldsymbol{x}) = c\boldsymbol{x}$*.*

2) $X = Range(T - I_V)$ is isotropic and $H = X^\perp$, T is a transvection with center X and axis $X^\perp = H$. Moreover, if $X = Span(\boldsymbol{x})$. then there is a $c \in \mathbb{F}$ with $Tr(c) = 0$ such that $T(\boldsymbol{y}) = \boldsymbol{y} + cf(\boldsymbol{y}, \boldsymbol{x})\boldsymbol{x}$ for all $\boldsymbol{y} \in V$.

Proof *Assume first that* $X \nsubseteq H$*. Then* $V = X \oplus H$*. Let* $\boldsymbol{x}$ *be a non-zero vector from* X*. Since* $\boldsymbol{x} \notin H, (T - I_V)(\boldsymbol{x}) \neq \mathbf{0}$ *and* $(T - I_V)(\boldsymbol{x}) \in X$*. Consequently,* $T(\boldsymbol{x}) = c\boldsymbol{x}$ *for some* $c \in \mathbb{F}^*$*. Since* $T \neq I_V, c \neq 1$*. We now prove that* $\boldsymbol{x}$ *is anisotropic. Suppose to the contrary that* $f(\boldsymbol{x}, \boldsymbol{x}) = 0$*. Since* H *is a hyperplane and* $\boldsymbol{x} \notin H$*, it follows that* $H \neq \boldsymbol{x}^\perp$*. In particular, there exists* $\boldsymbol{y} \in H$ *such that* $f(\boldsymbol{x}, \boldsymbol{y}) \neq 0$*. However,* $f(\boldsymbol{x}, \boldsymbol{y}) = f(T(\boldsymbol{x}), T(\boldsymbol{y})) = f(c\boldsymbol{x}, \boldsymbol{y}) = cf(\boldsymbol{x}, \boldsymbol{y})$ *from which we conclude that* $c = 1$*, a contradiction. So,* $\boldsymbol{x}$ *is anisotropic, as claimed. It remains to show that* $H = \boldsymbol{x}^\perp$ *and* $N(c) = 1$*. Suppose to the contrary that* $H \neq \boldsymbol{x}^\perp$ *and let* $\boldsymbol{y} \in H$ *with* $f(\boldsymbol{x}, \boldsymbol{y}) \neq 0$*. Multiplying* $\boldsymbol{y}$ *by* $\frac{1}{\sigma(f(\boldsymbol{x}, \boldsymbol{y}))}$*, if necessary, we may assume that* $f(\boldsymbol{x}, \boldsymbol{y}) = 1$*. Then* $1 \neq c = f(c\boldsymbol{x}, \boldsymbol{y}) = f(T(\boldsymbol{x}), T(\boldsymbol{y})) = f(\boldsymbol{x}, \boldsymbol{y}) = 1$*, a contradiction. Thus,* $H = X^\perp$*. Finally,* $f(\boldsymbol{x}, \boldsymbol{x}) = f(T(\boldsymbol{x}), T(\boldsymbol{x})) = f(c\boldsymbol{x}, c\boldsymbol{x}) = c\overline{c}f(\boldsymbol{x}, \boldsymbol{x})$ *and therefore* $N(c) = 1$*. Thus, in this case 1) holds. Note that if* S *is the operator defined by* $S(\boldsymbol{y}) = \boldsymbol{y} + (c - 1)\frac{f(\boldsymbol{y}, \boldsymbol{x})}{f(\boldsymbol{x}, \boldsymbol{x})}\boldsymbol{x}$*, then* $S = T$*. This follows since* $S(\boldsymbol{y}) = \boldsymbol{y} = T(\boldsymbol{y})$ *for* $\boldsymbol{y} \in \boldsymbol{x}^\perp = H$ *and* $S(\boldsymbol{x}) = c\boldsymbol{x} = T(\boldsymbol{x})$*.*

We may therefore assume that $X \subset H$*. Now let* $g : V \to \mathbb{F}$ *be defined by* $(T - I_V)(\boldsymbol{y}) = g(\boldsymbol{y})\boldsymbol{x}$*. Then* g *is in* $\mathcal{L}(V, \mathbb{F})$*. Since* f *is non-degenerate, there exists* $\boldsymbol{v} \in V$ *such that* $g(\boldsymbol{y}) = f(\boldsymbol{y}, \boldsymbol{v})$ *so that* $T(\boldsymbol{y}) = \boldsymbol{y} + f(\boldsymbol{y}, \boldsymbol{v})\boldsymbol{x}$*. Note that* $H = \boldsymbol{v}^\perp$*, and since* $\boldsymbol{x} \in H$ *we also have* $\boldsymbol{x} \perp \boldsymbol{v}$*. We will first show that* $f(\boldsymbol{x}, \boldsymbol{x}) = f(\boldsymbol{v}, \boldsymbol{v}) = 0$*. We have* $T(\boldsymbol{v}) = \boldsymbol{v} + f(\boldsymbol{v}, \boldsymbol{v})\boldsymbol{x}$*. Since* T *is an isometry,*

$$\begin{aligned} f(\boldsymbol{v},\boldsymbol{v}) &= f(T(\boldsymbol{v}),T(\boldsymbol{v})) \\ &= f(\boldsymbol{v}+f(\boldsymbol{v},\boldsymbol{v})\boldsymbol{x},\boldsymbol{v}+f(\boldsymbol{v},\boldsymbol{v})\boldsymbol{x}) \\ &= f(\boldsymbol{v},\boldsymbol{v})+f(\boldsymbol{v},\boldsymbol{v})\overline{f(\boldsymbol{v},\boldsymbol{v})}f(\boldsymbol{x},\boldsymbol{x}) \\ &= f(\boldsymbol{v},\boldsymbol{v})+f(\boldsymbol{v},\boldsymbol{v})^2 f(\boldsymbol{x},\boldsymbol{x}). \end{aligned}$$

Consequently, $f(\boldsymbol{v},\boldsymbol{v})^2 f(\boldsymbol{x},\boldsymbol{x})=0$. So, either $f(\boldsymbol{v},\boldsymbol{v})=0$ or $f(\boldsymbol{x},\boldsymbol{x})=0$.

Suppose $f(\boldsymbol{v},\boldsymbol{v})=0, f(\boldsymbol{x},\boldsymbol{x})\neq 0$. Then Span$(\boldsymbol{v})\neq$ Span$(\boldsymbol{x})$ and $\boldsymbol{v}^\perp\neq\boldsymbol{x}^\perp$. Let $\boldsymbol{y}\in\boldsymbol{x}^\perp\setminus\boldsymbol{v}^\perp$. Without loss of generality, we may assume that $f(\boldsymbol{y},\boldsymbol{v})=1$. We then have

$$\begin{aligned} f(\boldsymbol{y},\boldsymbol{y}) &= f(T(\boldsymbol{y}),T(\boldsymbol{y})) \\ &= f(\boldsymbol{y}+\boldsymbol{x},\boldsymbol{y}+\boldsymbol{x}) \\ &= f(\boldsymbol{y},\boldsymbol{y})+f(\boldsymbol{x},\boldsymbol{x}), \end{aligned}$$

But then $f(\boldsymbol{x},\boldsymbol{x})=0$, a contradiction. Suppose then that $f(\boldsymbol{v},\boldsymbol{v})\neq 0=f(\boldsymbol{x},\boldsymbol{x})$. Then $T(\boldsymbol{v})=\boldsymbol{v}+f(\boldsymbol{v},\boldsymbol{v})\boldsymbol{x}$. As above, $\boldsymbol{v}^\perp\neq\boldsymbol{x}^\perp$. Now choose $\boldsymbol{y}\in\boldsymbol{v}^\perp,\boldsymbol{y}\notin\boldsymbol{x}^\perp$. We then have

$$\begin{aligned} 0 &= f(\boldsymbol{y},\boldsymbol{v}) \\ &= f(T(\boldsymbol{y}),T(\boldsymbol{v})) \\ &= f(\boldsymbol{y},\boldsymbol{v}+f(\boldsymbol{v},\boldsymbol{v})\boldsymbol{x}) \\ &= f(\boldsymbol{y},\boldsymbol{v})+\overline{f(\boldsymbol{v},\boldsymbol{v})}f(\boldsymbol{y},\boldsymbol{x}) \\ &= f(\boldsymbol{v},\boldsymbol{v})f(\boldsymbol{y},\boldsymbol{x}). \end{aligned}$$

However, $f(\boldsymbol{v},\boldsymbol{v})\neq 0\neq f(\boldsymbol{y},\boldsymbol{v})$, and we have again arrived at a contradiction. Thus, $f(\boldsymbol{v},\boldsymbol{v})=f(\boldsymbol{x},\boldsymbol{x})=0$. We next show that Span$(\boldsymbol{v})=$ Span$(\boldsymbol{x})$, equivalently, that $\boldsymbol{v}^\perp=\boldsymbol{x}^\perp$. Suppose to the contrary. Then we can choose $\boldsymbol{u}\in\boldsymbol{v}^\perp$ such that $f(\boldsymbol{u},\boldsymbol{x})=1$; and then $\boldsymbol{w}\in$ Span$(\boldsymbol{u},\boldsymbol{x})^\perp$ such that $f(\boldsymbol{w},\boldsymbol{v})=1$. We now have

$$0=f(\boldsymbol{u},\boldsymbol{w})=f(T(\boldsymbol{u}),T(\boldsymbol{w}))=f(\boldsymbol{u},\boldsymbol{w}+\boldsymbol{x})=f(\boldsymbol{u},\boldsymbol{w})+f(\boldsymbol{u},\boldsymbol{x})=1,$$

a contradiction.

Thus, Span$(\boldsymbol{v})=$ Span$(\boldsymbol{x})$. Let $\boldsymbol{v}=b\boldsymbol{x}$ and set $c=\overline{b}$. Then $T(\boldsymbol{y})=\boldsymbol{y}+f(\boldsymbol{y},b\boldsymbol{x})\boldsymbol{x}=\boldsymbol{y}+\overline{b}f(\boldsymbol{y},\boldsymbol{x})\boldsymbol{x}=\boldsymbol{y}+cf(\boldsymbol{y},\boldsymbol{x})\boldsymbol{x}$ for all $\boldsymbol{y}\in V$. It remains to show that $Tr(c)=c+\overline{c}=0$. Toward that end, let $\boldsymbol{y}\in V$ such that $f(\boldsymbol{y},\boldsymbol{x})=1$ so that $T(\boldsymbol{y})=\boldsymbol{y}+c\boldsymbol{x}$. We then have

$$\begin{aligned} f(\boldsymbol{y},\boldsymbol{y}) &= f(T(\boldsymbol{y}),T(\boldsymbol{y})) \\ &= f(\boldsymbol{y}+c\boldsymbol{x},\boldsymbol{y}+c\boldsymbol{x}) \\ &= f(\boldsymbol{y},\boldsymbol{y})+cf(\boldsymbol{x},\boldsymbol{y})+\overline{c}f(\boldsymbol{y},\boldsymbol{x})+c\overline{c}f(\boldsymbol{x},\boldsymbol{x}) \\ &= f(\boldsymbol{y},\boldsymbol{y})+c+\overline{c}. \end{aligned}$$

Thus, $c+\overline{c}=0$ as claimed.

Definition 11.12 *Let (V,f) be a non-degenerate unitary space over the field $\mathbb{F}$, $\boldsymbol{u}$ an isotropic vector, and $c \in \Lambda = Ker(N)$. Denote bu $\tau_{\boldsymbol{u},c}$ the operator of V given by*

$$\tau_{\boldsymbol{u},c}(\boldsymbol{x}) = \boldsymbol{x} + cf(\boldsymbol{x},\boldsymbol{u})\boldsymbol{u}.$$

The operator $\tau_{\boldsymbol{u},c}$ is a transvection centered at $\boldsymbol{u}$. For any vector $\boldsymbol{x}$ such that $f(\boldsymbol{x},\boldsymbol{u})=1$ it takes $\boldsymbol{x}$ to $\boldsymbol{x}+c\boldsymbol{u}$.

Notation If (V,f) is an isotropic unitary space we will denote by $\Omega(V)$ the subgroup of $SU(V)$ generated by all transvections.

Lemma 11.33 *Assume (V,f) is a non-degenerate isotropic unitary space and that W is a non-degenerate isotropic subspace. Assume T is an isometry of V, that T restricted to $W^\perp$ is the identity on $W^\perp$, and that T restricted to W is in $\Omega(W)$. Then $T \in \Omega(V)$.*

We leave this as an exercise.

Definition 11.13 *Let $\boldsymbol{v}$ be an anisotropic vector, $c \in \Phi, c \neq 1$. We denote by $\rho_{\boldsymbol{v},c}$ the operator given by*

$$\rho_{\boldsymbol{v},c}(\boldsymbol{x}) = \boldsymbol{x} + (c-1)\frac{f(\boldsymbol{x},\boldsymbol{v})}{f(\boldsymbol{v},\boldsymbol{v})}\boldsymbol{v}.$$

This is a **unitary pseudoreflection**.

Lemma 11.34 *Let (V,f) be a hyperbolic two-dimensional unitary space. Let $\boldsymbol{x}$ be an isotropic vector. Then $T=\{\tau_{\boldsymbol{x},a} \mid a \in \Phi\}$ is transitive on the isotropic vectors $\boldsymbol{y}$ such that $f(\boldsymbol{x},\boldsymbol{y})=1$.*

Proof *Assume $\boldsymbol{y}, \boldsymbol{z}$ are isotropic vectors with $f(\boldsymbol{x}, \boldsymbol{y}) = f(\boldsymbol{x}, \boldsymbol{z}) = 1$. If $\boldsymbol{z} = a\boldsymbol{x} + b\boldsymbol{y}$ we must have $b = 1$. Since $f(\boldsymbol{z}, \boldsymbol{z}) = a + \overline{a} = 0$, it follows that $a \in \Phi$. Then $\tau_{\boldsymbol{x},a}(\boldsymbol{y}) = \boldsymbol{z}$.*

Corollary 11.14 *Let (V, f) be a hyperbolic two-dimensional unitary space. Then $\Omega(V)$ is doubly transitive on $I_1(V)$.*

Proof *Let $X = Span(\boldsymbol{x}), Y = Span(\boldsymbol{y})$ be distinct elements of $I_1(V)$. By Lemma (11.34) $T_X = \{\tau_{\boldsymbol{x},a} |\ a \in \Phi\}$ is transitive on $I_1(V) \setminus \{X\}$ and $T_Y = \{\tau_{\boldsymbol{y},b} | b \in \Phi\}$ is transitive on $I_k 1V) \setminus \{Y\}$. The result follows from this.*

Corollary 11.15 *Let (V, f) be a non-degenerate, isotropic unitary space. Then $\Omega(V)$ is transitive $I_1(V)$.*

Proof *Let $X = Span(\boldsymbol{x}), Y = Span(\boldsymbol{y})$ be isotropic points. If $f(\boldsymbol{x}, \boldsymbol{y}) \neq 0$ then the group generated by $\tau_{\boldsymbol{x},a}, \tau_{\boldsymbol{y},b}$ where $a, b \in \Phi$, is doubly transitive on $I_1(X + Y)$, in particular, there is a $\gamma \in \Omega(V)$ such that $\gamma(X) = Y$. On the other hand, if $f(\boldsymbol{x}, \boldsymbol{y}) = 0$ then there exists $Z \in I_1(V)$ such that $X \not\perp Z \not\perp Y$. By what we have just proved there are $\gamma_i \in \Omega(V), i = 1, 2$ such that $\gamma_1(X) = Z, \gamma_2(Z) = Y$. Set $\gamma = \gamma_2\gamma_1$. Then $\gamma \in \Omega(V)$ and $\gamma(X) = Y$.*

We next determine the group $SU(V)$ when $dim(V) = 2$. Since we are assuming that f is isotropic it follows from Lemma (9.14) that V has a basis $(\boldsymbol{u}, \boldsymbol{v})$ of isotropic vectors such that $f(\boldsymbol{u}, \boldsymbol{v}) = 1$. We show in this case that $SU(V)$ is isomorphic to $SL_2(\mathbb{E})$, where $\mathbb{E} = \mathbb{F}^\sigma$.

Theorem 11.25 *Assume (V, f) is a non-degenerate, isotropic two-dimensional unitary space. Then $SU(V)$ is isomorphic to $SL_2(\mathbb{E})$.*

Proof *Let $\mathcal{B} = (\boldsymbol{u}, \boldsymbol{v})$ be a basis of isotropic vectors such that $f(\boldsymbol{u}, \boldsymbol{v}) = 1$. Then $\mathcal{M}_f(\mathcal{B}, \mathcal{B}) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = J$. Assume $T \in GL(V)$ and let $\mathcal{M}_T(\mathcal{B}, \mathcal{B}) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = Q$. Then $T \in SU(V)$ if and only if $Q^{tr} J \overline{Q} = J$. This implies that $a\overline{c} + \overline{a}c = b\overline{d} + \overline{b}d = 0, a\overline{d} + \overline{b}d = 1$. Furthermore, if $T \in SU(V)$, then $det(T) = ad - bc = 1$. As we shall see this implies that $a, b \in \mathbb{E}$ and $c, d \in \Phi$. Consider $(a - \overline{a})(d - \overline{d}) - (b + \overline{b})(c + \overline{c})$. A straightforward calculation shows that this is equal to $(ad - bc) + (\overline{a}\overline{d} - \overline{b}\overline{c}) - (a\overline{d} + \overline{b}c) - (\overline{a}d + b\overline{c}) = 0$.*

Assume that $(a - \overline{a})(b + \overline{b})(c + \overline{c})(d - \overline{d}) \neq 0$. Then, in particular, $abcd \neq 0$.

Set $c = \alpha a$ and $b = \beta d$. From $a\overline{c} + \overline{a}c = 0$ it follows that $\overline{\alpha} = -\alpha$ and similarly $\overline{\beta} = -\beta$. Set $\phi = \frac{c+\overline{c}}{a-\overline{a}}$ and $\delta = \frac{b+\overline{b}}{d-\overline{d}}$. Then it is easy to check that $\phi = \alpha, \beta = \delta = \frac{1}{\alpha}$. However, it then follows that $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \det \begin{pmatrix} a & \frac{1}{\alpha}d \\ \alpha d & d \end{pmatrix} = 0$, a contradiction. Thus, at least one of $a - \overline{a}, d - \overline{d}, b + \overline{b}, c + \overline{c}$ is zero. Note that $a - \overline{a} = 0$ if and only if $c + \overline{c} = 0$ and $d - \overline{d} = 0$ if and only if $b + \overline{b} = 0$. So assume that $a - \overline{a} = 0$, that is, $a \in \mathbb{E}$ and $c + \overline{c} = 0$ so that $c \in \Phi$. We need to show that $b \in \Phi, d \in \mathbb{E}$.

Note that $(Q^{-1})^{tr} J Q^{-1} = J$ so we can apply what we have shown to the matrix $Q^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Since $a \in \mathbb{E}$ it follows that $b \in \Phi$ and hence $d \in \mathbb{E}$ as required.

Thus we have shown that $SU(V)$ is isomorphic to the subgroup of $GL_2(\mathbb{F})$ consisting of all matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $a, d \in \mathbb{E}, b, c \in \Phi$ and $ad - bc = 1$. We shall denote this subgroup of $SL_2(\mathbb{F})$ by $SU_2(\mathbb{F})$. We now demonstrate that $SU_2(\mathbb{F})$ is isomorphic to $SL_2(\mathbb{E})$. Fix a non-zero element $u \in \Phi$. Then an element $g \in \mathbb{F}$ is in Φ if and only if $ug \in \mathbb{E}$. Moreover, $u^{-1} \in \Phi$. For $Q = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SU_2(\mathbb{F})$ let $S(Q) = \begin{pmatrix} a & ub \\ u^{-1}c & d \end{pmatrix}$. Then $\det(S(Q)) = ad - bc = 1$ so that $S(Q) \in SL_2(\mathbb{E})$. It is a straightforward calculation, which we leave as an exercise, to see that $S(Q_1Q_2) = S(Q_1)S(Q_2)$, so that S is a homomorphism of groups. Clearly, the map is injective and there is an obvious inverse, so that it is an isomorphism.

Remark 11.8 *Let (V, f) be a non-degenerate, isotropic two-dimensional unitary space with a basis $\mathcal{B} = (\boldsymbol{u}, \boldsymbol{v})$, a hyperbolic pair. Under the isomorphism from $SU(V)$ to $SL_2(\mathbb{E})$ given by $\sigma(T) = S(\mathcal{M}_T(\mathcal{B}, \mathcal{B}))$, the transvections of $SU(V)$ correspond to the transvections of $SL_2(\mathbb{E})$. Because of the conjugacy of the transvection groups in $U(V)$ and $SL_2(\mathbb{E})$ it suffices to show this for one transvection subgroup of $SU(V)$, for example, $\{\tau_{\boldsymbol{u},c} | \ c \in \Lambda\}$. The matrix of $\tau_{\boldsymbol{u},c}$ with respect to $\mathcal{B}$ is $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$ maps to the matrix $\begin{pmatrix} 1 & uc \\ 0 & 1 \end{pmatrix}$, which is a transvection in $SL_2(\mathbb{E})$*

Lemma 11.35 *Assume (V, f) is a hyperbolic plane, $\boldsymbol{x}, \boldsymbol{y} \in V$ with $f(\boldsymbol{x}, \boldsymbol{x}) = f(\boldsymbol{y}, \boldsymbol{y}) \neq 0$. Then there exists $T \in SU(V)$ such that $T(\boldsymbol{x}) = \boldsymbol{y}$.*

Proof Let $\mathcal{B} = (\boldsymbol{u}, \boldsymbol{v})$ be a hyperbolic basis for V. Assume $\boldsymbol{x} = a\boldsymbol{u} + b\boldsymbol{v}$ and $\boldsymbol{y} = c\boldsymbol{u} + d\boldsymbol{v}$. Set $\boldsymbol{x}' = -\overline{a}\boldsymbol{u} + \overline{b}\boldsymbol{v}, \boldsymbol{y}' = -\overline{c}\boldsymbol{u} + \overline{d}\boldsymbol{v}$. Then $\boldsymbol{x} \perp \boldsymbol{x}'$ and $\boldsymbol{y} \perp \boldsymbol{y}'$. Note that since $f(\boldsymbol{x}, \boldsymbol{x}) \neq 0 \neq f(\boldsymbol{y}, \boldsymbol{y})$, it follows that $\boldsymbol{x}' \neq \boldsymbol{x}$ and

$\boldsymbol{y}' \neq \boldsymbol{y}$ so that $(\boldsymbol{x}, \boldsymbol{x}')$ and $(\boldsymbol{y}, \boldsymbol{y}')$ are (orthogonal) bases of V. We also note that $f(\boldsymbol{x}', \boldsymbol{x}') = -(a\overline{b} + \overline{a}b) = -f(\boldsymbol{x}, \boldsymbol{x}) = -f(\boldsymbol{y}, \boldsymbol{y}) = -(c\overline{d} + \overline{d}c) = f(\boldsymbol{y}', \boldsymbol{y}')$. Let T be the operator on V such that $T(\boldsymbol{x}) = \boldsymbol{y}, T(\boldsymbol{x}') = \boldsymbol{y}'$. It follows that T is an isometry of f. We show that T has determinant one. Let $A = \mathcal{M}_T(\mathcal{B}, \mathcal{B})$. Then $A\begin{pmatrix} a & -\overline{a} \\ b & \overline{b} \end{pmatrix} = \begin{pmatrix} c & -\overline{c} \\ d & \overline{d} \end{pmatrix}$. Since det $\begin{pmatrix} a & -\overline{a} \\ b & \overline{b} \end{pmatrix} = a\overline{b} + \overline{a}b = c\overline{d} + \overline{c}d =$ det $\begin{pmatrix} c & -\overline{c} \\ d & \overline{d} \end{pmatrix}$, it follows that det$(A) = 1$ and, therefore, det$(T) = 1$. Thus, $T \in SU(V)$.

We will eventually prove that, with a single exception, the group $SU(V)$ is generated by its transvections. We will then show that, with three exceptions, $SU(V)$ is perfect, whence that $PSU(V) = SU(V)/Z(SU(V))$ is simple when $SU(V)$ is perfect. In order to prove tis we will need to prove that $SU(V)$ is transitive on hyperbolic planes, which is our immediate goal. In the theorem that follows we have made extensive use of computations contained in ([8]).

Theorem 11.26 *Let (V, f) be a non-degenerate, isotropic unitary space over the field $\mathbb{F} \neq \mathbb{F}_4$. Then $SU(V)$ is transitive on its hyperbolic planes.*

Proof *Assume $X_i = Span(\boldsymbol{x}_i)$ and $Y_i = Span(\boldsymbol{y}_i) \in I_1(V)$ for $i = 1, 2$, with $f(\boldsymbol{x}_1, \boldsymbol{y}_1) = f(\boldsymbol{x}_2, \boldsymbol{y}_2) = 1$. Set $H_i = X_i + Y_i, i = 1, 2$. We desire an operator $S \in SU(V)$ such that $S(H_1) = H_2$. Since $SU(V)$ is transitive on $I_1(V)$, without loss of generality, we can assume that $X_1 = X_2$ so that $dim(H_1 + H_2) = 3$. Let $a = f(\boldsymbol{y}_2, \boldsymbol{y}_1)$ and assume that $a \neq 0$. Set $\boldsymbol{w} = a\boldsymbol{x}_1 + \boldsymbol{y}_1 - \boldsymbol{y}_2$. Then $f(\boldsymbol{w}, \boldsymbol{x}_1) = f(a\boldsymbol{x}_1 + \boldsymbol{y}_1 - \boldsymbol{y}_2, \boldsymbol{x}_1) = f(\boldsymbol{y}_1, \boldsymbol{x}_1) - f(\boldsymbol{y}_2, \boldsymbol{x}_1) = 1 - 1 = 0$. Thus, $\boldsymbol{w} \perp \boldsymbol{x}_1$. Also, $f(\boldsymbol{w}, \boldsymbol{y}_2) = f(a\boldsymbol{x}_1 + \boldsymbol{y}_1 - \boldsymbol{y}_2, \boldsymbol{y}_1) = af(\boldsymbol{x}_1, \boldsymbol{y}_1) - f(\boldsymbol{y}_2, \boldsymbol{y}_1) = a - a = 0$. So, $\boldsymbol{w} \perp \boldsymbol{y}_1$. Moreover,*

$$\begin{aligned} f(\boldsymbol{w}, \boldsymbol{w}) &= f(a\boldsymbol{x}_1 + \boldsymbol{y}_1 - \boldsymbol{y}_2, \boldsymbol{w}) \\ &= f(-\boldsymbol{y}_2, \boldsymbol{w}) \\ &= -f(\boldsymbol{y}_2, a\boldsymbol{x}_1 + \boldsymbol{y}_1 - \boldsymbol{y}_2) \\ &= -a - \overline{a} \\ &= -(a + \overline{a}. \end{aligned}$$

Let $\gamma(\boldsymbol{z}) = \boldsymbol{z} + f(\boldsymbol{z}, \boldsymbol{x}_1)\overline{a}\boldsymbol{x}_1 + f(\boldsymbol{z}, \boldsymbol{x}_1)\boldsymbol{w} - f(\boldsymbol{z}, \boldsymbol{w})\boldsymbol{x}_1$. Note that since $\boldsymbol{w} \perp \boldsymbol{x}_1$ and $\boldsymbol{x}_1$ is isotropic, $\gamma(\boldsymbol{x}_1) = \boldsymbol{x}_1$. We next compute $\gamma(\boldsymbol{y}_2)$;

$$\begin{aligned} \gamma(\boldsymbol{y}_2) &= \boldsymbol{y}_2 + f(\boldsymbol{y}_2, \boldsymbol{x}_1)\overline{a}\boldsymbol{x}_1 + f(\boldsymbol{y}_2, \boldsymbol{x}_1)\boldsymbol{w} - f(\boldsymbol{y}_2, \boldsymbol{w})\boldsymbol{x}_1 \\ &= \boldsymbol{y}_2 + \overline{a}\boldsymbol{x}_1 + (a\boldsymbol{x}_1 + \boldsymbol{y}_1 - \boldsymbol{y}_2) - (a + \overline{a})\boldsymbol{x}_1 \\ &= \boldsymbol{y}_1. \end{aligned}$$

Consequently, $\gamma(H_2) = H_1$.

We next claim that $\gamma \in U(V)$, that is, γ is an isometry.

Let $\boldsymbol{u}, \boldsymbol{v} \in V$. Then $f(\gamma(\boldsymbol{u}), \gamma(\boldsymbol{v})) =$

$$f(\boldsymbol{u}+f(\boldsymbol{u},\boldsymbol{x}_1)\overline{a}\boldsymbol{x}_1+f(\boldsymbol{u},\boldsymbol{x}_1)\boldsymbol{w}-f(\boldsymbol{u},\boldsymbol{w})\boldsymbol{x}_1,\boldsymbol{v}+f(\boldsymbol{v},\boldsymbol{x}_1)\overline{a}\boldsymbol{x}_1+f(\boldsymbol{v},\boldsymbol{x}_1)\boldsymbol{w}-f(\boldsymbol{v},\boldsymbol{w})\boldsymbol{x}_1) =$$

$$f(\boldsymbol{u},\boldsymbol{v}) + af(\boldsymbol{x}_1,\boldsymbol{v})f(\boldsymbol{u},\boldsymbol{x}_1) + f(\boldsymbol{x}_1,\boldsymbol{v})f(\boldsymbol{u},\boldsymbol{w}) - f(\boldsymbol{w},\boldsymbol{v})f(\boldsymbol{u},\boldsymbol{x}_1)+$$
$$\overline{a}f(\boldsymbol{u},\boldsymbol{x}_1)f(\boldsymbol{x}_1,\boldsymbol{v}) + f(\boldsymbol{u},\boldsymbol{x}_1)f(\boldsymbol{w},\boldsymbol{v}) - (a+\overline{a})f(\boldsymbol{u},\boldsymbol{x}_1)f(\boldsymbol{x}_1,\boldsymbol{v}) - f(\boldsymbol{u},\boldsymbol{w})f(\boldsymbol{x}_1,\boldsymbol{v}) =$$
$$f(\boldsymbol{u},\boldsymbol{w}).$$

Suppose $a + \overline{a} = 0$, from which we conclude that $\boldsymbol{w}$ is isotropic. In this case we claim that γ is the product of the transvections $\tau_{\boldsymbol{w},-\frac{1}{a}}$ and $\tau_{-a\boldsymbol{x}_1+\boldsymbol{w},\frac{1}{a}}$. We compute:

$$\begin{aligned}
\tau_{\boldsymbol{w},-\frac{1}{a}}(\boldsymbol{z}) &= \boldsymbol{z} - \frac{1}{a}f(\boldsymbol{z},\boldsymbol{w})\boldsymbol{w} \\
&= \tau_{-a\boldsymbol{x}_1+\boldsymbol{w},\frac{1}{a}}(\boldsymbol{z} - \frac{1}{a}f(\boldsymbol{z},\boldsymbol{w})\boldsymbol{w}) \\
&= \boldsymbol{z} - \frac{1}{a}f(\boldsymbol{z},\boldsymbol{w})\boldsymbol{w} + \frac{1}{a}[f(\boldsymbol{z} - \frac{1}{a}f(\boldsymbol{z},\boldsymbol{w})\boldsymbol{w}, -a\boldsymbol{x}_1 + \boldsymbol{w})(-a\boldsymbol{x}_1 + \boldsymbol{w}) \\
&= \boldsymbol{z} - \frac{1}{a}f(\boldsymbol{z},\boldsymbol{w})\boldsymbol{w} + \frac{1}{a}[af(\boldsymbol{z},\boldsymbol{x}_1) + f(\boldsymbol{z},\boldsymbol{w})](-a\boldsymbol{x}_1 + \boldsymbol{w}) \\
&= \boldsymbol{z} - \frac{1}{a}f(\boldsymbol{z},\boldsymbol{w})\boldsymbol{w} + [f(\boldsymbol{z},\boldsymbol{x}_1) + \frac{1}{a}f(\boldsymbol{z},\boldsymbol{w})](-a\boldsymbol{x}_1 + \boldsymbol{w}) \\
&= \boldsymbol{z} - \frac{1}{a}f(\boldsymbol{z},\boldsymbol{w})\boldsymbol{w} - af(\boldsymbol{z},\boldsymbol{x}_1)\boldsymbol{x}_1 + f(\boldsymbol{z},\boldsymbol{x}_1)\boldsymbol{w} - f(\boldsymbol{z},\boldsymbol{w})\boldsymbol{x}_1 \\
&\quad + \frac{1}{a}f(\boldsymbol{z},\boldsymbol{w})\boldsymbol{w} \\
&= \boldsymbol{z} - af(\boldsymbol{z},\boldsymbol{x}_1)\boldsymbol{x}_1 + f(\boldsymbol{z},\boldsymbol{x}_1)\boldsymbol{w} - f(\boldsymbol{z},\boldsymbol{w})\boldsymbol{x}_1 \\
&= \boldsymbol{z} + \overline{a}f(\boldsymbol{z},\boldsymbol{x}_1)\boldsymbol{x}_1 + f(\boldsymbol{z},\boldsymbol{x}_1)\boldsymbol{w} - f(\boldsymbol{z},\boldsymbol{w})\boldsymbol{x}_1 \\
&= \gamma(\boldsymbol{z}).
\end{aligned}$$

Since γ is a product of transvections, $\gamma \in \Omega(V)$.

It remains to consider the case that $a+\overline{a} \neq 0$. In this case $\gamma = \rho_2\rho_1$ where $\rho_1 = \rho_{\boldsymbol{w},\overline{a}a^{-1}}$ and $\rho_2 = \rho_{\overline{a}\boldsymbol{x}_1+\boldsymbol{w},-\overline{a}a^{-1}}$. As in the above case this can be established by computing the image of an arbitrary $\boldsymbol{z}$ under $\rho_2\rho_1$.

Since $\mathbb{F} \neq \mathbb{F}_4$, there exists an element $b \in \mathbb{E}, b \neq 0, 1$. Set $c = \frac{(1-b)a}{b(a+\overline{a}}$. Since $c\overline{c}(a + \overline{a}) \in \mathbb{E}$, there exists $d \in \mathbb{F}$ such that $d + \overline{d} = c\overline{c}(a + \overline{a})$. Set $\boldsymbol{w}' = d\boldsymbol{x}_1 + \boldsymbol{y}_1 + c\boldsymbol{w}$. We claim that $\boldsymbol{w}'$ is isotropic and that $f(\boldsymbol{x}_1, \boldsymbol{w}') = 1$ from which it follows that $Span(\boldsymbol{x}_1, \boldsymbol{w}')$ is a hyperbolic plane.

$$\begin{aligned}
f(\boldsymbol{w}',\boldsymbol{w}') &= f(d\boldsymbol{x}_1+\boldsymbol{y}_1+\boldsymbol{w}, d\boldsymbol{x}_1+\boldsymbol{y}_1+\boldsymbol{w}) \\
&= df(\boldsymbol{x}_1,\boldsymbol{y}_1)+\overline{d}f(\boldsymbol{y}_1,\boldsymbol{x}_1)+c\overline{c}f(\boldsymbol{w},\boldsymbol{w}) \\
&= d+\overline{d}-c\overline{c}(a+\overline{a}) \\
&= 0.
\end{aligned}$$

$$\begin{aligned}
f(\boldsymbol{x}_1,\boldsymbol{w}') &= f(\boldsymbol{x}_1, d\boldsymbol{x}_1+\boldsymbol{y}_1+c\boldsymbol{w}) \\
&= f(\boldsymbol{x}_1,\boldsymbol{y}_1) \\
&= 1.
\end{aligned}$$

Now define Ψ by

$$\Psi(\boldsymbol{z}) = \boldsymbol{z} - f(\boldsymbol{z},\boldsymbol{x}_1)b\boldsymbol{w}' - f(\boldsymbol{z},\boldsymbol{w}')(\frac{b}{b-1})\boldsymbol{x}_1.$$

Since Ψ is the identity on Span$(\boldsymbol{x}_1,\boldsymbol{w}')^\perp$, to show that Ψ is in $U(V)$ it suffices to prove that the restriction of Ψ to Span$(\boldsymbol{x}_1,\boldsymbol{w}')$ is an isometry. We compute $\Psi(\boldsymbol{x}_1)$ and $\Psi(\boldsymbol{w}')$:

$$\begin{aligned}
\Psi(\boldsymbol{x}_1) &= \boldsymbol{x}_1 - f(\boldsymbol{x}_1,\boldsymbol{x}_1)b\boldsymbol{w}' - f(\boldsymbol{x}_1,\boldsymbol{w}')(\frac{b}{b-1})\boldsymbol{x}_1 \\
&= \frac{1}{1-b}\boldsymbol{x}_1
\end{aligned}$$

$$\begin{aligned}
\Psi(\boldsymbol{w}') &= \boldsymbol{w}' - f(\boldsymbol{w}',\boldsymbol{x}_1)b\boldsymbol{w}' - f(\boldsymbol{w}',\boldsymbol{w}')(\frac{b}{b-1})\boldsymbol{x}_1 \\
&= \boldsymbol{w}' - b\boldsymbol{w}' \\
&= (1-b)\boldsymbol{w}'.
\end{aligned}$$

We have therefore shown that Ψ takes the hyperbolic pair $(\boldsymbol{x}_1,\boldsymbol{w}')$ to the hyperbolic pair $(\frac{1}{1-b}\boldsymbol{x}_1,(1-b)\boldsymbol{w}')$. Therefore, Ψ is not only in $U(V)$, but in $SU(V)$. Since Span$(\boldsymbol{x}_1,\boldsymbol{w}')$ is a hyperbolic plane, $\Psi \in \Omega(V)$. By a straightforward computation we have $\Psi(\boldsymbol{w}) = \overline{a}\boldsymbol{x}_1+\boldsymbol{w}$. Consequently, $\Psi\rho_1^{-1}\Psi^{-1} = \Psi\rho_{\boldsymbol{w},-\overline{a}a^{-1}}\Psi^{-1} = \rho_{\overline{a}\boldsymbol{x}_1+\boldsymbol{w},-\overline{a}a^{-1}} = \rho_2$. Therefore $\rho_2\rho_1 = \Psi\rho_1^{-1}\Psi^{-1}\rho_1$. Since $\Omega(V)$ is normal in $SU(V)$ and $\Psi \in \Omega(V)$, we conclude that $\rho_2\rho_1 \in \Omega(V)$.

Corollary 11.16 *Let (V,f) be a finite-dimensional, non-degenerate, isotropic unitary space over the field $\mathbb{F} \neq \mathbb{F}_4$. Assume $\boldsymbol{x},\boldsymbol{y} \in V$ with $f(\boldsymbol{x},\boldsymbol{x}) = f(\boldsymbol{y},\boldsymbol{y}) \neq 0$. Then there exists $\gamma \in \Omega(V)$ such that $\gamma(\boldsymbol{x}) = \boldsymbol{y}$.*

Proof *Set $f(\boldsymbol{x},\boldsymbol{x}) = c$ and choose $b \in \mathbb{F}$ such that $b+\overline{b} = c$. Let $(\boldsymbol{u},\boldsymbol{v})$ be a hyperbolic pair. Then $f(a\boldsymbol{u}+\boldsymbol{v}, a\boldsymbol{u}+\boldsymbol{v}) = b+\overline{b} = c$. By Theorem (8.12) there is an isometry T of V such that $T(\boldsymbol{x}) = a\boldsymbol{u}+\boldsymbol{v}$. Then $\boldsymbol{x} \in H_1 = Span(T^{-1}(\boldsymbol{u}), T^{-1}(\boldsymbol{v}))$. In a similar fashion there is a hyperbolic plane H_2 such that $\boldsymbol{y} \in H$. By Theorem (11.26) there is a $\tau_1 \in \Omega(V)$ such that $\tau_1(H_1) = H_2$. By Lemma (11.35), there is a τ_2 such that τ_2 restricted to $H_2^{\perp}$ is the identity, τ_2 restricted to H_2 is in $SU(H_2)$, and $\tau_2(\tau_1(\boldsymbol{x})) = \boldsymbol{y}$. However, by Theorem (11.25) and Remark (11.8), τ_2 restricted to H_2 is in $\Omega(H_2)$, whence $\tau_2 \in \Omega(V)$. Then $\tau = \tau_2\tau_1$ is the required isometry.*

We can now prove the following generation result:

Theorem 11.27 *Assume (V, f) is a finite-dimensional, non-degenerate, isotropic unitary space over the field $\mathbb{F} \neq \mathbb{F}_4$. Then $SU(V) = \Omega(V)$.*

Proof *The proof is by induction on $n = dim(V)$ for $n \geq 2$. The base case, $n = 2$, holds by Theorem (11.25) and Remark (11.8). Assume $n \geq 3$ and the result holds for spaces of dimension $n-1$. Let $T \in SU(V)$ and let $\boldsymbol{x}$ be a anisotropic vector. Set $\boldsymbol{y} = T(\boldsymbol{x})$. Then $f(\boldsymbol{y},\boldsymbol{y}) = f(\boldsymbol{x},\boldsymbol{x})$. By Corollary (11.16) there exists $\tau \in \Omega(V)$ such that $\tau(\boldsymbol{x}) = \boldsymbol{y}$. Set $S = \tau^{-1}T$. Then $T \in SU(V)$ and $S(\boldsymbol{x}) = \boldsymbol{x}$. Then S leaves $\boldsymbol{x}^{\perp}$ invariant and the restriction, $\widehat{s}$, of S to $\boldsymbol{x}^{\perp}$ is in $SU(\boldsymbol{x}^{\perp})$. By the induction hypothesis, $\widehat{S} \in \Omega(\boldsymbol{x}^{\perp})$. By Lemma(11.33) it follows that $S \in \Omega(V)$, whence $T = \tau S \in \Omega(V)$.*

We now deal with the case that (V, f) is a non-degenerate, finite-dimensional unitary space over $\mathbb{F}_4$. We will denote the elements of $\mathbb{F}_4$ by $0, 1, \omega$, and $\omega^2 = \omega + 1$ (so that $\omega^3 = 1$).

Remark 11.9 *By Exercise 8 of Section (9.2) if (V, f) is a non-degenerate unitary space of dimension n over a finite field, then the Witt index of (V, f) is $\lfloor \frac{n}{2} \rfloor$.*

Definition 11.14 *If (V, f) is a non-degenerate unitary space of dimension $2n$ and Witt index n, then a basis $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_n)$ such that $f(\boldsymbol{x}_i, \boldsymbol{x}_j) = f(\boldsymbol{x}_i, \boldsymbol{y}_j) = f(\boldsymbol{y}_i, \boldsymbol{y}_j) = 0$ for $i \neq j$ and $f(\boldsymbol{x}_i, \boldsymbol{y}_i) = 1$ for all i is a* **hyperbolic basis***.*

We will need the following simple result later when we have to prove that $\Omega(V)$ is transitive on anisotropic vectors. We leave it as an exercise.

Lemma 11.36 *Let (V, f) be a hyperbolic plane over $\mathbb{F}_4$. Then $SU(V) = \Omega(V)$ is transitive on the six anisotropic vectors of V.*

Lemma 11.37 *Let (V, f) be a non-degenerate three-dimensional unitary space over $\mathbb{F}_4$. Then $\Omega(V)$ is transitive on the set of isotropic vectors.*

Proof *By Corollary (11.15), $\Omega(V)$ is transitive on the set $I_1(V)$ of one-dimensional subspaces spanned by an isotropic vector. It therefore suffices to show for $\boldsymbol{v}$ isotropic that there is $\tau \in \Omega(V)$ such that $\tau(\boldsymbol{v}) = \omega\boldsymbol{v}$. Let $\mathcal{B} = (\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3)$ be a basis for V such that $(\boldsymbol{x}_1, \boldsymbol{x}_3)$ is a hyperbolic pair and $\boldsymbol{x}_1 \perp \boldsymbol{x}_2$ and $\boldsymbol{x}_2 \perp \boldsymbol{x}_3$. Note that for any anisotropic vector $\boldsymbol{x}, f(\boldsymbol{x}, \boldsymbol{x}) = 1$.*

In addition to $\boldsymbol{x}_1$ and $\boldsymbol{x}_3$, the following vectors are isotropic: $\boldsymbol{y}_1 = \boldsymbol{x}_1 + \boldsymbol{x}_2 + \omega\boldsymbol{x}_3$ and $\boldsymbol{y}_2 = \omega\boldsymbol{x}_1 + \boldsymbol{x}_2 + \boldsymbol{x}_3$ (there are five others but we do not require them). Let $\tau_1 = \tau_{\boldsymbol{x}_1,1}, \tau_2 = \tau_{\boldsymbol{x}_3,1}, \tau_3 = \tau_{\boldsymbol{y}_1,1}$ and $\tau_4 = \tau_{\boldsymbol{y}_2,1}$. A simple calculation gives the following:

$$\mathcal{M}_{\tau_1}(\mathcal{B}, \mathcal{B}) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \mathcal{M}_{\tau_2}(\mathcal{B}, \mathcal{B}) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix},$$

$$\mathcal{M}_{\tau_3}(\mathcal{B}, \mathcal{B}) = \begin{pmatrix} \omega^2 & 1 & 1 \\ \omega & 0 & 1 \\ 1 & \omega^2 & \omega \end{pmatrix}, \mathcal{M}_{\tau_4}(\mathcal{B}, \mathcal{B}) = \begin{pmatrix} \omega^2 & \omega & 1 \\ 1 & 0 & \omega^2 \\ 1 & 1 & \omega. \end{pmatrix}$$

Set $\zeta = \tau_1\tau_2\tau_3\tau_4$. Then $\mathcal{M}_\zeta(\mathcal{B}, \mathcal{B}) = \begin{pmatrix} \omega & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega \end{pmatrix}$. Thus, $\zeta \in \Omega(V)$ and $\zeta(\boldsymbol{v}) = \omega\boldsymbol{v}$ for every vector $\boldsymbol{v} \in V$.

Corollary 11.17 *Let (V, f) be a non-degenerate unitary space over $\mathbb{F}_4$ of dimension $n \geq 3$. Let $(\boldsymbol{u}, \boldsymbol{v})$ be a hyperbolic pair. Then there exists an operator τ in $\Omega(V)$ such that $\tau(\boldsymbol{u}) = \omega\boldsymbol{u}, \tau(\boldsymbol{v}) = \omega\boldsymbol{v}$.*

We leave this as an exercise.

Corollary 11.18 *Let (V, f) be a non-degenerate unitary space over $\mathbb{F}_4$ of dimension $n \geq 3$. Let $\boldsymbol{u}, \boldsymbol{v}$ be isotropic vectors. Then there exists $\tau \in \Omega(V)$ such that $\tau(\boldsymbol{u}) = \boldsymbol{v}$.*

This is left as an exercise.

Lemma 11.38 *Let (V, f) be a non-degenerate four-dimensional unitary space over $\mathbb{F}_4$. Then the following hold:*

i) The cardinality of $I_1(V)$ is 45.

ii) Each element of $I_1(V)$ is contained in exactly three elements of $I_2(V)$.

iii) Each element of $I_2(V)$ contains five elements of $I_1(V)$.

iv) For $X \in I_1(V)$, the cardinality of $\Delta(X)$ is 12 and the cardinality of $\Gamma(X)$ is 32.

These are fairly routine computations which we leave as exercises.

Lemma 11.39 *Let (V, f) be a non-degenerate four-dimensional unitary space over $\mathbb{F}_4$. Let $\mathcal{B} = (\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{y}_2, \boldsymbol{y}_1)$ be a basis of V such that $f(\boldsymbol{x}_1, \boldsymbol{x}_2) = f(\boldsymbol{x}_1, \boldsymbol{y}_2) = f(\boldsymbol{x}_2, \boldsymbol{y}_1) = f(\boldsymbol{y}_1, \boldsymbol{y}_2) = 0; f(\boldsymbol{x}_1, \boldsymbol{y}_1) = f(\boldsymbol{x}_2, \boldsymbol{y}_2) = 1$. Then a vector $a\boldsymbol{x}_1 + b\boldsymbol{x}_2 + c\boldsymbol{y}_2 + \boldsymbol{y}_1$ is isotropic if and only if $Tr(a) + Tr(b\overline{c}) = 0$.*

This is a straightforward computation and left as an exercise.

Lemma 11.40 *Assume the hypotheses of Lemma (11.39). Let $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{F}_4^2$ and $c \in \mathbb{F}_4$. Assume the operator T has matrix $A = \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & d \\ 0 & 0 & 1 & e \\ 0 & 0 & 0 & 1 \end{pmatrix}$ with respect to $\mathcal{B}$. Then $T \in SU(V)$ if and only if $e = \overline{a}, d = \overline{b}$, and $Tr(c) + a\overline{b} + \overline{a}b = 0$.*

Proof *Let J be the matrix of f with respect to the basis $\mathcal{B}$, so that $J = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$. Then $T \in SU(V)$ if and only if $A^{tr} J \overline{A} = J$. The conditions follow from this.*

Let $a, b, c \in \mathbb{F}_4$ satisfy $a\overline{b} + \overline{a}b + c + \overline{c} = 0$. Denote by $M(a, b, c)$ the matrix $\begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & \overline{b} \\ 0 & 0 & 1 & \overline{a} \\ 0 & 0 & 0 & 1 \end{pmatrix}$ and by $T(a, b, c)$ the operator on (V, f), which has matrix $M(a, b, c)$ with respect to $\mathcal{B}$. By Lemma (11.40), $T(a, b, c) \in SU(V)$. Also denote by $A(\boldsymbol{x}_1)$ the collection of all such operators. This is a subgroup of $SU(V)$ and every $T \in A(\boldsymbol{x}_1)$ fixes $\boldsymbol{x}_1$.

Remark 11.10 *The order of $A(\boldsymbol{x}_1)$ is 32, a and b can be chosen arbitrarily from $\mathbb{F}_4$ and once such a choice has been made there are two possibilities for c.*

Lemma 11.41 *Continue with the hypotheses of Lemma (11.39). Assume* $\boldsymbol{y}$ *is an isotropic vector and* $f(\boldsymbol{x}_1, \boldsymbol{y}) = 1$*. Then there is a unique operator* $T \in A(\boldsymbol{x}_1)$ *such that* $T(\boldsymbol{y}_1) = \boldsymbol{y}$*.*

Proof *Let* $\boldsymbol{y} = \boldsymbol{v} + d\boldsymbol{y}_1$ *where* $\boldsymbol{v} \in \boldsymbol{x}_1^{\perp}$*. Since* $f(\boldsymbol{x}_1, \boldsymbol{y}) = 1$ *it follows that* $d = 1$*. Write* $\boldsymbol{v} = a\boldsymbol{x}_1 + b\boldsymbol{x}_2 + c\boldsymbol{y}_2$*. Since* $\boldsymbol{y}$ *is isotropic it follows from Lemma (11.39) that* $a\overline{b} + \overline{a}b + c + \overline{c} = 0$*. Then* $T(a, b, c)$ *is the unique operator* $T \in A(\boldsymbol{x}_1)$ *such that* $T(\boldsymbol{y}_1) = \boldsymbol{y}$*.*

Theorem 11.28 *Let* (V, f) *be a non-degenerate four-dimensional unitary space over* $\mathbb{F}_4$*. Let* $(\boldsymbol{u}_1, \boldsymbol{v}_1)$ *and* $(\boldsymbol{u}_2, \boldsymbol{v}_2)$ *be hyperbolic pairs. Then there exists* $\tau \in \Omega(V)$ *such that* $\tau(\boldsymbol{u}_1) = \boldsymbol{u}_2$ *and* $\tau(\boldsymbol{v}_1) = \boldsymbol{v}_2$*.*

Proof *Since* $\Omega(V)$ *is transitive on isotropic vectors we can assume that* $\boldsymbol{u}_1 = \boldsymbol{u}_2 = \boldsymbol{x}_1$*. It then suffices to show that there exists* τ *in* $\Omega(V)$ *such that* $\tau(\boldsymbol{x}_1) = \boldsymbol{x}_1$ *and* $\tau(\boldsymbol{v}_1) = \boldsymbol{v}_2$*. By Lemma (11.41) it suffices to show that* $A(\boldsymbol{x}_1)$ *is contained in* $\Omega(V)$*. We exhibit below five explicit generators of* $A(\boldsymbol{x}_1)$ *which are transparently in* $\Omega(V)$ *(each will be a transvection or a product of two transvections).*

Let $T_1 = \tau_{\boldsymbol{y}_2}\tau_{\boldsymbol{x}_1+\boldsymbol{y}_2}$*. The matrix of* T_1 *with respect to* $\mathcal{B}$ *is* $\begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

Let $T_2 = \tau_{\boldsymbol{x}_2+\boldsymbol{y}_2}\tau_{\boldsymbol{x}_1+\boldsymbol{x}_2-\boldsymbol{y}_2}$*. The matrix of* T_2 *is* $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

Let $T_3 = \tau_{\boldsymbol{x}_2+\boldsymbol{y}_2}\tau_{\omega\boldsymbol{x}_1+\boldsymbol{x}_2+\boldsymbol{y}_2}$*. The matrix of* T_3 *is* $\begin{pmatrix} 1 & \omega & \omega & 1 \\ 0 & 1 & 0 & \omega^2 \\ 0 & 0 & 1 & \omega^2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

Let $T_4 = \tau_{\boldsymbol{x}_2}\tau_{\omega\boldsymbol{x}_1-\boldsymbol{x}_2}$*. The matrix of* T_4 *is* $\begin{pmatrix} 1 & 0 & \omega & 1 \\ 0 & 1 & 0 & \omega^2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

Let $T_5 = \tau_{\boldsymbol{x}_1}$*. The matrix of* T_5 *is* $\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

We are almost ready to prove: if (V, f) is a non-degenerate unitary space of dimension $n \geq 4$ over $\mathbb{F}_4$, then $\Omega(V) = SU(V)$. Before doing so we require one more result.

Lemma 11.42 *Let (V, f) be a non-degenerate unitary space of dimension $n \geq 4$ over $\mathbb{F}_4$. Then $\Omega(V)$ is transitive on the set of anisotropic vectors.*

Proof *Assume $\boldsymbol{x}, \boldsymbol{y}$ are anisotropic vectors. If $f(\boldsymbol{x}, \boldsymbol{y}) = 0$, then $X = Span(\boldsymbol{x}, \boldsymbol{y})$ is a hyperbolic plane. By Lemma (11.36), there is a τ such that $\tau_{|X^\perp} = I_{X^\perp}, \tau_{|X} \in SU(X)$ such that $\tau(\boldsymbol{x}) = \boldsymbol{y}$. By Theorem (11.28), it follows that $\tau_{|X} \in \Omega(X)$. Then by Lemma (11.33), we have $\tau \in \Omega(V)$. Thus, we may assume that $f(\boldsymbol{x}, \boldsymbol{y}) \neq 0$.*

Note that $\boldsymbol{x}^\perp$ is a non-degenerate three-dimensional space and so has Witt index one. Therefore, $\boldsymbol{x}^\perp \cap \boldsymbol{y}^\perp$ is not totally isotropic. Choose an anisotropic vector $\boldsymbol{z} \in \boldsymbol{x}^\perp \cap \boldsymbol{y}^\perp$. By the first paragraph there exists $\tau_1, \tau_2 \in \Omega(V)$ such that $\tau_1(\boldsymbol{x}) = \boldsymbol{z}, \tau_2(\boldsymbol{z}) = \boldsymbol{y}$. Set $\tau = \tau_2\tau_1$. Then $\tau \in \Omega(V)$ and $\tau(\boldsymbol{x}) = \boldsymbol{y}$.

Theorem 11.29 *Let (V, f) be a non-degenerate unitary space of dimension $n \geq 4$ over $\mathbb{F}_4$, then $\Omega(V) = SU(V)$.*

Proof *The proof is by induction on $n \geq 4$. Suppose $n = 4$. Let $T \in SU(V)$ and $(\boldsymbol{u}, \boldsymbol{v})$ be a hyperbolic pair. Then $(T(\boldsymbol{u}), T(\boldsymbol{v}))$ is a hyperbolic pair. By Theorem (11.28), there is a $\tau \in \Omega(V)$ such that $\tau(\boldsymbol{u}) = T(\boldsymbol{u}), \tau(\boldsymbol{v}) = T(\boldsymbol{v})$. Set $U = Span(\boldsymbol{u}, \boldsymbol{v})$ and $S = \tau^{-1}T$. Then S restricted to U is I_U, S leaves $U^\perp$ invariant, and $S_{|U^\perp} \in SU(U^\perp)$. By Theorem (11.25) and Remark (11.8), $S \in \Omega(U^\perp)$ and then by Lemma (11.33), $S \in \Omega(V)$. Consequently, $T = \tau S \in \Omega(V)$.*

Now assume $n \geq 4$ and we have shown that $\Omega(U) = SU(U)$ for a non-degenerate unitary space (U, g) of dimension n over $\mathbb{F}_4$ and that (V, f) is a non-degenerate unitary space of dimension $n+1$ over $\mathbb{F}_4$. Let $T \in SU(V)$ and let $\boldsymbol{x}$ be an anisotropic vector. Then, of course, $f(T(\boldsymbol{x}), T(\boldsymbol{x})) = f(\boldsymbol{x}, \boldsymbol{x})$. By Lemma (11.42), there is a $\tau \in \Omega(V)$ such that $\tau(\boldsymbol{x}) = T(\boldsymbol{x})$. Set $S = \tau^{-1}T$. Then $S(\boldsymbol{x}) = \boldsymbol{x}$. Consequently, S leaves $\boldsymbol{x}^\perp$ invariant and $S_{|\boldsymbol{x}^\perp} \in SU(\boldsymbol{x}^\perp)$. By the inductive hypothesis, $S \in \Omega(\boldsymbol{x}^\perp)$. By Lemma (11.33), $S \in \Omega(V)$. Consequently, $T = \tau S \in \Omega(V)$.

We can now determine when $SU(V)$ is a perfect group:

Theorem 11.30 *Assume $(n, \mathbb{F})$ is not one of $(2, \mathbb{F}_4), (2, \mathbb{F}_9), (3, \mathbb{F}_4)$ and (V, f) is a non-degenerate isotropic unitary space of dimension n over $\mathbb{F}$. Then $SU(V)$ is perfect.*

Proof *Assume $(n, \mathbb{F})$ is not one of $(2, \mathbb{F}_4), (2, \mathbb{F}_9), (3, \mathbb{F}_4)$. Suppose we can show that there is an isotropic vector $\boldsymbol{x}$ such that commutator subgroup of $SU(V)$ contains $\mathcal{T}_{\boldsymbol{x}} = \{\tau_{\boldsymbol{x},c} | c \in \Lambda\}$. Since $SU(V)'$ is normal in $SU(V)$ and since $SU(V)$ is transitive on the subgroups $\{calT_{\boldsymbol{u}}, \boldsymbol{u}$ isotropic, it will then follow that $SU(V)'$ contains $\Omega(V) = SU(V)$.*

Suppose first that $\mathbb{F}$ has greater than 9 elements. Let $X = Span(\boldsymbol{x}, \boldsymbol{y})$ be a hyperbolic plane with $(\boldsymbol{x}, \boldsymbol{y})$ a hyperbolic pair. Let $S(X)$ consist of those T such that the restriction to $X^\perp$ is the identity on $X^\perp$. Then $S(X)$ is isomorphic to $SU(X)$, whence isomorphic to $SL_2(\mathbb{E})$ by Theorem (11.25). This group is perfect and contains $\mathcal{T}_{\boldsymbol{x}}$. By Lemma (11.33), it follows that $SU(V)'$ contains full transvections groups and is therefore perfect.

We will next show if $dim(V) = 3$, then the commutator subgroup of $SU(V)$ contains full transvection subgroups. Let $(\boldsymbol{x}, \boldsymbol{y})$ be a hyperbolic pair and let $\boldsymbol{z} \in \boldsymbol{x}^\perp \cap \boldsymbol{y}^\perp$. Multiplying f by $\frac{1}{f(\boldsymbol{z},\boldsymbol{z})}$, if necessary, we can assume that $f(\boldsymbol{z}, \boldsymbol{z}) = 1$. Then $\mathcal{B} = (\boldsymbol{x}, \boldsymbol{z}, \boldsymbol{y})$ is a basis for V. The matrix of f with respect to $\mathcal{B}$ is $J = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$. Assume $a, b \in \mathbb{F}$ satisfy $b + \overline{b} + a\overline{a} = 0$. Then let $T(a, b)$ be the operator on V such that $\mathcal{M}_{T(a,b)}(\mathcal{B}, \mathcal{B}) = \begin{pmatrix} 1 & a & b \\ 0 & 1 & -\overline{a} \\ 0 & 0 & 1 \end{pmatrix} = M(a, b)$. An easy matrix computation confirms that $M(a, b)^{tr} J\overline{M(a, b)} = M(a, b)^{tr} JM(\overline{a}, \overline{b}) = J$ so that $T(a, b) \in SU(V)$. Suppose also that $c, d \in \mathbb{F}$ and that $d + \overline{d} + c\overline{c} = 0$. Then $T(a, b)T(c, d) = T(a + c, b + d - a\overline{c})$. We can then conclude that $T(a, b)^{-1} = T(-a, \overline{b})$ and, finally, that

$$T(a, b)^{-1}T(c, d)^{-1}T(a, b)T(c, d) = T(0, \overline{a}c - a\overline{c}) = \tau_{\boldsymbol{x}, \overline{a}c - a\overline{c}}.$$

Assume now that the characteristic of $\mathbb{F}$ is not equal to 2. Let $a = 1$ and let c range over $\mathbb{F}$. Then $\overline{a}c - a\overline{c}$ varies over all of Φ. So in this case $SU(V)^\perp$ contains $\mathcal{T}_{\boldsymbol{x}}$ and therefore is perfect.

On the other hand, if the characteristic of $\mathbb{F}$ is 2, let $a = 1$. Then as c varies over $\mathbb{F}$, $c + \overline{c}$ varies over all of $\mathbb{E} = \Phi$. This proves that $SU(V)'$ contains $\mathcal{T}_{|xx}$ and we can conclude that $SU(V)' \subset \Omega(V)$. By an induction argument on $n = dim(V)$, for $n \geq 3$, we conclude that $\Omega(V) \subset SU(V)'$.

Suppose $\mathbb{F} = \mathbb{F}_9$. By Theorem (11.27), $SU(V) = \Omega(V)$. Thus, $\Omega(V) \subset SU(V)' \subset SU(V) = \Omega(V)$. We can therefore conclude that $SU(V)' = SU(V)$ and $SU(V)$ is perfect.

Finally, assume $n \geq 4$ and $\mathbb{F} = \mathbb{F}_4$. By Theorem (11.29) we have $SU(V) = \Omega(V) \subset SU(V)' \subset SU(V)$ and we can again conclude that $SU(V)$ is perfect.

Remark 11.11 *The three excluded cases really are truly exceptions: The group $SU_2(\mathbb{F}_4)$ is isomorphic to $SL_2(\mathbb{F}_2)$, which is isomorphic to the symmetric group S_3. The group $SU_2(\mathbb{F}_9)$ is isomorphic to $SL_2(\mathbb{F}_3)$, has order 24, and is solvable. The group $SU_3(\mathbb{F}_4)$ has order $216 = 2^3 3^3$ and is solvable.*

We now determine the structure of the center of $SU(V)$.

Theorem 11.31 *Let (V, f) be an n-dimensional, non-degenerate, isotropic unitary space. Then $Z(U(V)) = \{cI_V | c \in \Lambda\}$ and $Z(SU(V)) = \{\lambda I_V | c \in \Lambda$ and $\lambda^n = 1\}$.*

Proof *Let $\boldsymbol{v}$ be an isotropic vector and $c \in \Phi$. Since $S\tau_{\boldsymbol{v},c} = \tau_{\boldsymbol{v},c}S$, it follows that S leaves $Ker(\tau_{\boldsymbol{v},c} - I_V) = \boldsymbol{v}^{\perp}$ invariant. Consequently, $S(\boldsymbol{v}) \in Span(\boldsymbol{v})$, that is, $\boldsymbol{v}$ is an eigenvector for S. Since $\boldsymbol{v}$ is arbitrary, for each isotropic vector $\boldsymbol{v}$ there is a scalar $\lambda_{\boldsymbol{v}}$ such that $S(\boldsymbol{v}) = \lambda_{\boldsymbol{v}}\boldsymbol{v}$. Now suppose $\boldsymbol{w}$ is also an isotropic vector. If $\boldsymbol{w}$ is a multiple of $\boldsymbol{v}$ then $\lambda_{\boldsymbol{w}} = \lambda_{\boldsymbol{v}}$; so assume $(\boldsymbol{v}, \boldsymbol{w})$ is linearly independent. If $\boldsymbol{v} \perp \boldsymbol{w}$ then $\boldsymbol{v} + \boldsymbol{w}$ is also isotropic. We then have $\lambda_{\boldsymbol{v}}\boldsymbol{v} + \lambda_{\boldsymbol{w}}\boldsymbol{w} = S(\boldsymbol{v}) + S(\boldsymbol{w}) = S(\boldsymbol{v} + \boldsymbol{w}) = \lambda_{\boldsymbol{v}+\boldsymbol{w}}(\boldsymbol{v} + \boldsymbol{w})$ from which we conclude that $\lambda_{\boldsymbol{v}} = \lambda_{\boldsymbol{v}+\boldsymbol{w}} = \lambda_{\boldsymbol{w}}$. On the other hand, suppose $f(\boldsymbol{v}, \boldsymbol{w}) \neq 0$. Since $\lambda_{\boldsymbol{w}} = \lambda_{c\boldsymbol{w}}$ for any scalar, without loss of generality we may assume that $f(\boldsymbol{v}, \boldsymbol{w}) = 1$. Let $c \in \Phi$. Then $c\boldsymbol{v} + \boldsymbol{w}$ is isotropic. Now $\lambda_{\boldsymbol{v}}(c\boldsymbol{v}) + \lambda_{\boldsymbol{w}}\boldsymbol{w}$ $= S(c\boldsymbol{v}) + S(\boldsymbol{w}) = S(c\boldsymbol{v} + \boldsymbol{w}) = \lambda_{c\boldsymbol{v}+\boldsymbol{w}}(c\boldsymbol{v} + \boldsymbol{w})$ from which we again conclude that $\lambda_{\boldsymbol{w}} = \lambda_{\boldsymbol{v}}$. Thus, there is an element $\lambda \in \mathbb{F}$ such that $S(\boldsymbol{v}) = \lambda\boldsymbol{v}$ for every isotropic vector. Since every anisotropic vector is contained in some hyperbolic plane, it follows that $S(\boldsymbol{x}) = \lambda\boldsymbol{x}$ for every vector $\boldsymbol{x}$ and $S = \lambda I_V$. If $\boldsymbol{x}$ is anisotropic, then $\lambda\overline{\lambda} = f(S(\boldsymbol{x}), S(\boldsymbol{x})) = f(\boldsymbol{x}, \boldsymbol{x})$. Since $f(\boldsymbol{x}, \boldsymbol{x}) \neq 0$ we get $\lambda\overline{\lambda} = 1$.*

We next prove that if $X \in I_1(V)$ then $SU(V)_X = \{T \in SU(V) | S(X) = X\}$ is transitive on $\Gamma(X)$ and $\Delta(X)$ (the latter when the Witt index is at least two).

Lemma 11.43 *Assume (V, f) is an n-dimensional, non-degenerate isotropic unitary space over the field $\mathbb{F}$ with $n \geq 3$ and $n \geq 4$ if $\mathbb{F} = \mathbb{F}_4$. Then the following hold:*

i) If $X, Y, Z \in I_1(V)$ and $X \not\perp Y, X \not\perp Z$, then there exists $S \in SU(V)$ such that $S(X) = X$ and $S(Y) = Z$.

ii) Assume the Witt index of (V, f) is at least two. If $X, Y, Z \in I_1(V)$, $X \perp Y$, and $X \perp Z$, then there exists $S \in SU(V)$ such that $S(X) = X$ and $S(Y) = Z$.

Proof *i) If $\mathbb{F} \neq \mathbb{F}_4$ this was proved in Theorem (11.26). Suppose $\mathbb{F} = \mathbb{F}_4$ so that $n \geq 4$. Now either $X+Y+Z$ is non-degenerate or the radical of $X+Y+Z$ has dimension one, since $X+Y$ is non-degenerate. In either case there exists a non-degenerate subspace U of V containing $X+Y+Z$. Now the result holds by Theorem (11.28).*

ii. Since the Witt index is at least two, it follows that $n \geq 4$. Let $X = Span(\boldsymbol{x})$ and let $\boldsymbol{w}$ be an isotropic vector such that $f(\boldsymbol{x}, \boldsymbol{w}) = 1$. Set $W = Span(\boldsymbol{x}, \boldsymbol{w})^{\perp}$. Let $Y' = (X+Y) \cap \boldsymbol{w}^{\perp}$ and $Z' = (X+Z) \cap \boldsymbol{w}^{\perp}$. Then $Y', Z' \in I_1(W)$. By Lemma (11.15), $\Omega(W) = SU(W)$ and there is an $\gamma \in SU(W)$ such that $\gamma(Y') = Z'$. Extend γ to an element of $SU(V)$ by defining $\gamma_{|W^{\perp}} = I_{W^{\perp}}$. We may therefore assume that $Y \subset X+Z = X+Z'$. Let $Z' = Span(\boldsymbol{z})$ where $f(\boldsymbol{z}, \boldsymbol{w}) = 1$. Then there are scalars $a, b \in \mathbb{F}$ such that $Y = Span(a\boldsymbol{x} + \boldsymbol{z}), Z = Span(b\boldsymbol{x} + \boldsymbol{z})$. We show that there are operators $\gamma_a, \gamma_b \in SU(V)$ such that $\gamma_a(\boldsymbol{x}) = \boldsymbol{x}$ and $\gamma_a(\boldsymbol{z}) = a\boldsymbol{x} + \boldsymbol{z}, \gamma_b(\boldsymbol{z}) = b\boldsymbol{x} + \boldsymbol{z}$ and then $\gamma_b\gamma_a^{-1}$ is the desired S. Since W is non-degenerate, there exists an isotropic vector $\boldsymbol{u} \in W$ such that $f(\boldsymbol{z}, \boldsymbol{u}) = 1$. Let $c \in \mathbb{F}$ and choose any $\delta \in \Phi$. Set $\gamma_c = \tau_{\boldsymbol{u},-\delta}\tau_{\frac{c}{\delta}\boldsymbol{x}+\boldsymbol{u},\delta}$. Then

$$\begin{aligned}
\gamma_c(\boldsymbol{z}) &= \tau_{\boldsymbol{u},-\delta}\tau_{\frac{c}{\delta}\boldsymbol{x}+\boldsymbol{u},\delta}(\boldsymbol{z}) \\
&= \tau_{\boldsymbol{u},-\delta}(\boldsymbol{z} + \delta f(\boldsymbol{z}, \frac{c}{\delta}\boldsymbol{x} + \boldsymbol{u})(\frac{c}{\delta}\boldsymbol{x} + \boldsymbol{u}) \\
&= \tau_{\boldsymbol{u},-\delta}(\boldsymbol{z} + \delta(\frac{c}{\delta + \boldsymbol{u}})) \\
&= \tau_{\boldsymbol{u},-\delta}(\boldsymbol{z} + c\boldsymbol{x} + \delta\boldsymbol{u}) \\
&= \boldsymbol{z} + c\boldsymbol{x} + \delta\boldsymbol{u} - \delta f(\boldsymbol{z} + c\boldsymbol{x} + \delta\boldsymbol{u}, \boldsymbol{u})\boldsymbol{u} \\
&= \boldsymbol{z} + c\boldsymbol{x} + \delta\boldsymbol{u} - \delta\boldsymbol{u} \\
&= \boldsymbol{z} + c\boldsymbol{x}.
\end{aligned}$$

As an immediate consequence of part i) of Lemma (11.43) we have:

Corollary 11.19 *Let (V, f) is an n-dimensional, non-degenerate unitary space over the field $\mathbb{F}$ with Witt index one. Then $SU(V)$ is doubly transitive on $I_1(V)$. In particular, if the Witt index is one, then the action of $SU(V)$ on $I_1(V)$ is primitive.*

Lemma 11.44 *Assume (V, f) is an n-dimensional, non-degenerate unitary space over the field $\mathbb{F}$ with Witt index of at least two. Then the following hold:*

i) If $X \in I_1(V)$ and $Y \in \Delta(X)$, then there exists $W \in \Delta(Y) \cap \Gamma(X)$.

ii) If $X \in I_1(V)$ and $Y \in \Gamma(X)$, then there exists $W \in \Gamma(Y) \cap \Delta(X)$.

Proof *i) Let $U \in \Gamma(X)$ so that $X + U$ is a hyperbolic plane. Since the Witt index of (V, f) is at least two, $X^\perp \cap U^\perp$ is non-degenerate and isotropic. Let $Z \in I_1(X^\perp \cap U^\perp)$. By part ii) of Lemma (11.43), there exists $S \in SU(V)$ such that $S(X) = X$ and $S(Z) = Y$. Set $W = S(U)$. Then $X \not\perp W$ and $Y \not{p}erpW$.*

ii) Let $X = Span(\boldsymbol{x})$ and $Y = Span(\boldsymbol{y})$. Since $X \not\perp Y, U = X + Y$ is a hyperbolic plane. Since the Witt index of (V, f) is at least two, $U^\perp$ is isotropic. Let $Z = Span(\boldsymbol{z})$ be in $U^\perp$. Then $\boldsymbol{z}+\boldsymbol{y}$ is isotropic and $f(\boldsymbol{x}, \boldsymbol{z}+\boldsymbol{y}) = f(\boldsymbol{x}, \boldsymbol{y}) \neq 0$. Thus, $W = Span(\boldsymbol{z} + \boldsymbol{y}) \in \Gamma(X) \cap \Delta(Y)$.

We can use part ii) of Lemma (11.43) and Lemma (11.44) to show that, in general, the action of $SU(V)$ on $I_1(V)$ is primitive.

Theorem 11.32 *Assume (V, f) is an n-dimensional, non-degenerate unitary space over the field $\mathbb{F}$ with Witt index at least two. Then $SU(V)$ is primitive in its action on $I_1(V)$.*

Proof *Let $X, Y \in I_1(V)$ and let B be a subset of $I_1(V)$ which contains X and Y. Assume for any $\sigma \in SU(V)$ that $\sigma(B) = B$ or $\sigma(B) \cap B = \emptyset$. We prove that $B = I_1(V)$. Assume first that $Y \in \Delta(X)$ and let Z be in $\Delta(X)$. By part ii) of Lemma (11.43) there is an $S \in SU(V)$ such that $S(X) = X$ and $S(Y) = Z$. Then $X \in S(B)$ so that $S(B) = B$. Then $Z = S(Y) \in S(B) = B$. Thus, $\Delta(X)$ is contained in B. Similarly, $\Delta(Y)$ is contained in B. By part i) Lemma (11.44), there is a $W \in \Delta(Y) \cap \Gamma(X)$. But then by arguments similar to the above, $\Gamma(X) \subset B$, and then $B = I_1(V)$. If $Y \in \Gamma(X)$, then a similar argument yields $B = I_1(V)$.*

We can now prove our main theorem.

Theorem 11.33 *Let (V, f) be an n-dimensional, non-degenerate isotropic unitary space over the field $\mathbb{F}$ and assume that $(n, \mathbb{F})$ is not one of $(2, \mathbb{F}_4), (2, \mathbb{F}_9)$ or $(3, \mathbb{F}_4)$. Then $PSU(V) = SU(V)/Z(SU(V))$ is a simple group.*

Proof *It follows from Theorem (11.31) that the kernel of the action of $SU(V)$ on $I_1(V)$ is $Z(SU(V))$. We can then conclude that the action of $PSU(V) = SU(V)/Z(SU(V))$ on $I_1(V)$ is faithful. By Theorem (11.19) and Theorem (11.32), the action of $PSU(V)$ on $I_1(V)$ is primitive. By Theorem (11.30), $SU(V)$, consequently, $PSU(V)$ is a perfect group. Denote the image of an element S of $SU(V)$ in $PSU(V)$ by $\widehat{S}$. For $X = Span(\boldsymbol{x}) \in I_1(V)$ let $\widehat{\mathcal{T}_{\boldsymbol{x}}} = \{\widehat{\tau_{\boldsymbol{x},c}} | c \in \Phi\}$. Then $\widehat{\mathcal{T}_{\boldsymbol{x})}}$ is a normal Abelian subgroup of $PSU(V)_X$ and the conjugates of $\widehat{\mathcal{T}_{\boldsymbol{x}}}$ generate $PSU(V)$. Therefore, by Iwasawa's theorem $PSU(V)$ is simple.*

Exercises

1. Let (V, f) be a non-degenerate isotropic unitary space and W a non-degenerate isotropic subspace. Assume T is an operator of V, which leaves both W and $W^\perp$ invariant. Further, assume T restricted to $W^\perp$ is the identity on $W^\perp$ and W restricted to W is in $\Omega(W)$. Then $T \in \Omega(V)$.

2. Let (V, f) be a hyperbolic plane over $\mathbb{F}_4$. Then $SU(V) = \Omega(V)$ is transitive on the six anisotropic vectors of V.

3. Let (V, f) be a non-degenerate unitary space over $\mathbb{F}_4$ of dimension $n \geq 3$. Let $(\boldsymbol{u}, \boldsymbol{v})$ be a hyperbolic pair. Then there exists a $\tau \in \Omega(V)$ such that $\tau(\boldsymbol{u}) = \omega \boldsymbol{u}$ and $\tau(\boldsymbol{v}) = \omega \boldsymbol{v}$.

4. Let (V, f) be a non-degenerate unitary space over $\mathbb{F}_4$ of dimension $n \geq 3$. Let $\boldsymbol{u}, \boldsymbol{v}$ be isotropic vectors. Then there exists $\tau \in \Omega(V)$ such that $\tau(\boldsymbol{u}) = \boldsymbol{v}$.

In Exercises 5–8 let (V, f) be a non-degenerate four-dimensional unitary space over $\mathbb{F}_4$.

5. Prove that the cardinality of $I_1(V)$ is 45.

6. Prove that each element of $I_1(V)$ is contained in exactly three elements of $I_2(V)$.

7. Prove that each element of $I_2(V)$ contains five elements of $I_1(V)$.

8. Prove if $X \in I_1(V)$, then the cardinality of $\Delta(X)$ is 12 and the cardinality of $\Gamma(X)$ is 32.

9. Let (V, f) be a non-degenerate four-dimensional unitary space over $\mathbb{F}_4$. Let $\mathcal{B} = (\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{y}_2, \boldsymbol{y}_1)$ be a basis of V such that $f(\boldsymbol{x}_1, \boldsymbol{x}_2) = f(\boldsymbol{x}_1, \boldsymbol{y}_2) = f(\boldsymbol{x}_2, \boldsymbol{y}_1) = f(\boldsymbol{y}_1, \boldsymbol{y}_2) = 0; f(\boldsymbol{x}_1, \boldsymbol{y}_1) = f(\boldsymbol{x}_2, \boldsymbol{y}_2) = 1$. Prove that a vector $a\boldsymbol{x}_1 + b\boldsymbol{x}_2 + c\boldsymbol{y}_2 + d\boldsymbol{y}_1$ is isotropic if and only if $Tr(a\overline{d}) + Tr(b\overline{c}) = 0$.

Let (V, f) be a non-degenerate unitary space of dimension four over $\mathbb{F}_4$. Set $\mathcal{P} = L_1(V) \setminus I_1(V)$, that is, the anisotropic one-dimensional subspaces.

10. For $X \in \mathcal{P}$ show that there are 12 elements in $L_1(X^\perp) \cap \mathcal{P}$.

11 If $X, Y \in \mathcal{P}$ and $X \perp Y$ prove that $|L_1(X^\perp \cap Y^\perp) \cap \mathcal{P}| = 2$ and if Z, W are anisotropic one spaces in $X^\perp \cap Y^\perp$, then $Z \perp W$.

12. If $X, Y \in \mathcal{P}$ and $X \perp Y$ let $l(X, Y) = \{X, Y, Z, W\}$ where Z and W are the anisotropic one spaces in $X^\perp \cap Y^\perp$. Show that there are 40 such sets.

13. Let $l = \{X_1, X_2, X_3, X_4\} \subset \mathcal{P}$ such that $X_i \perp X_j$ for $i \neq j$ (which implies that X_i are distinct). Let $Y \in \mathcal{P}, Y \notin l$. Prove that there is a unique $i \in \{1, 2, 3, 4\}$ such that $X_i \perp Y$.

This page intentionally left blank

12

Additional Topics in Linear Algebra

CONTENTS

This chapter is devoted to several additional topics in linear algebra and, more specifically, the theory of matrices. In the first section we introduce the notion of a matrix norm and show how such norms can be induced from norms on the spaces $\mathbb{R}^n$ and $\mathbb{C}^n$. The second section deals with the Moore–Penrose inverse of a matrix (also called the pseudoinverse). Section three takes up the theory of (real) non-negative matrices, that is, matrices all of whose entries are non-negative, which has multiple applications. Section four, where we prove the Geršgorin disc theorem, deals with the location of eigenvalues of a complex matrix. Finally, in section five we give meaning to the notion of exponentiating a real or complex matrix.

12.1 Matrix Norms

In this section we define the notion of a matrix norm and give several examples. We show how to induce a norm on $M_{mn}(\mathbb{F}), \mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$ from a pair of normed spaces $(\mathbb{F}^m, \| \cdot \|)$ and $(\mathbb{F}^n, \| \cdot \|')$.

What You Need to Know

Understanding the new material in this section depends on mastery of the following concepts: real and complex inner product space, norm of a vector in an inner product space, unit vector in an inner product space, the space $\mathbb{R}^n$, the space $\mathbb{C}^n$, abstract norm on a real or complex vector space, linear transformation from a vector space V to a vector space W, the vector space $\mathcal{L}(V, W)$ of linear transformations from V to W, the space $M_{mn}(\mathbb{F})$ of $m \times n$ matrices over a field $\mathbb{F}$, operator on a vector space V, composition of transformations, product of matrices, the algebra $\mathcal{L}(V, V)$ of linear operators on V, the algebra $M_{nn}(\mathbb{F})$ of $n \times n$ matrices with entries in $\mathbb{F}$, and the eigenvalues of a matrix.

We begin with the definition of a matrix norm.

Definition 12.1 *Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. A vector norm $\| \cdot \|$ that is defined on all the spaces $M_{mn}(\mathbb{F})$ for any choice of m and n is a* **matrix norm** *if for any pair of matrices A, B which can be multiplied we have*

$$\| AB \| \leq \| A \| \cdot \| B \| .$$

Definition 12.2 *Let A be an $m \times n$ matrix. The* **Frobenius norm** *on A is defined to be $\| A \|_F = Trace(A^{tr}\overline{A})^{\frac{1}{2}}$. If the entries of A are a_{ij} then*

$$\| A \|_F = \left(\sum_{i=1}^{m} \sum_{j=1}^{n} |a_{ij}|^2 \right)^{\frac{1}{2}} .$$

Remark 12.1 *If we identify $M_{mn}(\mathbb{F})$ with $\mathbb{F}^{mn}$ then the Frobenius norm on $M_{nn}(\mathbb{F})$ is the l_2-norm.*

Theorem 12.1 *The Frobenius norm is a matrix norm.*

Proof *For any pair of natural numbers we denote by* $\| \cdot \|_F$ *the Frobenius norm on* $M_{mn}(\mathbb{F})$. *We also denote by* $\| \cdot \|$ *the Euclidean norm on* $\mathbb{F}^n$. *Let* A *be an* $m \times n$ *matrix and* B *an* $n \times p$ *matrix. Let the rows of* A *be* $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ *and the columns of* B *be* $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_p$. *Then the* (i,j)*-entry of* AB *is* $\boldsymbol{a}_i \boldsymbol{b}_j$ *and by the definition we have*

$$\| AB \|_F = \left(\sum_{i=1}^{m} \sum_{j=1}^{p} |\boldsymbol{a}_i \boldsymbol{b}_j|^2 \right)^{\frac{1}{2}} .$$

Assume that $\mathbb{F} = \mathbb{R}$. *By the Cauchy–Schwartz inequality, Theorem (5.4), for* $\mathbb{R}^n$ *with the Euclidean inner product we have* $|\boldsymbol{a}_i \boldsymbol{b}_j|^2 \leq \| \boldsymbol{a}_i \|^2 \cdot \| \boldsymbol{b}_j \|^2$. *Consequently,*

$$\begin{aligned} \left(\sum_{i=1}^{n} \sum_{j=1}^{n} |\boldsymbol{a}_i \boldsymbol{b}_j|^2 \right)^{\frac{1}{2}} &\leq \left(\sum_{i=1}^{n} \sum_{j=1}^{n} \| \boldsymbol{a}_i \|^2 \cdot \| \boldsymbol{b}_j \|^2 \right)^{\frac{1}{2}} \\ &= \left[\left(\sum_{i=1}^{n} \| \boldsymbol{a}_i \|^2 \right) \cdot \left(\sum_{j=1}^{n} \| \boldsymbol{b}_j \|^2 \right) \right]^{\frac{1}{2}} . \end{aligned}$$

The latter expression is less than or equal to $\left(\| A \|_F^2 \cdot \| B \|_F^2 \right)^{\frac{1}{2}}$ *which, in turn, is equal to* $\| A \|_F \cdot \| B \|_F$.

On the other hand, suppose $\mathbb{F} = \mathbb{C}$. *Then* $\boldsymbol{a}_i \boldsymbol{b}_j = \langle \boldsymbol{a}_i, \overline{\boldsymbol{b}_j} \rangle$ *where* $\langle \boldsymbol{v}, \boldsymbol{w} \rangle$ *is the Euclidean inner product for* $\mathbb{C}^n$. *By the Cauchy–Schwartz inequality, Theorem (5.4),*

$$|\langle \boldsymbol{a}_i, \overline{\boldsymbol{b}_j} \rangle|^2 \leq \| \boldsymbol{a}_i \|^2 \cdot \| \overline{\boldsymbol{b}_j} \|^2 = \| \boldsymbol{a}_i \|^2 \cdot \| \boldsymbol{b}_j \|^2 .$$

Now we can complete the proof exactly as in the case that $\mathbb{F} = \mathbb{R}$.

Lemma 12.1 *Let* $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}, V = \mathbb{F}^n, W = \mathbb{F}^m$ *with norms* $\| \quad \|_V$ *and* $\| \quad \|_W$, *respectively, and let* A *be an* $m \times n$ *matrix with entries in* $\mathbb{F}$. *Then there exists a non-negative real number* M *such that* $\| A\boldsymbol{x} \|_W \leq M \| \boldsymbol{x} \|$.

Proof *Let* $\mathcal{B} = (\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n)$ *be the standard basis of* V. *Set*

$$m = max\{\| A\boldsymbol{e}_i \| \, | 1 \leq i \leq n\}.$$

Now let $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ *be an arbitrary vector in* V. *Note that the* l_1*-norm on* V

and the norm $\| \cdot \|$ are equivalent by Theorem (5.29) and therefore there is a constant C such that

$$\sum_{i=1}^{n} |x_i| \leq C \parallel \boldsymbol{x} \parallel_V .$$

Set $M = mC$. We claim that $\parallel A\boldsymbol{x} \parallel_W \leq M \parallel \boldsymbol{x} \parallel_V$ for every vector $\boldsymbol{x} \in X$. Thus,

$$\parallel A\boldsymbol{x} \parallel_W \;=\; \parallel \sum_{i=1}^{n} x_i A\boldsymbol{e}_i \parallel_W \;\leq\; \sum_{i=1}^{n} |x_i| \cdot \parallel A\boldsymbol{e}_i \parallel_W$$

by the triangle inequality. Since each $\parallel A\boldsymbol{e}_i \parallel_W \leq m$, we have

$$\sum_{i=1}^{n} |x_i| \cdot \parallel A\boldsymbol{e}_i \parallel_W \;\leq\; m \sum_{i=1}^{n} |x_i| \;\leq\; mC \parallel \boldsymbol{x} \parallel_V = M \parallel \boldsymbol{x} \parallel_V .$$

Remark 12.2 *It is straightforward to extend Lemma (12.1) to the case where $(V, \| \ \|_V)$ and $(W, \| \ \|_W)$ are finite dimensional normed spaces over the reals or complexes and $T : V \to W$ is a linear transformation.*

Corollary 12.1 *Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}, V = \mathbb{F}^n$, $W = \mathbb{F}^m$ and $\| \cdot \|_V, \| \cdot \|_W$ be norms on V and W, respectively. Let $A \in M_{mn}(\mathbb{F})$ and assume $T_A : V \to W$ is defined by $T_A(\boldsymbol{x}) = A\boldsymbol{x}$. Then T_A is continuous.*

Proof *We leave this as an exercise.*

Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}, V = \mathbb{F}^n$, and $W = \mathbb{F}^m$ with norms $\| \cdot \|_V$ and $\| \cdot \|_W$, respectively. We use Lemma (12.1) to define a norm on $M_{mn}(\mathbb{F})$.

Definition 12.3 *Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}, V = \mathbb{F}^n$, and $W = \mathbb{F}^m$ with norms $\| \cdot \|_V$ and $\| \cdot \|_W$, respectively. Let A be an $m \times n$ matrix. The* **matrix norm induced by** *$\| \ \|_V$ and $\| \ \|_W$, denoted by $\| \cdot \|_{V,W}$ is given by*

$$\parallel A \parallel_{V,W} = \sup_{\boldsymbol{x} \neq \boldsymbol{0}_V} \frac{\parallel A\boldsymbol{x} \parallel_W}{\parallel \boldsymbol{x} \parallel_V}.$$

The expression “sup” in the definition is an abbreviation for *supremum* which, for a set of reals is the least upper bound of the set. By Lemma (12.1) the set $\{\frac{\|A\boldsymbol{x}\|_W}{\|\boldsymbol{x}\|_V} | \boldsymbol{x} \in V, \boldsymbol{x} \neq \mathbf{0}\}$ is bounded above and, consequently, has a least upper bound. Note that if $\boldsymbol{x} \neq \mathbf{0}_V$ then

$$\frac{\| A\boldsymbol{x} \|_W}{\| \boldsymbol{x} \|_V} =\| \frac{1}{\| \boldsymbol{x} \|_V} A\boldsymbol{x} \|_W =\| A(\frac{\boldsymbol{x}}{\| \boldsymbol{x} \|_V}) \|_W .$$

Moreover, $\frac{\boldsymbol{x}}{\|\boldsymbol{x}\|}$ is a unit vector in V. Therefore we have the following alternative expression for the operator norm:

Theorem 12.2 *Let $(V, \| \cdot \|_V), (W, \| \cdot \|_W)$ be as in Definition (12.3), respectively, and let A be an $m \times n$ matrix. Then*

$$\| A \|_{V,W} = \sup_{\|\boldsymbol{v}\|=1} \| A\boldsymbol{v} \|_W .$$

We have referred to $\| \quad \|_{V,W}$ as a norm, and we now demonstrate that this is so.

Theorem 12.3 *Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}, V = \mathbb{F}^n$, and $W = \mathbb{F}^m$ with norms $\| \cdot \|_V$ and $\| \cdot \|_W$, respectively. Then $\| \cdot \|_{V,W}$ is a norm on $M_{mn}(\mathbb{F})$.*

Proof *Let A be an $m \times n$ matrix. Clearly, $\| A \|_{V,W} \geq 0$. Suppose $\| A \|_{V,W} = 0$. Then $A\boldsymbol{x} = \mathbf{0}_W$ for every $\boldsymbol{x}$ and $A = \mathbf{0}_{mn}$. This establishes the first property.*

Assume $A \in M_{mn}(\mathbb{R})$ and $c \in \mathbb{F}$. Then

$$\begin{aligned}
\| cA \|_{V,W} &= \sup_{\|\boldsymbol{v}\|_V=1} \| (cA)(\boldsymbol{v}) \|_W \\
&= \sup_{\|\boldsymbol{v}\|_V=1} \| c(A\boldsymbol{v}) \|_W \\
&= \sup_{\|\boldsymbol{v}\|_V=1} |c| \| A\boldsymbol{v} \|_W \\
&= |c| \sup_{\|\boldsymbol{v}\|_V=1} \| A\boldsymbol{v} \|_W \\
&= |c| \| A \|_{V,W} .
\end{aligned}$$

Now assume that $A, B \in M_{mn}(\mathbb{F})$. Then

$$\begin{aligned}\| A+B \|_{V,W} &= \sup_{\|\boldsymbol{v}\|_V=1} \| (A+B)(\boldsymbol{v}) \|_W \\ &= \sup_{\|\boldsymbol{v}\|_V=1} \| A\boldsymbol{v}+B\boldsymbol{v} \|_W \\ &\leq \sup_{\|\boldsymbol{v}\|_V=1} (\| A\boldsymbol{v} \|_W + \| B\boldsymbol{v} \|_W) \\ &= \sup_{\|\boldsymbol{v}\|_V=1} \| A\boldsymbol{v} \|_W + \sup_{\|\boldsymbol{v}\|_V=1} \| B\boldsymbol{v} \|_W \\ &= \| A \|_{V,W} + \| B \|_{V,W} .\end{aligned}$$

We next prove that operator norms are matrix norms.

Theorem 12.4 *Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}, U = \mathbb{F}^n, V = \mathbb{F}^m$, and $W = \mathbb{F}^l$ with norms $\| \cdot \|_U, \| \cdot \|_V$, and $\| \cdot \|_W$, respectively. Let $A \in M_{mn}(\mathbb{F})$ and $B \in M_{lm}(\mathbb{F})$. Then*

$$\| BA \|_{U,W} \leq \| B \|_{V,W} \quad \| A \|_{U,V} .$$

Proof *Let $\boldsymbol{u} \in U = \mathbb{F}^n, \boldsymbol{u} \neq \mathbf{0}_U$. If $A\boldsymbol{u} = \mathbf{0}_m$ then $BA\boldsymbol{u} = B\mathbf{0}_m = \mathbf{0}_l$. In this case we have*

$$0 = \frac{\| BA\boldsymbol{u} \|_W}{\| \boldsymbol{u} \|_U} \leq \| B \|_{V,W} \cdot \| A \|_{U,V} .$$

Suppose $A\boldsymbol{u} \neq \mathbf{0}_m$. Then $\| B(A\boldsymbol{u}) \|_W \leq \| B \|_{V,W} \| A\boldsymbol{u} \|_V$ by the definition of $\| B \|_{V,W}$. By the definition of $\| A \|_{U,V}$ we have

$$\| A\boldsymbol{u} \|_V \leq \| A \|_{U,V} \| \boldsymbol{u} \|_V .$$

Consequently,

$$\| (BA)\boldsymbol{u} \|_W \leq \| B \|_{V,W} \cdot \| A \|_{U,V} \cdot \| \boldsymbol{u} \|_U$$

from which we conclude that $\frac{\|(BA)\boldsymbol{u}\|_W}{\|\boldsymbol{u}\|_U} \leq \| B \|_{V,W} \cdot \| A \|_{U,W}$.

Since for every $\boldsymbol{u} \neq \mathbf{0}_U, \frac{\|(BA)\boldsymbol{u}\|_W}{\|\boldsymbol{u}\|_U} \leq \| B \|_{V,W} \cdot \| A \|_{U,W}$ we can conclude that $\| BA \|_{U,W} \quad \leq \quad \| B \|_{V,W} \cdot \| A \|_{U,V}$.

It is often the case when $V = \mathbb{F}^n, W = \mathbb{F}^m$ to use the same norm in both when inducing a matrix norm. When we equip both V and W with the l_p-norm with $1 \leq p \leq \infty$ we will denote the induced operator norm on $M_{mn}(\mathbb{F})$ by $\| \quad \|_{p,p}$.

The next result gives the values of a matrix in terms of its entries with respect to the most common induced operator norms. But first we make a definition:

Definition 12.4 *Let A be a square complex matrix. The* **spectral radius** *of A is the maximum of $|\lambda|$ taken over all eigenvalues λ of A. This denoted by $\rho(A)$.*

Theorem 12.5 *Let $A \in M_{mn}(\mathbb{F})$ with entries a_{ij}. Then*

i) $\| A \|_{1,1} = \max_{1 \leq i \leq m}\{\sum_{j=1}^{n} |a_{ij}|\}$.

ii) $\| A \|_{\infty,\infty} = \max_{1 \leq j \leq n}\{\sum_{i=1}^{m} |a_{ij}|\}$.

iii) $\| A \|_{2,2} = \rho(A^{tr}\overline{A})^{\frac{1}{2}}$.

Proof *i) First note that*

$$A\boldsymbol{x} = \begin{pmatrix} \sum_{j=1}^{n} a_{1j}x_j \\ \vdots \\ \sum_{j=1}^{n} a_{mj}x_j \end{pmatrix}$$

and therefore

$$\| A\boldsymbol{x} \|_1 \ = \ \sum_{i=1}^{m}\left|\sum_{j=1}^{n} a_{ij}x_j\right| \ \leq \ \sum_{j=1}^{n}\left(\sum_{i=1}^{m}|a_{ij}|\right)|x_j|. \tag{12.1}$$

Consequently,

$$\| A\boldsymbol{x} \|_1 \leq \max_{1 \leq j \leq n}\left\{\sum_{i=1}^{m}|a_{ij}|\right\} \| \boldsymbol{x} \|_1 \ . \tag{12.2}$$

Thus,

$$\| A \|_{1,1} \ \leq \ \max_{1 \leq i \leq m}\{\sum_{j=1}^{n}|a_{ij}|\}.$$

To get the desired equality it suffices to demonstrate the existence of a unit vector $\boldsymbol{x}$ with respect to the l_1-norm such that we have equality in Equation (12.1).

Let us suppose that the maximum of $\{\sum_{i=1}^{n}|a_{ij}||1 \leq j \leq n\}$ occurs for $j = 1$. For an arbitrary non-zero vector $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ we have

$$\| A \|_{1,1} \geq \frac{\| A\boldsymbol{x} \|_1}{\| \boldsymbol{x} \|_1} = \sum_{i=1}^{m}\left|\sum_{j=1}^{n} a_{ij}x_j.\right|$$

Now take $\boldsymbol{x} = \boldsymbol{e}_1$. *Then we get*

$$\| A \|_{1,1} \ \geq \ \sum_{i=1}^{m} |a_{i1}| = \max_{1\leq j\leq n} \left\{ \sum_{i=1}^{m} |a_{ij}| \right\}.$$

which gives us the desired equality. The proof is exactly the same if the maximum in Equation (12.2) occurs when $j = k$.

ii) Let $\boldsymbol{x} \in \mathbb{F}^n$ *be a non-zero vector and note that*

$$\left| \sum_{j=1}^{n} a_{ij} x_j \right| \ \leq \ \sum_{j=1}^{n} |a_{ij}| \cdot |x_j| \leq \sum_{j=1}^{n} |a_{ij} \cdot \| \boldsymbol{x} \|_\infty .$$

Consequently, we can conclude that

$$\| A\boldsymbol{x} \|_\infty \ = \ \max_{i=1}^{m} \left\{ \left| \sum_{j=1}^{n} a_{ij} x_j \right| \right\} \ \leq \ \max_{i=1}^{m} \left\{ \sum_{j=1}^{n} |a_{ij}| \right\} \| \boldsymbol{x} \|_\infty .$$

It therefore follows that

$$\| A \|_{\infty,\infty} \leq \max_{i=1}^{m} \left\{ \sum_{j=1}^{n} |a_{ij}| \right\}.$$

To get equality we need only show that there exists a unit vector $\boldsymbol{x}$ *with respect to the* l_∞*-norm such that* $\| A\boldsymbol{x} \|_\infty = \max_{i=1}^{m} \left\{ \sum_{j=1}^{n} |a_{ij}| \right\} \| \boldsymbol{x} \|_\infty$.

By way of illustration, assume $\max_{i=1}^{m} \left\{ \sum_{j=1}^{n} |a_{ij}| \right\} = \sum_{j=1}^{n} |a_{1j}|$ *(and is positive). Set* $x_j = \frac{\overline{a_{1j}}}{|a_{1j}|}$ *if* $a_{1j} \neq 0$ *and is 0 otherwise and set* $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$.

Then $\| \boldsymbol{x} \|_\infty = 1$ *and*

$$\| A \|_{\infty,\infty} \ \geq \| A\boldsymbol{x} \|_\infty \geq \left| \sum_{j=1}^{n} a_{1j} x_j \right| =$$

$$\sum_{j=1}^{n} \frac{|a_{ij}|^2}{|a_{ij}|} = \sum_{j=1}^{n} |a_{ij}| = \max \left\{ \sum_{j=1}^{n} |a_{ij}| | 1 \leq i \leq n \right\}.$$

iii) Suppose first that A *is a complex matrix. Let* $\alpha_1 > \cdots > \alpha_t$ *be the non-zero* *eigenvalues of* $\overline{A}^{tr}A$ *(note the matrix* $\overline{A}^{tr}A$ *is semi-positive and therefore its eigenvalues are all non-negative real numbers). Set* $s_i = \sqrt{\alpha_i}$ *for* $1 \leq i \leq t$ *and* $s_i = 0$ *for* $t < i \leq n$*. By the matrix version of the singular value theorem, Corollary (6.5), there are unitary matrices* Q *and* P *such that* $A = QSP$*. Now* $\parallel A \parallel_{2,2}= sup_{\|\boldsymbol{x}\|_2=1} \parallel QSP\boldsymbol{x} \parallel_2$*. Since* Q *is unitary,* $\parallel QSP\boldsymbol{x} \parallel_2 = \parallel SP\boldsymbol{x} \parallel_2$*. On the other hand,* $\parallel P\boldsymbol{x} \parallel_2 = \parallel \boldsymbol{x} \parallel_2$ *and as* $\boldsymbol{x}$ *ranges over all vectors of norm one so does* $P\boldsymbol{x}$*. Therefore,*

$$\begin{aligned}\parallel A \parallel_{2,2} &= sup\{\parallel SP\boldsymbol{x}| \parallel \boldsymbol{x} \parallel_2 = 1\} \\ &= sup\{\parallel \boldsymbol{y} \parallel_2 \mid \parallel \boldsymbol{y} \parallel_2 = 1\}.\end{aligned}$$

Suppose now that $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$*. Then* $S\boldsymbol{x} = \begin{pmatrix} s_1x_1 \\ \vdots \\ s_tx_t \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ *and*

$$\begin{aligned}\parallel S\boldsymbol{x} \parallel_2^2 &= \sum_{i=1}^{t}(s_ix_i)^2 \\ &\leq \textstyle\sum_{i=1}^{t}(s_1x_1)^2 = s_1^2\sum_{i=1}^{t} x_i^2 \\ &\leq s_1^2\textstyle\sum_{i=1}^{n} x_i^2 = s_1^2.\end{aligned}$$

Thus, $\parallel A \parallel_{2,2} \leq \sqrt{s_1^2} = s_1 = \rho(\overline{A}^{tr}A)^{\frac{1}{2}}$*. On the other hand if* $\boldsymbol{x} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ *then* $\parallel S\boldsymbol{x} \parallel_2 = s_1$*. Thus,* $\parallel A \parallel_{2,2} = s_1 = \rho(\overline{A}^{tr}A)^{\frac{1}{2}}$*.*

We will conclude this section with a couple of significant results that illustrate the power of these ideas and the utility of matrix and operator norms. First a definition.

Definition 12.5 *A norm* $\parallel \quad \parallel$ *on the space* $M_{nn}(\mathbb{C})$ *is* **multiplicative** *if for any two matrices* $A, B \in M_{n\times n}(\mathbb{C})$ *we have* $\parallel AB \parallel \quad \leq \parallel A \parallel \cdot \parallel B \parallel$ *.*

The following is elementary and we leave it as an exercise.

Lemma 12.2 *Assume* $\parallel \cdot \parallel$ *is a multiplicative norm on* $M_{nn}(\mathbb{C})$*. Then* $\parallel I_n \parallel \geq 1$*.*

The next result is known as Banach's lemma.

Theorem 12.6 *Assume* $\| \cdot \|$ *is a multiplicative norm on* $M_{nn}(\mathbb{C})$*. If* $A \in M_{nn}(\mathbb{C})$ *and* $\| A \| \ < 1$ *then the following hold:*

i) $I_n - A$ *is invertible;*

ii) the sum $\sum_{j=0}^{\infty} A^j$ *converges and is equal to* $(I_n - A)^{-1}$*; and*

iii) $\| (I_n - A)^{-1} \| \ \leq \ \frac{1}{1-\|A\|}$.

Proof *Let* $\epsilon > 0$*. Set* $S_k = \sum_{j=0}^{k} A^j$*. Assume* $l > k$*. Then*

$$\| S_l - S_k \| \ = \ \left\| \sum_{j=k+1}^{l} A^j \right\| \ \leq \ \sum_{j=k+1}^{l} \| A^j \|$$

$$\sum_{j=k+1}^{l} \| A \|^j \leq \sum_{j=k+1}^{\infty} \| A \|^j = \| A \|^{k+1} (1- \| A \|)^{-1}.$$

Since $\| A \| < 1$ *we can find a natural number* M *such that if* $m > M$ *then* $\| A \|^m \ (1- \| A \|)^{-1} < \epsilon$*. It follows that* $\{S_k\}_{k=1}^{\infty}$ *is a Cauchy sequence in* $M_{nn}(\mathbb{C})$*. Since* $M_{nn}(\mathbb{C})$ *is complete (every Cauchy sequence has a limit) there is a matrix* B *such that* $\lim_{k\to\infty} S_k = B$*. Next, note that*

$$(I_n - A)B - I_n = (I_n - A)(B - S_k) + (I_n - A)S_k - I_n.$$

Also note that $(I_n - A)S_k - I_n = -A^{k+1}$*.*
If we take norms, by the triangle inequality we have

$$\begin{aligned} \| (I_n - A)B - I_n \| \ &\leq \ \| (I_n - A)(B - S_k) \| + \| (I_n - A)S_k - I_n \| \\ &\leq \ \| I_n - A \| \cdot \| B - S_k \| + \| -A^{k+1} \| \\ &\leq \ \| I_n - A \| \cdot \| B - S_k \| + \| A \|^{k+1} . \end{aligned}$$

However, $\lim_{k\to\infty} \| B - S_k \| = 0$ *and* $\lim_{k\to\infty} \| A \|^{k+1} = 0$ *and therefore* $(I_n - A)B = I_n$ *and* $B = (I_n - A)^{-1}$*.*

Finally,

$$\begin{aligned} \parallel S_k \parallel &= \parallel I_n + A + \cdots + A^k \parallel \\ &\leq \parallel I_n \parallel + \parallel A \parallel + \cdots + \parallel A^k \parallel \\ &\leq \parallel I_n \parallel + \parallel A \parallel + \ldots \parallel A \parallel^k \\ &\leq \sum_{j=0}^{\infty} \parallel A \parallel^j \\ &= \frac{1}{1- \parallel A \parallel}. \end{aligned}$$

Taking limits we get

$$\parallel B \parallel \;=\; \parallel \lim_{k\to\infty} S_k \parallel \;=\; \lim_{k\to\infty} \parallel S_k \parallel \;\leq\; \frac{1}{1- \parallel A \parallel}.$$

For more on this topic a good source is [12]).

Exercises

1. Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. Assume $\parallel \cdot \parallel'$ is a matrix norm induced on $M_{nn}(\mathbb{F})$ by a norm on $\mathbb{F}^n$. Prove that $\parallel I_n \parallel' = 1$.

2. Let $\parallel \quad \parallel_F$ be the Frobenius norm on $M_{nn}(\mathbb{F})$. Prove that $\parallel I_n \parallel_F = \sqrt{n}$ and conclude that the Frobenius norm is not induced by any norm on $\mathbb{F}^n$.

In Exercises 3 and 4 compute $\parallel A \parallel_F, \parallel A \parallel_{1,1}, \parallel A \parallel_{\infty,\infty}$, and $\parallel A \parallel_{2,2}$ for the given matrix A.

3. $A = \begin{pmatrix} 12 & 2 \\ 7 & 0 \end{pmatrix}$

4. $A = \begin{pmatrix} 3 & 1 & 1 \\ 1 & 3 & 1 \\ 1 & 1 & 3 \end{pmatrix}$

5. Prove Corollary (12.1).

6. Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$ and assume $\parallel \cdot \parallel$ is a matrix norm on $M_{nn}(\mathbb{F})$ so that $\parallel AB \parallel \;\leq\; \parallel A \parallel \cdot \parallel B \parallel$. Prove that $\parallel I_n \parallel \geq 1$.

12.2 The Moore–Penrose Inverse of a Matrix

This section is devoted to the introduction and development of the Moore–Penrose inverse, also referred to as the pseudoinverse of a matrix. We will show that every matrix has a unique pseudoinverse and give a method for computing it. We will also obtain a criterion for a linear system to have a solution in terms of the pseudoinverse of the coefficient matrix of the system.

What You Need to Know

Understanding the new material in this section depends on mastery of the following concepts: Column space of a matrix, rank of a matrix, null space of a matrix, eigenvalue of a matrix, eigenvector of a matrix, linearly independent sequence of vectors, basis of a vector space, coordinate vector of a vector with respect to a basis, dimension of a vector space, consistent linear system of equations, and the coefficient matrix of a linear system.

We begin with a definition.

Definition 12.6 *Let A be an $m \times n$ matrix with rank r. A* **full rank factorization** *of A is an expression $A = BC$ where B is an $m \times r$ matrix of rank r and C is an $r \times n$ matrix of rank r.*

In our first result we prove that every matrix has a full rank factorization.

Theorem 12.7 *Let A be an $m \times n$ matrix with entries in the field $\mathbb{F}$ and assume the rank of A is r. Then there exists an $m \times r$ matrix B with rank r and an $r \times n$ matrix C with rank r such that $A = BC$.*

Proof *Denote by $\boldsymbol{a}_1, \dots, \boldsymbol{a}_n$ the columns of A and set $V = col(A)$. Let $\mathcal{B} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_r)$ be any basis of the column space of A and let B be the matrix whose columns are the vectors of $\mathcal{B}$. Then B is an $m \times r$ matrix and the columns of B are linearly independent. Therefore the rank of B is r. Now let $1 \leq j \leq n$ and denote by $\boldsymbol{c}_j$ the coordinate vector of $\boldsymbol{a}_j$ with respect to $\mathcal{B}$ and let C be the matrix whose columns are the vectors $\boldsymbol{c}_1, \dots, \boldsymbol{c}_n$. Then C is an $r \times n$ matrix also of rank r. We claim that $BC = A$. Toward that objective, let $\boldsymbol{c}_j = \begin{pmatrix} c_{1j} \\ \vdots \\ c_{rj} \end{pmatrix}$. By the definition of matrix multiplication we have*

$$BC = B(\boldsymbol{c}_1 \dots \boldsymbol{c}_n) = (B\boldsymbol{c}_1 \dots B\boldsymbol{c}_n).$$

However,

$$B\boldsymbol{c}_j = (\boldsymbol{v}_1 \dots \boldsymbol{v}_r) \begin{pmatrix} c_{1j} \\ \vdots \\ c_{rj} \end{pmatrix} = c_{1j}\boldsymbol{v}_1 + \cdots + c_{rj}\boldsymbol{v}_r = \boldsymbol{a}_j.$$

In our next result we show that though a full rank factorization of a matrix is not unique, for a fixed left factor B there is a unique matrix C which completes it, that is, such that $A = BC$ is a full rank factorization.

Lemma 12.3 *Let A be an $m \times n$ matrix with rank r with entries in a field $\mathbb{F}$. Assume B is an $m \times r$ matrix with rank r and that $A = BC = BC'$. Then $C = C'$.*

Proof *Note that for any two matrices X and Y compatible for multiplication, that every column of XY is a linear combination of the columns of X and therefore col(XY) is contained in col(X). Therefore in the present situation we have that col(A) is contained in col(B). However, since rank$(A) = r =$ rank(B), we have equality and, furthermore, the columns of B are a basis of col(A). Let the sequence of columns of B be $\mathcal{B} = (\boldsymbol{b}_1, \dots, \boldsymbol{b}_r)$ and the sequence of columns of A be $(\boldsymbol{a}_1, \dots, \boldsymbol{a}_n)$. Let $\boldsymbol{c}_j = \begin{pmatrix} c_{1j} \\ \vdots \\ c_{rj} \end{pmatrix}$ be the j^{th} column of C. Then*

$$c_{1j}\boldsymbol{b}_1 + \cdots + c_{rj}\boldsymbol{b}_r = \boldsymbol{a}_j.$$

It follows that $\boldsymbol{c}_j$ is the coordinate vector of $\boldsymbol{a}_j$ with respect to $\mathcal{B}$, which implies that C is unique.

We can now show how any two full factorizations of a matrix are related:

Theorem 12.8 *Let A be an $m \times n$ matrix with rank r and entries in a field $\mathbb{F}$. Let $A = BC$ be a full rank factorization of A. Assume D is an $m \times r$ matrix with rank r and E is an $r \times n$ matrix with rank r. Then $A = DE$ if and only if there is an invertible $r \times r$ matrix Q such that $D = BQ, E = Q^{-1}C$.*

Proof *If $D = BQ$ and $E = Q^{-1}C$ for some invertible $r \times r$ matrix Q then D and E have rank r and $DE = (BQ)(Q^{-1}C) = B(QQ^{-1})C = BI_rC = BC = A$. It remains to prove the converse.*

We noted at the beginning of the proof of Lemma (12.3) that col(A) is contained in col(B) and col(D). Since rank$(A) = r =$ rank$(B) =$ rank(D), *it follows that we have the equality col(A) = col(B) = col(D). Moreover, if $\mathcal{B} = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_r)$ is the sequence of columns of B and $\mathcal{D} = (\boldsymbol{d}_1, \ldots, \boldsymbol{d}_r)$ is the sequence of columns of D then $\mathcal{B}$ and $\mathcal{D}$ are both bases of col(A). Let T denote the identity operator on col(A) and set $Q = \mathcal{M}_T(\mathcal{D}, \mathcal{B})$ (that is, the j^{th} column of Q is the coordinate vector of $\boldsymbol{d}_j$ with respect to $\mathcal{B}$. We then have $BQ = D$. Consequently, $A = BC = DE = (BQ)E = B(QE)$. By Lemma (12.3), $C = QE$ from which we conclude that $E = Q^{-1}C$ as required.*

Remark 12.3 *If A is an $m \times n$ matrix of rank r over a finite field $\mathbb{F}_q$ then the number of full rank factorization is equal to the number of bases in $\mathbb{F}_q^r$ which is $|GL_r(\mathbb{F}_q)| = q^{\binom{r}{2}}(q^r - 1) \ldots (q - 1)$. If $\mathbb{F}$ is an infinite field then there are infinitely many full rank factorizations.*

We now define the pseudoinverse of a complex matrix A.

Definition 12.7 *Let A be an $m \times n$ matrix with entries in $\mathbb{C}$. A* **pseudoinverse***, also referred to as a* **Moore–Penrose inverse** *of A, is an $n \times m$ matrix X which satisfies the following four matrix equations:*

(PI1) $AXA = A$
(PI2) $XAX = X$
(PI3) $(AX)^* = AX$
(PI4) $(XA)^* = XA$.

The four equations in the definition are called the **Moore–Penrose equations**.

We remark that for a complex matrix $B, \overline{B}$ is the matrix obtained from B by taking the complex conjugate of each entry and $B^* = \overline{B^{tr}}$ is the adjoint of B.

In our next result we prove that if a matrix A has a pseudoinverse, then it is unique.

Theorem 12.9 *Let A be an $m \times n$ matrix with complex coefficients. If A has a pseudoinverse then it is unique.*

Proof *Assume $X, Y \in M_{n \times m}(\mathbb{C})$ are both pseudoinverses of A so that (PI1)–(PI4) hold for both X and Y. We then have*

$$X = X(AX) = X(AX)^* = XX^*A^* = XX^*(AYA)^* =$$
$$XX^*A^*(AY)^* = X(AX)^*(YA)^* = X(AX)(AY) =$$
$$XAY = X(AYA)Y = (XA)^*(YA)^*Y = A^*X^*A^*Y^*Y =$$
$$(AXA)^*Y^*Y = A^*Y^*Y = (YA)^*Y = YAY = Y.$$

Let A be an $m \times n$ complex matrix. If A has a pseudoinverse we will denote it by $A^\dagger$. The following are a few examples of pseudoinverses. The proofs are left to the exercises.

Example 12.1 *Assume A is an invertible $n \times n$ matrix. Then $A^\dagger \ = A^{-1}$.*

Example 12.2 *Let U be a subspace of $\mathbb{C}^n$ and let P be the matrix of the orthogonal projection onto U (with respect to the standard orthonormal basis). Then P is self-adjoint and satisfies $P^2 = P$. In this case, $P^\dagger \ = P$.*

Example 12.3 *Let $D = diag\{d_1, \ldots, d_r, 0, \ldots, 0\}$ be an $n \times n$ complex diagonal matrix with $d_i \neq 0$ for $1 \leq i \leq r$. Then $D^\dagger \ = diag\{\frac{1}{d_1}, \ldots, \frac{1}{d_r}, 0 \ldots, 0\}$.*

Example 12.4 *Let $\boldsymbol{v} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ be a non-zero vector in $\mathbb{C}^n$ (so that $\boldsymbol{v}$ is an $n \times 1$ matrix). Then*

$$\boldsymbol{v}^\dagger \ = \frac{1}{\parallel \boldsymbol{v} \parallel^2}(\overline{a_1} \ldots \overline{a_n}).$$

In our next result we show the existence of the pseudoinverse in two special cases, which will lead to existence in general.

Theorem 12.10 *i) Assume B is an $m \times r$ complex matrix with rank r. Then $B^\dagger \ = (B^*B)^{-1}B^*$.*

ii) Assume C is an $r \times n$ complex matrix with rank r. Then $C^\dagger \ = C^*(CC^*)^{-1}$.

Remark 12.4 *Multiplication of vectors in $\mathbb{C}^r$ by B gives an injective transformation from the inner product space $\mathbb{C}^r$ to $\mathbb{C}^m$. It then follows that the operator $B^*B : \mathbb{C}^r \to \mathbb{C}^r$ is injective (and positive) and hence invertible. Similarly, CC^* is invertible.*

Proof *i) We prove each of the Moore–Penrose equations is satisfied:*

(PI1) $B[(B^*B)^{-1}B^*]B = B(B * B)^{-1}(B^*B) = BI_r = B$.

(PI2) $[(B^*B)^{-1}B^*]B[(B^*B)^{-1}B^*] = [(B^*B)^{-1}(B^*B)][(B^*B)^{-1}B^*] = I_r[(B^*B)^{-1}B^*] = (B^*B)^{-1}B^*$.

(PI3) Note that B^*B is self-adjoint and therefore $(B^*B)^{-1}$ is self-adjoint. We therefore have

$$\{B[(B^*B)^{-1}B^*]\}^* = (B^*)^*(B^*B)^{-1}B^* = B(B^*B)^{-1}B^*$$

as required.

(PI4) Finally, $[(B^*B)^{-1}B^*]B = (B^*B)^{-1}(B^*B) = I_r$. Consequently, $\{[(B^*B)^{-1}B^*]B\}^* = I_r^* = I_r = [(B^*B)^{-1}B^*]B$.

ii) This is left as an exercise.

Theorem 12.11 *Let A be an $m \times n$ complex matrix of rank r. Assume $A = BC$ is a full rank factorization of A. Set $A^\sharp = C^\dagger B^\dagger = [C^*(CC^*)^{-1}][(B^*B)^{-1})B^*]$. Then $A^\sharp = A^\dagger$. Moreover, $AA^\dagger = BB^\dagger$ and $A^\dagger A = C^\dagger C$ for any full rank factorization $A = BC$.*

Proof *We prove that the four Moore–Penrose equations are satisfied: Note that $B^\dagger B = I_r = CC^\dagger$.*

(PI1) $AA^\sharp A = AC^\dagger B^\dagger A = AC^\dagger B^\dagger BC = AC^\dagger C = BCC^C = BC = A$.

(PI2) $A^\sharp AA^\sharp = (C^\dagger B^\dagger)(BC)(C^\dagger B^\dagger) = C^\dagger(B^\dagger B)(CC^\dagger)B^\dagger = C^\dagger I_r I_r B^\dagger = C^\dagger B^\dagger = A^\sharp$.

(PI3) $AA^\sharp = BC(C^\dagger B^\dagger) = B(CC^\dagger)B^\dagger = BB^\dagger$ and $(BB^\dagger)^* = BB^\dagger$.

(PI4) $A^\sharp A = (C^\dagger B^\dagger)(BC) = C^\dagger(B^\dagger B)C = C^\dagger C$ and $(C^\dagger C)^* = C^\dagger C$.

Remark 12.5 *Let A be an $m \times n$ complex matrix with rank r. It follows from the Moore–Penrose equations and the uniqueness of the pseudoinverse that $(A^\dagger)^\dagger = A$.*

Let A be an $m \times n$ matrix with rank r. In the next result we show that when we view $AA^\dagger$ as an operator on the space $\mathbb{C}^m$ equipped with the standard inner product via matrix multiplication, then $AA^\dagger$ is the (orthogonal) projection onto the column space of A.

Theorem 12.12 *Let A be an $m \times n$ complex matrix with rank r. View A as a linear transformation from $\mathbb{C}^n$ to $\mathbb{C}^m$ via matrix multiplication on the left. Let $\langle\ ,\ \rangle_n$ be the inner product defined on $\mathbb{C}^n$ by $\langle \boldsymbol{v}, \boldsymbol{w}\rangle_n = \boldsymbol{v}^{tr}\overline{\boldsymbol{w}}$ for $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{C}^n$ with $\langle\ ,\ \rangle_m$ defined similarly. Set $U = col(A)$, the column space of A, and $P = AA^\dagger$, an operator on $\mathbb{C}^m$. Then the following hold:*

i) P is Hermitian matrix.
ii) For $\boldsymbol{u} \in U, P\boldsymbol{u} = \boldsymbol{u}$.
iii) If $\boldsymbol{w} \in U^\perp$ then $P\boldsymbol{w} = \boldsymbol{0}_m$.

Consequently, P is the orthogonal projection onto U.

Proof *i) This follows from (PI3).*

ii) Let $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ be the columns of A. Then $PA = P(\boldsymbol{a}_1 \ldots \boldsymbol{a}_n) = (P\boldsymbol{a}_1 \ldots P\boldsymbol{a}_n)$. By (PI1) we have $PA = A$ and therefore for each $j, P\boldsymbol{a}_j = \boldsymbol{a}_j$. Consequently, if $\boldsymbol{u}$ is a linear combination of $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$, then $P\boldsymbol{u} = \boldsymbol{u}$.

iii) Since $P = AA^\dagger$, it follows that $rank(P) \leq rank(A) = r$. However, as shown in ii) the column space of P contains the column space of A and therefore $rank(P) = r$ and we have the equality $col(P) = col(A)$. Since P is self-adjoint, we have $ker(P) = range(P)^\perp = U^\perp$.

Remark 12.6 *Let A be an $m \times n$ matrix with rank r. Note that in light of Remark (12.5) it follows that $A^\dagger A$ is the orthogonal projection of $\mathbb{C}^n$ onto $col(A^\dagger\ )$.*

The following can be deduced from Theorem (12.12) and Remark (12.6).

Corollary 12.2 *Let A be an $m \times n$ complex matrix. Set $P = AA^\dagger\ \in M_{mm}(\mathbb{C})$ and $Q = A^\dagger A \in M_{nn}(\mathbb{C})$. Then the following hold:*

i) $P^2 = P = P^*$.
ii) $(I_m - P)^2 = I_m - P = (I_m - P)^*$.
iii) $(I_m - P)P = \mathbf{0}_{m \times m}$.
iv) $Q^2 = Q = Q^*$.
v)$(I_n - Q)^2 = I_n - Q = (I_n - Q)^*$.
vi) $(I_n - Q)Q = \mathbf{0}_{n \times n}$.

Proof *The first three all follow from Theorem (12.12). The subsequent three follow from the fact that $(A^\dagger)^\dagger = A$, Theorem (12.12), and the first three applied to $A^\dagger$.*

The next result indicates how the pseudoinverse of a matrix interacts with its adjoint.

Theorem 12.13 *Let A be an $m \times n$ complex matrix. Then the following hold:*

i) $(A^*)^\dagger\ = (A^\dagger\ )^*$.
ii) $(A^*A)^\dagger\ = A^\dagger\ (A^*)^\dagger\ $.
iii) $A^* = A^*(AA^\dagger\ ) = (A^\dagger\ A)A^*$.
iv) $A^\dagger\ = (A^*A)^\dagger\ A^* = A^*(AA^*)^\dagger\ $.

Proof *These are left as exercises.*

In our next result we make use of the pseudoinverse of a matrix to determine its null space.

Theorem 12.14 *Let A be an $m\times n$ complex matrix with rank r. Set $Q = A^\dagger A$. Then the null space of A is the column space of $I_n - Q$.*

Proof *First note that $A(I_n - Q) = A - AQ = A - AA^\dagger\ A = A - A = \mathbf{0}_{m\times n}$. Consequently, the column space of $I_n - Q$ is contained in the null space of A. On the other hand, it follows from Remark (12.6) that Q is an orthogonal projection on $\mathbb{C}^n$ and rank$(Q) = r$. Then rank$(I_n - Q) = n - r$. By Theorem (2.9) it follows that the nullity of A is $n - r$. Since col$(I_n - Q) \subset$ null(A) and dim(col$(I_n - Q)) = n - r =$ dim(null(A)) we get the equality null$(A) =$ col$(I_n - Q)$.*

In our last result we get a criterion for a vector to be in the column space of a matrix in terms of the pseudoinverse and use this to describe the solutions to a consistent linear system.

Theorem 12.15 *Let A be an $m \times n$ complex matrix and $\boldsymbol{b} \in \mathbb{C}^m$. Then $\boldsymbol{b} \in$ col(A) if and only if $AA^\dagger\boldsymbol{b} = \boldsymbol{b}$. Moreover, if $\boldsymbol{b} \in$ col(A) and $\boldsymbol{x} \in \mathbb{C}^n$ satisfies $A\boldsymbol{x} = \boldsymbol{b}$, then there exists a vector $\boldsymbol{y} \in \mathbb{C}^n$ such that $\boldsymbol{x} = A^\dagger\boldsymbol{b} + (I_n - A^\dagger A)\boldsymbol{y}$.*

Proof *Assume $AA^\dagger\boldsymbol{b} = \boldsymbol{b}$. Setting $\boldsymbol{x} = A^\dagger\boldsymbol{b}$ we get $A\boldsymbol{x} = \boldsymbol{b}$ and $\boldsymbol{b} \in$ col(A). On the other hand, suppose $\boldsymbol{b} \in$ col(A). Then there is an $\boldsymbol{x} \in \mathbb{C}^n$ such that $A\boldsymbol{x} = \boldsymbol{b}$. Then $AA^\dagger\boldsymbol{b} = (AA^\dagger)(A\boldsymbol{x}) = (AA^\dagger A)\boldsymbol{x}$. By the first of the Moore–Penrose equations, $AA^\dagger A = A$ and therefore $AA^\dagger\boldsymbol{b} = A\boldsymbol{x} = \boldsymbol{b}$.*

Now suppose $A\boldsymbol{x} = \boldsymbol{b}$. Then $\boldsymbol{x} - A^\dagger\boldsymbol{b} \in$ null(A). By Theorem (12.14), null$(A) =$ col$(I_n - A^\dagger A)$ and there is a vector $\boldsymbol{y} \in \mathbb{C}^n$ such that $\boldsymbol{x} - A^\dagger\boldsymbol{b} = (I_n - A^\dagger A)\boldsymbol{y}$.

We will make use of the pseudoinverse of a matrix when we develop the method of least squares.

For more on the topics introduced in this section as well as extensions to other generalizations of the inverse of a matrix, see ([4]) and ([16]).

Exercises

1. Assume P is a Hermitian matrix and $\mu_P(x) = x^2 - x$. Prove that $P^\dagger\ = P$.

2. Assume $D = diag\{d_1, \ldots, d_r, 0, \ldots, 0\}$ is a diagonal matrix of rank r with non-zero diagonal entries $d_1, \ldots, d_r$. Prove that $D^\dagger = diag\{\frac{1}{d_1}, \ldots, \frac{1}{d_r}, 0, \ldots, 0\}$.

3. Assume $\boldsymbol{v} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ is a non-zero vector in $\mathbb{C}^n$. Prove that $\boldsymbol{v}^\dagger = \frac{1}{\|\boldsymbol{v}\|^2}(\overline{a_1}, \dots, \overline{a_n})$.

4. Assume A is an invertible $n \times n$ matrix. Prove that $A^\dagger = A^{-1}$.

5. Prove part ii) of Theorem (12.10).

In 6 and 7 below let A be an $m \times n$ complex matrix. Set $P = AA^\dagger$.

6. Prove algebraically, that $P^2 = P = P^*$.

7. Prove algebraically that $(I_m - P)^2 = I_m - P = (I_m - P)^*$.

In Exercises 8–11 assume that A is an $m \times n$ complex matrix.

8. Prove that $(A^*)^\dagger = (A^\dagger)^*$.

9. $(A^*A)^\dagger = A^\dagger (A^*)^\dagger$.

10. $A^* = A^*(AA^\dagger) = (A^\dagger A)A^*$.

11. $A^\dagger = (A^*A)^\dagger A^* = A^*(AA^*)^\dagger$.

12. Assume A is a normal matrix ($AA^* = A^*A$). Prove $AA^\dagger = A^\dagger A$.

13. Assume A is a normal matrix and n is a natural number. Prove that $(A^n)^\dagger = (A^\dagger)^n$.

14. Let A be an $m \times n$ complex matrix and $\lambda \neq 0$ a complex number. Prove that $(\lambda A)^\dagger = \frac{1}{\lambda}A^\dagger$.

15. Let A be a complex $m \times n$ matrix. Prove that $A^\dagger = A^*$ if an only if $(A^*A)^2 = A^*A$.

12.3 Nonnegative Matrices

In this section we study the properties of real matrices, all of whose entries are non-negative. These matrices play an important role in many applications such as Markov chains, text retrieval, and search engine optimization.

What You Need to Know

Understanding the new material in this section depends on a mastery of the following concepts: product of a matrix and a vector, product of two matrices, eigenvalue of a square matrix, eigenvector of a square matrix, characteristic polynomial of a square matrix, division algorithm of polynomials, the Euclidean inner product on $\mathbb{R}^n$, the l_1 norm on $\mathbb{R}^n$, range of a function, continuity of a function between normed spaces, convexity of a subset of $\mathbb{R}^n$, a subset of $\mathbb{R}^n$ is compact, and the Brouwer fixed point theorem. The latter material can be found in Appendix A.

We begin with several definitions.

Definition 12.8 *A matrix $A \in M_{mn}(\mathbb{R})$ is* **nonnegative** *if every entry of A is nonnegative and we write $A \geq 0$. The matrix A is said to be* **positive***, and we write $A > 0$, if every entry is positive. Note that this applies to the case where $n = 1$ so we can talk about nonnegative and positive vectors in $\mathbb{R}^n$.*

Definition 12.9 *Let* $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$ *be a complex matrix. We will denote by $|A|$ the nonnegative matrix whose (i, j) term is $|a_{ij}|$. Note that this applies to the case that $n = 1$, that is, to vectors in $\mathbb{C}^n$.*

Definition 12.10 *A nonnegative square matrix A is* **irreducible** *if for every pair (i, j) there is a natural number k such that the (i, j)-entry of A^k is positive. A nonnegative square matrix which is not irreducible is said to be* **reducible**.

Let $\boldsymbol{e}_i$ denote the i^{th} standard basis vector of $\mathbb{R}^n$, that is, the vector all of whose entries are zero except the i^{th}, which is one. Further, let $\langle\ ,\ \rangle$ be the Euclidean inner product on $\mathbb{R}^n$ so that $\langle \boldsymbol{e}_i, \boldsymbol{e}_j \rangle$ is zero unless $i = j$, in which case it is 1. The following gives a characterization of irreducibility in terms of the inner product $\langle\ ,\ \rangle$.

Lemma 12.4 *Let A be an $n \times n$ nonnegative matrix. Then A is irreducible if for every pair natural numbers i, j such that $1 \leq i, j \leq n$ there exists a natural number k such that $\langle A^k \boldsymbol{e}_j, \boldsymbol{e}_i \rangle > 0$.*

Proof *This follows immediately since the (i, j)-entry of A^k is $\langle A^k \boldsymbol{e}_j, \boldsymbol{e}_i \rangle$.*

Example 12.5 *Clearly, if A is a nonnegative square matrix and for some natural number k, A^k is positive then A is irreducible. On the other hand, if $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ then A is irreducible but A^k is never positive.*

Example 12.6 *The matrix $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is reducible.*

Because of their importance we give a name to nonnegative matrices A such that $A^k > 0$ for some natural number k.

Definition 12.11 *Let A be an $n \times n$ nonnegative matrix. A is said to be* **primitive** *if A^k is positive for some natural number k.*

The next result follows from the triangle inequality.

Lemma 12.5 *Let $A \in M_{lm}(\mathbb{C}), B \in M_{mn}(\mathbb{C})$. Then $|AB| \leq |A||B|$.*

Proof *We first prove the result for $n = 1$, that is, where $B = \boldsymbol{x} \in \mathbb{C}^m$. Let $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$ and $A = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \dots & \vdots \\ a_{l1} & \dots & a_{lm} \end{pmatrix}$. Then the i^{th} entry of $A\boldsymbol{x}$ is $\sum_{j=1}^m x_j a_{ij}$ so that the i^{th} entry of $|A\boldsymbol{x}|$ is $|\sum_{j=1}^m x_j a_{ij}|$ which by the triangle inequality is less than or equal to $\sum_{j=1}^m |x_j a_{ij}| = \sum_{j=1}^m |x_j||a_{ij}|$, which is the i^{th} entry of $|A||\boldsymbol{x}|$.*

Now suppose B has columns $\boldsymbol{b}_1, \dots, \boldsymbol{b}_n$. Then the j^{th} column of AB is $A\boldsymbol{b}_j$. Whence the j^{th} column of $|AB|$ is $|A\boldsymbol{b}_j|$. By what we have shown, $|A\boldsymbol{b}_j| \leq |A||\boldsymbol{b}_j|$, which is the j^{th} column of $|A||B|$.

The following characterizes nonnegative and positive matrices:

Theorem 12.16 *Let $A \in M_{mn}(\mathbb{R})$. Then $A \geq 0$ if and only if $A\boldsymbol{x} \geq 0$ for all $\boldsymbol{x} \geq 0$ in $\mathbb{R}^n$. Also, $A > 0$ if and only if $A\boldsymbol{x} > 0$ for all $\boldsymbol{x} \geq 0, \boldsymbol{x} \neq \mathbf{0}_n$.*

Proof *Clearly, if $A \geq 0$ and $\boldsymbol{x} \geq 0$ then $A\boldsymbol{x} \geq 0$. Assume conversely that $A\boldsymbol{x} \geq 0$ for every $\boldsymbol{x} \geq 0$. Then, in particular, $A\boldsymbol{e}_j \geq 0$. However, $A\boldsymbol{e}_j$ is the j^{th} column of A. Consequently, all the entries in A are nonnegative.*

Now assume $A > 0$ and $\boldsymbol{x} \geq 0, \boldsymbol{x} \neq \mathbf{0}_n$. Then there exists i such that $x_i \neq 0$. Then the 1^{st} entry of $A\boldsymbol{x}$ is greater than or equal to $x_i a_{1i} > 0$.

The following is a fundamental result:

Theorem 12.17 *Assume $A \in M_{nn}(\mathbb{R})$ is nonnegative and irreducible. Then $(I_n + A)^{n-1} > 0$.*

Proof *Suppose to the contrary that there exists i, j such that the (i, j)-entry of $(I_n + A)^{n-1}$ is zero. Since I_n and A commute, we have*

$$(I_n + A)^{n-1} = \sum_{k=0}^{n-1} \binom{n-1}{k} A^k.$$

The (i, j)-entry of $(I_n + A)^{n-1}$ is

$$\left\langle \sum_{k=0}^{n-1} A^k \boldsymbol{e}_j, \boldsymbol{e}_i \right\rangle = \sum_{k=0}^{n-1} \binom{n-1}{k} \langle A^k \boldsymbol{e}_j, \boldsymbol{e}_i \rangle = 0.$$

Since $\langle A^k \boldsymbol{e}_j, \boldsymbol{e}_i \rangle \geq 0$ it follows for $0 \leq k \leq n-1$ that $\langle A^k \boldsymbol{e}_j, \boldsymbol{e}_i \rangle = 0$. This implies for every polynomial $f(x)$ of degree less than or equal $n-1$ that $\langle f(A)\boldsymbol{e}_j, \boldsymbol{e}_i \rangle = 0$. Now let $g(x)$ be an arbitrary polynomial. We claim that $\langle g(A)\boldsymbol{e}_j, \boldsymbol{e}_i \rangle = 0$. Let $\chi_A(x)$ be the characteristic polynomial of A. Using the division algorithm write $g(x) = q(x)\chi_A(x) + r(x)$ where $r(x) = 0$ or $deg(r(x)) \leq n-1$. Then $g(A) = r(A)$. If $r(x) = 0$ then clearly $\langle r(A)\boldsymbol{e}_j, \boldsymbol{e}_i \rangle = 0$. So assume $r(x) \neq 0$ so that $deg(r(x)) < n$. Then $\langle g(A)\boldsymbol{e}_j, \boldsymbol{e}_i \rangle = \langle r(A)\boldsymbol{e}_j, \boldsymbol{e}_i \rangle = 0$ by what we have shown. In particular, for every natural number k, $\langle A^k \boldsymbol{e}_j, \boldsymbol{e}_i \rangle = 0$ which contradicts the assumption that A is irreducible.

We now turn our attention to results about eigenvalues of a square nonnegative matrix. The following result, a corollary of Theorem (12.17), will be used in the proof of the strong version of the Perron–Frobenius theorem.

Corollary 12.3 *Assume A is an irreducible nonnegative matrix and $\boldsymbol{x} \geq 0$ is an eigenvector of A. Then $\boldsymbol{x} > 0$.*

Proof *Assume $\boldsymbol{x} \geq 0$ and $A\boldsymbol{x} = \gamma\boldsymbol{x}$. Since A is irreducible and nonnegative, $A\boldsymbol{x} \neq \boldsymbol{0}_n$ and therefore $\gamma > 0$. Then $\boldsymbol{x}$ is an eigenvector of $I_n + A$ with eigenvalue $1 + \gamma$ and an eigenvector of $(I_n + A)^{n-1}$ with eigenvalue $(1 + \gamma)^{n-1}$. Thus, $\boldsymbol{x}$ is an eigenvector of $\frac{1}{(1+\gamma)^{n-1}}(I_n + A)^{n-1}$ with eigenvalue 1. By Theorem (12.17), the matrix $(I_n + A)^{n-1}$ is a positive matrix. Since $\boldsymbol{x} \geq 0$ and $\boldsymbol{x} \neq \boldsymbol{0}_n$, it follows that $(I_n + A)^{n-1}\boldsymbol{x}$ is a positive vector, hence $\boldsymbol{x}$ is a positive vector.*

We now prove the weak version of the Perron–Frobenius theorem. It requires some knowledge of analysis, in particular, the notion of continuity, convexity, compactness, as well as Brouwer's fixed point theorem. We refer the reader not familiar with these concepts and results to Appendix A.

Theorem 12.18 *Let $A \in M_{nn}(\mathbb{R})$ be a nonnegative matrix. Then $\rho(A)$, the spectral radius of A, is an eigenvalue of A and has a nonnegative eigenvector.*

Proof *Let λ be an eigenvalue with $|\lambda| = \rho(A)$ and let $\boldsymbol{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$ be an eigenvector with eigenvalue λ such that $\parallel \boldsymbol{v} \parallel_1 = \sum_{i=1}^n |v_i| = 1$. We then have $\rho(A)|\boldsymbol{v}| = |\lambda\boldsymbol{v}| = |A\boldsymbol{v}| \leq A|\boldsymbol{v}|$.*

Let $\mathcal{C}$ consist of all those $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$ such that $\boldsymbol{x} \geq 0, \sum_{i=1}^n x_i = 1$, and $A\boldsymbol{x} \geq \rho(A)\boldsymbol{x}$. Since $\boldsymbol{v} \in \mathcal{C}$, in particular, $\mathcal{C}$ is non-empty. It is also closed and convex, that is, for any $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}$ and real number $t, 0 \leq t \leq 1, t\boldsymbol{x} + (1-t)\boldsymbol{y} \in \mathcal{C}$. Moreover, $\mathcal{C}$ is bounded since for $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathcal{C}, 0 \leq x_i \leq 1$. Thus, $\mathcal{C}$ is a compact subset of $\mathbb{R}^n$.

Suppose first that $\boldsymbol{x} \in \mathcal{C} \cap null(A)$. Then $A\boldsymbol{x} = \boldsymbol{0}_n$. Since $A\boldsymbol{x} \geq \rho(A)\boldsymbol{x}$ it follows that $\rho(A)\boldsymbol{x} \leq 0$ from which we conclude that $\rho(A) = 0$ and A is the zero matrix. We may therefore assume for $\boldsymbol{x} \in \mathcal{C}$ that $A\boldsymbol{x} \neq \boldsymbol{0}_n$. Define a map $f : \mathcal{C} \to \mathbb{R}^n$ by

$$f(\boldsymbol{x}) = \frac{1}{\parallel A\boldsymbol{x} \parallel_1} A\boldsymbol{x}.$$

We claim that $Range(f) \subset \mathcal{C}$. First of all, since $\parallel A\boldsymbol{x} \parallel_1 > 0, A$ is nonnegative, and $\boldsymbol{x}$ is nonnegative, it follows that $f(\boldsymbol{x}) \geq 0$. Also, $\parallel f(\boldsymbol{x}) \parallel_1 = 1$. Moreover,

$$Af(\boldsymbol{x}) = \frac{1}{\parallel A\boldsymbol{x} \parallel_1} A(A\boldsymbol{x}) \geq \frac{1}{\parallel A\boldsymbol{x} \parallel_1} A[\rho(A)\boldsymbol{x}] = \rho(A)f(\boldsymbol{x}).$$

Thus, $f(\mathcal{C}) \subset \mathcal{C}$ as claimed. Note that f is a continuous function. Since $\mathcal{C}$ is convex, closed, and bounded, we can apply Brouwer's fixed point theorem, Theorem (A.5), to obtain a vector $\boldsymbol{x} \in \mathcal{C}$ such that $f(\boldsymbol{x}) = \boldsymbol{x}$. Since $\boldsymbol{x} \in \mathcal{C}, \boldsymbol{x}$ is a nonnegative vector. By the definition of f we have $A\boldsymbol{x} = \parallel A\boldsymbol{x} \parallel_1 \boldsymbol{x}$ so that $\boldsymbol{x}$ is an eigenvector of A with eigenvalue $\gamma = \parallel A\boldsymbol{x} \parallel_1$. Since $\boldsymbol{x} \in \mathcal{C}$ we have $\gamma\boldsymbol{x} = A\boldsymbol{x} \geq \rho(A)\boldsymbol{x}$. Consequently, $\gamma \geq \rho(A)$. Since $\rho(A) \geq |\gamma| = \gamma$ we get the equality $\rho(A) = \gamma$, which completes the proof.

Our next result is the strong version of the Perron–Frobenius theorem. With the additional hypothesis that A is irreducible we can prove that the algebraic multiplicity of $\rho(A)$ is one, among other conclusions.

Theorem 12.19 *Let $A \in M_{nn}(\mathbb{R})$ be nonnegative and irreducible. Then $\rho(A)$ is a simple eigenvalue for A and among its eigenvectors (all multiples of one another) there is a positive vector.*

Proof *For a nonnegative real number r, let $\mathcal{C}_r$ consist of those vectors $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ in $\mathbb{R}^n$ such that $\boldsymbol{x} \geq 0, \parallel \boldsymbol{x} \parallel_1 = \sum_{i=1}^n |x_i| = 1$, and $A\boldsymbol{x} \geq r\boldsymbol{x}$.*

Each $\mathcal{C}_r$ is a convex, closed, and bounded (hence compact) subset of $\mathbb{R}^n$. Suppose γ is an eigenvalue of A with associated eigenvector $\boldsymbol{x}$ such that $\parallel \boldsymbol{x} \parallel_1 = 1$. Then $A|\boldsymbol{x}| \geq |A\boldsymbol{x}| = |\gamma\boldsymbol{x}| = |\gamma||\boldsymbol{x}|$. We can therefore conclude that $|\boldsymbol{x}| \in \mathcal{C}_{|\gamma|}$. It follows from Theorem (12.18) that $\mathcal{C}_{\rho(A)}$ is nonempty. On the other hand, suppose r is a positive real number and $\boldsymbol{x} \in \mathcal{C}_r$. Then

$$r = r \parallel \boldsymbol{x} \parallel_1 \quad \leq \quad \parallel A\boldsymbol{x} \parallel_1 \quad \leq \quad \parallel A \parallel_1 \parallel \boldsymbol{x} \parallel_1 \quad = \quad \parallel A \parallel_1 .$$

Consequently, $r \leq \parallel A \parallel_1$. Clearly, for $s < r$, $\mathcal{C}_r \subset \mathcal{C}_s$. Moreover, if $0 < r \leq \parallel A \parallel_1$ then

$$\mathcal{C}_r = \bigcap_{0 \leq s < r} \mathcal{C}_s.$$

Let Λ be the least upper bound of $\{r|\mathcal{C}_r \neq \emptyset\}$. Since $\mathcal{C}_{\rho(A)} \neq \emptyset, \rho(A) \leq \Lambda$ and therefore $\rho(A) \leq \Lambda \leq \parallel A \parallel_1$. We remark that since $\mathcal{C}_\Lambda$ is an intersection of a totally ordered family of nonempty compact sets, $\mathcal{C}_\Lambda$ is nonempty. It is our immediate goal to prove that $\Lambda \neq 0$ and if $\boldsymbol{x} \in \mathcal{C}_\Lambda$ then $\boldsymbol{x}$ is an eigenvector with eigenvalue Λ.

Suppose to the contrary that $\Lambda = 0$. Let $\boldsymbol{x} \in \mathcal{C}_\Lambda$. Since A is irreducible and nonnegative and $\boldsymbol{x} \geq 0$ it follows that $A\boldsymbol{x} \neq \mathbf{0}_n$. Set $\boldsymbol{y} = (I_n + A)^{n-1}\boldsymbol{x}$. Since $\boldsymbol{x} \geq 0, \boldsymbol{x} \neq \mathbf{0}_n$, and $(I_n + A)^{n-1}$ is positive by Theorem (12.17) it follows that $\boldsymbol{y} > 0$. Also, $A\boldsymbol{y} = A(I_n + A)^{n-1}\boldsymbol{x} = (I_n + A)^{n-1}A\boldsymbol{x}$ is positive. Write $\boldsymbol{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ and $A\boldsymbol{y} = \begin{pmatrix} y_1' \\ \vdots \\ y_n' \end{pmatrix}$. Let s be the minimum of $\frac{y_i'}{y_i}$. Clearly $s > 0$. We have $A\boldsymbol{y} \geq s\boldsymbol{y}$ and therefore $\frac{1}{\|\boldsymbol{y}\|_1}\boldsymbol{y} \in \mathcal{C}_s$ which contradicts the assumption that $\Lambda = 0$.

Now suppose $\Lambda > 0, \boldsymbol{x} \in \mathcal{C}_\Lambda$ but $A\boldsymbol{x} \neq \Lambda\boldsymbol{x}$. Since $\boldsymbol{x} \in \mathcal{C}_\Lambda, A\boldsymbol{x} \geq \Lambda\boldsymbol{x}$. Since $A\boldsymbol{x} \neq \Lambda\boldsymbol{x}, A\boldsymbol{x} - \Lambda\boldsymbol{x} \geq 0$ and $A\boldsymbol{x} - \Lambda\boldsymbol{x} \neq \mathbf{0}_n$. Set $\boldsymbol{y} = (I_n + A)^{n-1}\boldsymbol{x}$. As we have seen, $\boldsymbol{y} > 0$. Similarly, $A\boldsymbol{y} - \Lambda\boldsymbol{y} = (I_n + A)^{n-1}(A\boldsymbol{x} - \Lambda\boldsymbol{x})$ is a positive vector. Write $\boldsymbol{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ and $A\boldsymbol{y} = \begin{pmatrix} y_1' \\ \vdots \\ y_n' \end{pmatrix}$. Let s be the minimum of $\frac{y_i'}{y_i}$. Clearly $s > 0$. We have $A\boldsymbol{y} \geq s\boldsymbol{y}$ and therefore $\frac{1}{\|\boldsymbol{y}\|_1}\boldsymbol{y} \in \mathcal{C}_s$. However, $A\boldsymbol{y} - s\boldsymbol{y} \geq 0$ but is not positive and therefore $s > \Lambda$, which contradicts the assumption that $\Lambda = sup\{r|\mathcal{C}_r \neq \emptyset\}$. This proves that $A\boldsymbol{x} = \Lambda\boldsymbol{x}$.

As stated above, since $\mathcal{C}_\Lambda \neq \emptyset$ we have $\rho(A) \leq \Lambda$. On the other hand, $\Lambda = |\Lambda| \leq \rho(A)$ so we may conclude that $\Lambda = \rho(A)$. Thus, $\rho(A)$ is an eigenvalue of A associated to the vector $\boldsymbol{x}$. By Corollary (12.3), $\boldsymbol{x}$ is a positive vector. It remains to show that the algebraic multiplicity of $\rho(A)$ is one.

We first prove that the geometric multiplicity of $\rho(A)$ is one. Suppose to the contrary that $\boldsymbol{y}$ is an eigenvector for $\rho(A)$ and $\boldsymbol{y}$ is not a multiple of $\boldsymbol{x}$. Suppose $\boldsymbol{y} \geq 0$. Then by Corollary (12.3), we must have $\boldsymbol{y} > 0$. We will get a contradiction. Let $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ and $\boldsymbol{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$. Let s be the minimum of $\{\frac{y_i}{x_i}|1 \leq i \leq n\}$ and assume $s = \frac{y_j}{x_j}$. Then the j^{th} component of $-s\boldsymbol{x} + \boldsymbol{y}$ is zero and all other components are nonnegative. Moreover, since $\boldsymbol{y} \neq s\boldsymbol{x}, -s\boldsymbol{x} + \boldsymbol{y} \neq \mathbf{0}_n$. Thus, $-s\boldsymbol{x} + \boldsymbol{y}$ is nonnegative, but not positive and an eigenvector for $\rho(A)$ which contradicts Corollary (12.3). Consequently, we can assume that some component of $\boldsymbol{y}$ is negative. Let t be the minimum of $\{\frac{y_i}{x_i}|1 \leq i \leq n\}$ and assume $t = \frac{y_j}{x_j}$. Then the j^{th} component of $-t\boldsymbol{x} + \boldsymbol{y}$ is zero and every other component is nonnegative and we again have a contradiction. Thus, the geometric multiplicity of $\rho(A)$ is one.

Suppose there exists a nonnegative vector $\boldsymbol{y}$ such that $A\boldsymbol{y} > \rho(A)\boldsymbol{y}$. Let $A\boldsymbol{y} = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$, s be the minimum of $\frac{y_i}{z_i}$, and let j be an index such that $s = \frac{z_i}{y_i}$. It *then follows that $s > \rho(A)$ and $A\boldsymbol{y} \geq s\boldsymbol{y}$. Normalizing $\boldsymbol{y}$ we get a vector $\boldsymbol{y}'$ in $\mathcal{C}_s$ which contradicts the assumption that $\rho(A) = \Lambda$ is the sup of $\{r \mid \mathcal{C}_r \neq \emptyset\}$.*

Suppose now that the algebraic multiplicity of $\rho(A)$ is greater than one. Then there exists a vector $\boldsymbol{y}$ such that $\mu_{\boldsymbol{y}}(x) = (x - \rho(A))^2$. Since $(A - \rho(A)I_n)\boldsymbol{y}$ is a eigenvector, we can assume that $A\boldsymbol{y} - \rho(A)\boldsymbol{y} = \boldsymbol{x}$. As shown above, it cannot be the case that $\boldsymbol{y} \geq 0$. Let $\boldsymbol{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$. Then some $\boldsymbol{y}_i < 0$. Let m be the minimum of $\{\frac{y_i}{x_i} | 1 \leq i \leq n\}$ and assume that $m = \frac{y_j}{x_j}$. Set $\boldsymbol{y}' = -m\boldsymbol{x} + \boldsymbol{y}$. Then $\boldsymbol{y}' \geq 0$ and $(A - \rho(A)I_n)\boldsymbol{y}' = \boldsymbol{x}$ and we have a final contradiction.

Remark 12.7 *If A is an $n \times n$ nonnegative and irreducible matrix then A^{tr} is a nonnegative and irreducible matrix.*

Definition 12.12 *Let A be an $n \times n$ nonnegative and irreducible matrix and set $\rho = \rho(A)$. A positive vector $\boldsymbol{x}$ with $\parallel \boldsymbol{x} \parallel_1 = 1$ such that $A\boldsymbol{x} = \rho\boldsymbol{x}$ is a* **right Perron vector**. *A positive vector $\boldsymbol{y}$ with such that $A^{tr}\boldsymbol{y} = \rho\boldsymbol{y}$ and $\langle \boldsymbol{y}, \boldsymbol{x} \rangle = \boldsymbol{y}^{tr}\boldsymbol{x} = 1$ is a* **left Perron vector**.

Let A be an irreducible nonnegative matrix with spectral radius $\rho = \rho(A)$. It is a natural question to ask whether there can be other eigenvalues γ of A such that $|\gamma| = \rho$. The answer is certainly yes as illustrated by the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, which has eigenvalues ±1. What is perhaps surprising is the existence of other such eigenvalues dictates that A is similar by a permutation matrix to a matrix with a very special form. We state this result but omit its proof. The interested reader can find a proof in ([19])

Theorem 12.20 *Assume A is an irreducible nonnegative matrix with spectral radius $\rho = \rho(A)$. Let $S_\rho(A) = \{\gamma \in Spec(A) || \gamma| = \rho\}$. Assume that the cardinality of $S_\rho(A)$ is p. Then $S_\rho(A) = \{e^{\frac{2\pi k}{p}} | 0 \leq k < p\}$. Each eigenvalue $\gamma \in S_\rho(A)$ is simple. $Spec(A)$ is invariant under multiplication by $\{e^{\frac{2\pi K}{p}} | 0 \leq k < p\}$. Moreover, A is similar by a permutation matrix to a block diagonal matrix with the following cyclic form*

$$\begin{pmatrix} 0 & A_1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & & & \ddots & A_{p-1} \\ A_p & 0 & \dots & \dots & 0 \end{pmatrix}.$$

We will make use of the following result when we discuss Markov chains.

Theorem 12.21 *Let A be an $n \times n$ nonnegative and primitive matrix with spectral radius ρ. Assume $\boldsymbol{x}, \boldsymbol{y}$ are the right and left Perron vectors, respectively. Then*

$$\lim_{k\to\infty} [\frac{1}{\rho}A]^k = \boldsymbol{x}\boldsymbol{y}^{tr}.$$

Note that $\boldsymbol{x}\boldsymbol{y}^{tr}$ is a rank one matrix.

Proof *Let $\mathcal{S}$ be the standard basis for $V = \mathbb{R}^n$ and let $T : V \to V$ be the operator such that $T(\boldsymbol{v}) = A\boldsymbol{v}$. Since $\boldsymbol{y}^{tr}\boldsymbol{x} = 1$ by Exercise 14 of Section (5.6) there is an invertible operator $R : V \to V$ such that $R(\boldsymbol{e}_1) = \boldsymbol{x}, R^*(\boldsymbol{y}) = \boldsymbol{e}_1$. Set $\mathcal{B} = (R(\boldsymbol{e}_1), \dots, R(\boldsymbol{e}_n)) = (\boldsymbol{x}, R(\boldsymbol{e}_2), \dots, R(\boldsymbol{e}_n))$. Let $Q = \mathcal{M}_R(\mathcal{S}, \mathcal{S}) = \mathcal{M}_{I_V}(\mathcal{B}, \mathcal{S})$. Then $Q^{tr} = \mathcal{M}_{R^*}(\mathcal{S}, \mathcal{S})$. The first column of Q is $\boldsymbol{x}$ and the first row of Q^{-1} is $\boldsymbol{y}^{tr}$. Set $B = Q^{-1}AQ = \mathcal{M}_T(\mathcal{B}, \mathcal{B})$ which has the form*

$$\begin{pmatrix} \rho & \mathbf{0}_{n-1}^{tr} \\ \mathbf{0}_{n-1} & C \end{pmatrix}.$$

Then $A = QBQ^{-1}$. Let $Q = \begin{pmatrix} \boldsymbol{x} & Q_1 \end{pmatrix}$ and $Q^{-1} = \begin{pmatrix} \boldsymbol{y}^{tr} \\ R_1^{tr} \end{pmatrix}$. Then

$$[\frac{1}{\rho}A]^m = Q \begin{pmatrix} 1 & \mathbf{0}_{n-1}^{tr} \\ \mathbf{0}_{n-1} & (\frac{1}{\rho}C)^m \end{pmatrix} Q^{-1}.$$

Since eigenvalues of C are eigenvalues of $A, \rho(C) < \rho(A)$ and consequently, every eigenvalue of $\frac{1}{\rho}C$ is less than one. Therefore the limit of $(\frac{1}{\rho}C)^m$ is $0_{(n-1)\times(n-1)}$. It then follows that

$$\lim_{k\to\infty} [\frac{1}{\rho}A]^k = Q \begin{pmatrix} 1 & \mathbf{0}_{n-1}^{tr} \\ \mathbf{0}_{n-1} & 0_{(n-1)\times(n-1)} \end{pmatrix} Q^{-1} =$$

$$\begin{pmatrix} \boldsymbol{x} & Q_1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0}_{n-1}^{tr} \\ \mathbf{0}_{n-1} & 0_{(n-1)\times(n-1)} \end{pmatrix} \begin{pmatrix} \boldsymbol{y}^{tr} \\ R_1^{tr} \end{pmatrix} = \boldsymbol{x}\boldsymbol{y}^{tr}.$$

Stochastic Matrices and Markov Chains

Nonnegative matrices have many applications, for example, to modeling population growth and to the creation of page rank algorithms. The latter makes use of stochastic matrices and the notion of a Markov process. We introduce these now.

Definition 12.13 *A nonnegative vector* $\boldsymbol{p} = \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix}$ *is a* **probability vector** *if* $p_1 + \cdots + p_n = 1$*.*

An $n \times n$ *real matrix* A *is said to be a* **column stochastic matrix** *if every column of* A *is a probability vector. An* $n \times n$ *real matrix* A *is said to be a* **row stochastic matrix** *if* A^{tr} *is column stochastic matrix.* A *is said to be* **doubly stochastic or bistochastic** *if* A *and* A^{tr} *are both stochastic.*

The following results about probability vectors and stochastic matrices are fundamental (but easy). We leave them as exercises.

Lemma 12.6 *Let* j_n *denote the real* n*-vector with all entries equal to one and let* $\boldsymbol{p}$ *be a nonnegative* n*-vector. Then* $\boldsymbol{p}$ *is a probability vector if and only if* $\langle \boldsymbol{p}, j_n \rangle = \boldsymbol{p}^{tr} j_n = 1$*.*

Lemma 12.7 *Let* $\boldsymbol{p}_1, \ldots \boldsymbol{p}_t$ *be probability vectors in* $\mathbb{R}^n$ *and* $(s_1, \ldots, s_t)$ *a nonnegative sequence of real numbers such that* $s_1 + \cdots + s_t = 1$*. Then* $s_1\boldsymbol{p}_1 + \cdots + s_t\boldsymbol{p}_t$ *is a probability vector.*

Corollary 12.4 *Let* A *be a stochastic matrix and* $\boldsymbol{p}$ *a probability vector. Then* $A\boldsymbol{p}$ *is a probability vector.*

Corollary 12.5 *Let* A *and* B *be stochastic matrices. Then* AB *is a stochastic matrix. In particular, for every natural number* k*,* A^k *is a stochastic matrix.*

In the theory of Markov chains with finite many states, central to the analysis is the existence of a **stationary vector**.

Definition 12.14 *Let* A *be a stochastic matrix. A probability vector* $\boldsymbol{p}$ *is a* **stationary vector** *if* $A\boldsymbol{p} = \boldsymbol{p}$*, that is, if* $\boldsymbol{p}$ *is an eigenvector of* A *with eigenvalue one.*

Remark 12.8 *Let* j_n *be the vector in* $\mathbb{R}^n$ *all of whose components are one and let* $\boldsymbol{p}$ *be a probability vector. Then* $\langle \boldsymbol{p}, j_n \rangle = \boldsymbol{p}^{tr} j_n = 1$*. It follows if* A *is a column stochastic matrix then* $A^{tr} j_n = j_n$ *so that* j_n *is an eigenvector of* A^{tr} *with eigenvalue one. Consequently, one is an eigenvalue of* A *as well. However, this does not prove the existence of a stationary vector since it is not immediately clear that an eigenvector of* A *for one is nonnegative. We make use of the Perron–Frobenius heorems to obtain a stationary vector.*

Theorem 12.22 *Let A be a stochastic matrix. Then $\rho(A) = 1$. Consequently, A has a stationary vector. If A is also irreducible then a stationary vector is unique.*

Proof *Set $r = \rho(A)$. By the weak form of the Perron–Frobenius theorem, Theorem (12.18), there is a probability vector $\boldsymbol{p}$ which is an eigenvector of A with eigenvalue r. Then $A\boldsymbol{p} = r\boldsymbol{p}$. Since A is stochastic, $A\boldsymbol{p}$ is a probability vector and $\parallel A\boldsymbol{p} \parallel_1 = 1$. On the other hand, $\parallel A\boldsymbol{p} \parallel_1 = \parallel r\boldsymbol{p} \parallel_1 = r \parallel \boldsymbol{p} \parallel_1 = r$. This proves that $r = 1$. The rest follows from the strong version of the Perron–Frobenius theorem.*

Definition 12.15 *A* **Markov chain** *consists of a sequence $(\boldsymbol{x}_0, \boldsymbol{x}_1, \boldsymbol{x}_2, \dots)$ of state vectors and a stochastic matrix A, called the* **transition matrix***, such that for every $k, \boldsymbol{x}_{k+1} = A\boldsymbol{x}_k$.*

Think of a Markov chain as modeling some process that changes over time with the state of the process recorded at discrete intervals of equal duration. We will need the following result later when we discuss how webpages are ranked by a search engine.

Theorem 12.23 *Let A be a primitive stochastic matrix with stationary vector $\boldsymbol{x}$. Let $\boldsymbol{z}$ be a probability vector. Then*

$$\lim_{k\to\infty} A^k\boldsymbol{z} = \boldsymbol{x}.$$

Proof *We first point out that $\rho(A) = 1$ has algebraic multiplicity one. The stationary vector $\boldsymbol{x}$ is the right Perron vector for A. The vector $\boldsymbol{j}_n = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$ is the left Perron vector. Note that since $\boldsymbol{x}$ is a probability vector, $\boldsymbol{j}_n^{tr}\boldsymbol{x} = 1$ and $\boldsymbol{x}\boldsymbol{j}_n^{tr}$ is the rank one matrix all of whose columns are $\boldsymbol{x}$. By Theorem (12.21)*

$$\lim_{k\to\infty} A^k = \boldsymbol{x}\boldsymbol{j}_n^{tr}.$$

If $\boldsymbol{z} = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$ is a probability vector then $z_1 + \cdots + z_n = 1$ and

$$\lim_{k\to\infty} A^k\boldsymbol{z} = \begin{pmatrix}\boldsymbol{x} & \boldsymbol{x} & \dots \boldsymbol{x}\end{pmatrix} \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} =$$

$$z_1\boldsymbol{x} + \cdots + z_n\boldsymbol{x} = (z_1 + \cdots + z_n)\boldsymbol{x} = \boldsymbol{x}.$$

Doubly Stochastic Matrices

We now turn our attention to doubly stochastic matrices. We will denote by Δ_n the collection of all doubly stochastic matrices in $\mathbb{R}^n$. We begin with a lemma.

Lemma 12.8 *Let $A_1, \dots, A_t$ be $n \times n$ doubly stochastic matrices and $(s_1, \dots, s_t)$ nonnegative real numbers such that $s_1 + \dots + s_t = 1$. Then $s_1A_1 + \dots + s_tA_t$ is doubly stochastic.*

Proof *Let $\boldsymbol{p}_{jk}$ denote the j^{th} column of A_k. By Lemma (12.7) it follows that $s_1\boldsymbol{p}_{j1} + \dots + s_t\boldsymbol{p}_{jt}$ is a probability vector. Thus, every column of $s_1A_1 + \dots + s_tA_t$ is a probability vector so $s_1A_1 + \dots + s_tA_t$ is stochastic. Applying the same argument to $(s_1A_1 + \dots + s_tA_t)^{tr} = s_1A_1^{tr} + \dots + s_tA_t^{tr}$ when the A_i are doubly stochastic yields the result.*

Another way to phrase Lemma (12.8) is that Δ_n is convex. Also note that Δ_n is contained in the set $\{\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} | 0 \leq a_{ij} \leq 1 \text{ for all } i, j\}$ and therefore Δ_n is bounded. It is also a closed subset of $M_{nn}(\mathbb{R})$ and hence compact.

Let $(\boldsymbol{e}_1, \dots, \boldsymbol{e}_n)$ be the standard basis of $\mathbb{R}^n$, that is, the sequence of columns of the identity matrix I_n. Let σ be a permutation of $\{1, 2, \dots, n\}$. Denote by P_σ the matrix with columns the sequence $(\boldsymbol{e}_{\sigma(1)}, \dots, \boldsymbol{e}_{\sigma(n)})$. Note that each of these is doubly stochastic. By Lemma (12.8) every matrix in the convex hull of $\{P_\sigma | \sigma \in S_n\}$ is also doubly stochastic. This is the easy half of the Birkoff–von Neumann theorem, to which we now turn.

Theorem 12.24 *A real $n \times n$ matrix A is doubly stochastic if and only if there are permutation matrices $P_{\sigma_1}, \dots, P_{\sigma_t}$ and nonnegative real numbers $s_1, \dots, s_t$ with $s_1 + \dots + s_t = 1$ such that $A = s_1P_{\sigma_1} + \dots s_tP_{\sigma_t}$.*

Proof *As mentioned, we only have to prove if A is doubly stochastic then there are permutation matrices $P_{\sigma_1}, \dots, P_{\sigma_t}$ and nonnegative real numbers $s_1, \dots, s_t$ with $s_1 + \dots + s_t = 1$ such that $A = s_1P_{\sigma_1} + \dots s_tP_{\sigma_t}$. Since Δ_n is convex and compact, by the Krein-Milman theorem, Theorem (A.4), Δ_n is the convex hull of its extreme points. Here a point $\boldsymbol{p}$ is extreme in a convex subset C of $\mathbb{R}^m$ if, whenever $\boldsymbol{x}, \boldsymbol{y} \in C$ and $0 \leq s \leq 1$ satisfies $\boldsymbol{p} = s\boldsymbol{x} + (1 - s)\boldsymbol{y}$, then $\boldsymbol{p} = \boldsymbol{x} = \boldsymbol{y}$. Clearly, the permutation matrices are extreme points of Δ_n so we need to prove that no other matrix in Δ_n is extreme.*

Assume $A \in \Delta_n$ and A is not a permutation matrix. Then there exists an entry a_{i_1,j_1} such that $0 < a_{i_1,j_1} < 1$. Since A is stochastic, there must be a $j_2 \neq j_1$ such that $0 < a_{i_1,j_2} < 1$. Since A^{tr} is stochastic, there must be an $i_2 \neq i_1$ such that $0 < a_{i_2,j_2} < 1$. We can continue this way to obtain a sequence $(j_1, i_1, j_2, i_2, \dots)$ such that $0 < a_{i_{t-1},j_t} < 1$ and $0 < a_{i_t,j_t} < 1$. Since n is finite, by the pigeonhole principle some row or column index must repeat. Suppose we obtain the sequence $(j_1, i_1, \dots, j_s, i_s, j_{s+1} = j_1)$. Let B be the matrix with entries b_{ij} so that $b_{i_t,j_t} = 1, b_{i_t,b_{t+1}} = -1$ and all other entries are zero. By construction, $Bj_n = \mathbf{0}_n = B^{tr}j_n$. Now for any real number $\gamma, (A + \gamma B)j_n = (A - \gamma B)j_n = (A + \gamma B)^{tr}j_n = (A - \gamma B)^{tr}j_n = j_n$. For small γ both $A + \gamma B$ and $A - \gamma B$ will be nonnegative. By Lemma (12.6) each column and row of $A + \gamma B$ and every column and row of $A - \gamma B$ is a probability vector. Thus, both $A + \gamma B$ and $A - \gamma B$ are stochastic matrices. Since $A = \frac{1}{2}(A + \gamma B) + \frac{1}{2}(A - \gamma B)$ it follows that A is not an extreme point of Δ_n which completes the proof.

Among others, some good references for the material of this section are ([4]), ([12]) and ([19]).

Exercises

In Exercises 1–3 let $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$ be a real nonnegative matrix. For natural numbers i, j, k with $1 \leq i, j \leq n$, denote by a_{ij}^k the (i, j)-entry of A^k.

1. Define a directed graph on $\{1, \dots, n\}$ as follows: $(i, j) \in \Delta$ if there is a natural number k such that $a_{ij}^k \neq 0$. Prove if $(i, j), (j, l) \in \Delta$ then $(i, l) \in \Delta$.

2. We continue with the notation of Exercise 1. For $i \in \{1, \dots, n\}$ denote by $\Delta(i)$ the collection of all j such that $(i, j) \in \Delta$. Suppose $j \in \Delta(i)$. Prove that $\Delta(j) \subset \Delta(i)$.

3. Assume A is reducible. Then for some $i, \Delta(i) \neq \{1, \dots, n\}$. Choose such an i with $\Delta(i)$ maximal and set $I = \Delta(i)$. Prove that $Span(\boldsymbol{e}_j | j \in I)$ is an A-invariant subspace of $\mathbb{R}^n$. Conclude that a nonnegative matrix A is reducible if and only if there is a proper subset I of $\{1, \dots, n\}$ such that $Span(\boldsymbol{e}_j | j \in I)$ is A-invariant.

4. Let A be an $n \times n$ nonnegative matrix and D a diagonal matrix with positive diagonal entries. Prove that A is irreducible if and only if AD is irreducible if and only if DA is irreducible.

5. Let A be an $n \times n$ nonnegative matrix and assume that $(I_n + A)^{n-1} > 0$. Prove A is irreducible.

6. Let A be a positive $m \times n$ matrix and $\boldsymbol{x}, \boldsymbol{y}$ real n-vectors such that $\boldsymbol{x} \geq \boldsymbol{y}$. Prove that $A\boldsymbol{x} \geq A\boldsymbol{y}$ with equality if and only if $\boldsymbol{x} = \boldsymbol{y}$.

7. Assume A is a nonnegative matrix and $A^k > 0$ for some natural number k. Prove that $\rho(A) > 0$.

8. Assume A is a nonnegative $n \times n$ matrix and A is not the zero matrix. Prove if A has a positive eigenvector then $\rho(A) > 0$.

9. Assume A is a nonnegative $n \times n$ matrix and $\boldsymbol{d} = \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix}$ is a positive eigenvector. Set $D = diag\{d_1, \dots, d_n\}$. Prove that $D^{-1}AD$ has constant row sums equal to $\rho(A)$.

10. Let A be a nonnegative irreducible matrix with spectral radius ρ. Assume if $\lambda \in Spec(A), \lambda \neq \rho$ then $|\lambda| < \rho$. Prove that there exists a natural number k such that A^k is a positive matrix.

11. Let $z_1, \dots, z_n \in \mathbb{C}^*$. Prove that $|z_1 + \cdots + z_n| = |z_1| + \cdots + |z_n|$ if and only if there is a $\theta \in [0, 2\pi)$ such that for all $i, e^{i\theta} z_i = |z_i|$.

12. Let A be a nonnegative irreducible matrix. Assume $\lambda \in Spec(A) \setminus \{\rho\}$. Then $|\lambda| < \rho$.

13. Prove Lemma (12.6).

14. Prove Lemma (12.7).

15. Prove Corollary (12.4).

16. Prove Corollary (12.5).

17. Assume A and B are (doubly) stochastic matrices. Prove that AB is a (doubly) stochastic matrix.

18. Assume A is an invertible $n \times n$ doubly stochastic matrix and that A^{-1} is doubly stochastic. Prove A is a permutation matrix.

19. Assume A is an $n \times n$ doubly stochastic matrix. Prove that A cannot have exactly $n + 1$ nonzero entries.

20. Prove that a 2×2 doubly stochastic matrix is symmetric with equal diagonal entries.

21. Assume A is a reducible doubly stochastic $n \times n$ matrix. Prove that A is permutation similar to a block matrix $\begin{pmatrix} A_1 & 0_{st} \\ 0_{ts} & A_2 \end{pmatrix}$ where $s + t = n, A_1$ is an $s \times s$ doubly stochastic matrix and A_2 is a doubly stochastic $t \times t$ matrix.

12.4 The Location of Eigenvalues

In applications of linear algebra it is often important to determine the eigenvalues of an operator or, equivalently, a matrix, for example when solving a linear system of differential equations. Of course, determining the eigenvalues of a diagonal or triangular matrix is easy. However, the problem is intractable for an arbitrary matrix, even one which is similar to a diagonal matrix. It is, of course, straightforward to determine the minimal and characteristic polynomials of a square matrix A, in fact, all the invariant factors. So, determining the eigenvalues reduces to factoring these polynomials. However, for any real or complex polynomial $f(x)$ of degree n there is an $n \times n$ matrix whose characteristic polynomial, $\chi_A(x)$, is equal to $f(x)$, namely, the companion matrix, $C(f(x))$, of the polynomial $f(x)$. We know that there is no algorithm for determining the roots of a polynomial of degree $n \geq 5$ by results of Abel and Galois. Therefore, one must be satisfied with approximating the eigenvalues. This section deals with the location of the eigenvalues of real and complex matrices (and therefore operators). Among other results we prove the Geršgorin Disc theorem which places the eigenvalues of a matrix in a union of discs in the complex plane determined in a simple manner from the entries of the matrix.

What You Need to Know

To make sense of the new material of this section is it essential that you have mastery of the following concepts: norm on a vector space, matrix norm, induced matrix norm, eigenvalue of a matrix or operator, an eigenvector of a matrix or operator.

We begin with a result which gives a bound for the spectral radius of a complex matrix A.

Theorem 12.25 *Let* $A \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$ *be an* $n \times n$ *complex matrix and assume* $\lambda_1, \dots, \lambda_n$ *are the roots of* $\chi_A(x)$. *Then*

$$\sum_{i=1}^{n} |\lambda_i|^2 \leq \sum_{i=1}^{n} \sum_{j=1}^{n} |a_{ij}|^2.$$

Proof *Note that* $\sum_{i=1}^n \sum_{j=1}^n |a_{ij}|^2 = Trace(A^*A)$ *is* $\parallel A \parallel_F^2$, *the Frobenius norm of* A. *By Lemma (6.8) there is a unitary matrix* Q *such that* $A = QTQ^*$, *where* $T = \begin{pmatrix} t_{11} & t_{12} & \dots & t_{1n} \\ 0 & t_{21} & \dots & t_{2n} \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & t_{nn} \end{pmatrix}$ *is an upper triangular matrix. Since* A *and* T *are similar* $(x - t_{11}) \dots (x - t_{nn}) = \chi_T(x) = \chi_A(x) = (x - \lambda_1) \dots (x - \lambda_n)$. *Consequently,*

$$\sum_{i=1}^{n} |\lambda_i|^2 = \sum_{i=1}^{n} |t_{ii}|^2 \leq \sum_{i=1}^{n}\sum_{j=1}^{n} |t_{ij}|^2 = Trace(T^*T).$$

Since $A^*A = (QT^*Q^*)(QTQ^*) = Q(T^*T)Q^*$, *it follows that* T^*T *and* A^*A *are similar. Therefore*

$$\sum_{i=1}^{n}\sum_{j=1}^{n} |t_{ij}|^2 = Trace(A^*A) = \sum_{i=1}^{n}\sum_{j=1}^{n} |a_{ij}|^2.$$

The following is an immediate consequence.

Corollary 12.6 *Let* A *be an* $n \times n$ *complex matrix. Then* $\rho(A) \leq Trace(A^*A) = \| A \|$ *where* $\| \cdot \|$ *is the Frobenius norm.*

The next result is due to S. Geršgorin and was proved in 1931. It locates the eigenvalues of a complex matrix in discs centered at the diagonal entries of the matrix. We begin with the definition of the Geršgorin discs of a matrix.

Definition 12.16 *Let* $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$ *be a complex matrix. For* $1 \leq i \leq n$, *the* i^{th} *deleted row sum is* $R_i'(A) = \sum_{j \neq i} a_{ij}$. *The* i^{th} *Geršgorin (row) disc is*

$$\Gamma_i(A) = \{z \in \mathbb{C} | |z - a_{ii}| \leq R_i'(A)\}.$$

The (row) Geršgorin set of A *is*

$$\Gamma(A) = \cup_{i=1}^{n} \Gamma_i(A).$$

Theorem 12.26 *Let* $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$. *Then* $Spec(A) \subset \Gamma(A)$. *Moreover, assume there is a partition* $\{I_1, I_2\}$ *of* $\{1, \dots, n\}$ *with* $|I_k| = n_k, k = 1, 2$ *such that* $[\cup_{i \in I_1} \Gamma_i(A)] \cap [\cup_{i \in I_2} \Gamma_i(A)] = \emptyset$. *Then* $\cup_{i \in I_k} \Gamma_i(A)$ *contains exactly* n_k *eigenvalues of* A *for* $k = 1, 2$.

Proof *Assume $\lambda \in Spec(A)$ and $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{C}^n$ is an eigenvector with eigenvalue λ. Let s be an index such that $\parallel \boldsymbol{x} \parallel_\infty = |x_s|$. Since $\boldsymbol{x} \neq \boldsymbol{0}, x_s \neq 0$. Then $|x_i| \leq |x_s|$ for $1 \leq i \leq n$. Since $\boldsymbol{x}$ is an eigenvector of A with eigenvalue λ, we have*

$$\sum_{j=1}^{n} a_{sj} x_j = \lambda x_s.$$

Consequently, $\sum_{j \neq s} a_{sj} x_j = (\lambda - a_{ss}) x_s$. We then have

$$\begin{aligned} |\lambda - a_{ss}||x_s| &= \left| \sum_{j \neq s} a_{sj} x_j \right| \\ &\leq \sum_{j \neq s} |a_{sj} x_j| \\ &= \sum_{j \neq s} |a_{sj}||x_j| \\ &\leq |x_s| \sum_{j \neq s} |a_{sj}| \\ &= |x_s| R'_s(A). \end{aligned}$$

Since $x_s \neq 0$, it follows that $|\lambda - a_{ss}| \leq R'_s(A)$, equivalently, $\lambda \in \Gamma_s(A)$. Since λ is arbitrary in $Spec(A)$, it follows that $Spec(A) \subset \Gamma(A)$.

We sketch the second part and refer the reader to ([21]) for a complete proof. Assume now that $\{1, \dots, n\} = I_1 \cup I_2$, $I_1 \cap I_2 = \emptyset$, so that $G_1 \cap G_2 = \emptyset$ where $G_k = \cup_{i \in I_k} \Gamma_i(A), k = 1, 2$. Set $n_k = |I_k|, k = 1, 2$. Replacing A with $P^{-1}AP$ for a permutation matrix P, if necessary, we can assume that $I_1 = \{1, \dots, n_1\}$ and $I_2 = \{n_1 + 1, \dots, n\}$.

Set $D = diag\{a_{11}, \dots, a_{nn}\}$ set $B = A - D$. Set $A(\gamma) = D + \gamma B$ with $0 \leq \gamma \leq 1$. Note that $A(0) = D$ and $A(1) = A$. Also note that $R'_i(A(\gamma)) = R'_i(\gamma B) = \gamma R'_i(A)$. Thus, the j^{th} Geršgorin disc of $A(\gamma)$ is given by

$$\Gamma_j(A(\gamma)) = \{z \in \mathbb{C} | |z - a_{ii}| \leq \gamma R'_i(A)\}.$$

It therefore follows that $\Gamma_j(A(\gamma)) \subset \Gamma_j(A)$. Consequently, $\cup_{j=1}^{n_1} \Gamma_j(A(\gamma))$ is contained in $\cup_{j=1}^{n_1} \Gamma_j(A)$ and is disjoint from $\cup_{j=n_1+1}^{n} \Gamma_j(A)$. Set $G_1 = \cup_{i=1}^{n} \Gamma_i(A)$ and $G_2 = \Gamma(A) \setminus G_1$. Let C be a smooth closed curve which contains G_1 and does not intersect G_1. Let $\chi_\gamma(x)$ denote the characteristic polynomial *of $A(\gamma)$, so $\chi_\gamma(x) = det(xI_n - A(\gamma)) = det(xI_n - D - \gamma B)$. This is a polynomial in γ. The number of zeros of $\chi_\gamma(x)$ inside C (equal to the number of roots of $\chi_\gamma(x) = 0$ in C), is given by*

$$\frac{1}{2\pi i}\oint_C \frac{\chi'_\gamma(x)}{\chi_\gamma(x)}dx.$$

This is an integer valued function on the interval [0,1] and therefore constant. Now $\chi_0(x) = (x-a_{11})\dots(x-a_{nn})$ has exactly n_1 zeros inside C and therefore so does $\chi_1(x) = \chi_A(x)$. Since these zeros must also belong to $\Gamma(A)$, in fact they lie in $\Gamma_1 = \cup_{i=1}^{n_1}\Gamma_i(A)$.

As a corollary to Theorem (12.26) we get an improved bound for the spectral radius of a complex matrix.

Corollary 12.7 *Let $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nn}\end{pmatrix}$. Then*

$$\rho(A) \leq max\left\{\sum_{j=1}^n |a_{ij}| 1 \leq i \leq n\right\}.$$

Proof *Assume $\lambda \in Spec(A)$. By Theorem (12.26) there is a k such that $|\lambda - a_{kk}| \leq R'_k(A)$. Then $|\lambda| - |a_{kk}| \leq |\lambda - a_{kk}| \leq R'_k(A)$. Therefore*

$$\lambda \leq |a_{kk}| + R'_k(A) = \sum_{j=1}^n |a_{kj}| \leq max\left\{\sum_{j=1}^n |a_{kj}||1 \leq k \leq n\right\}.$$

In particular, the inequality holds for $\lambda = \rho(A)$.

Remark 12.9 *We point out that*

$$max\left\{\sum_{j=1}^n |a_{kj}||1 \leq k \leq n\right\} = \parallel A \parallel_1 .$$

Since A and A^{tr} have the same invariant factors and characteristic polynomial, we can also locate the eigenvalues in discs arising from deleted column sums.

Definition 12.17 *Let* $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$ *be a complex matrix. If* $1 \leq j \leq n$ *then the* j^{th} *deleted column sum of* A *is*

$$C'_j(A) = \sum_{i \neq j} |a_{ij}| = R'_j(A^{tr}).$$

The j^{th} *(column) Geršgorin disc is*

$$\Delta_j(A) = \{z \in \mathbb{C} | |z - a_{jj}| \leq C'_j(A)\} = \Gamma_j(A^{tr}).$$

The (column) Geršgorin set is $\Delta(A) = \cup_{j=1}^{n} \Delta_j(A) = \Gamma(A^{tr})$.

Since $Spec(A^{tr}) = Spec(A)$, the proof of Theorem (12.26) applies to A^{tr}, from which we can conclude the following:

Theorem 12.27 *Let* $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$ *be a complex matrix. Then* $Spec(A) \subset \Delta(A)$.

Theorem (12.27) also gives a bound on the spectral radius.

Theorem 12.28 *Let* $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$ *be a complex matrix. Then*

$$\rho(A) \leq max \left\{ \sum_{i=1}^{n} |a_{ij}| | 1 \leq j \leq n \right\} = \| A \|_{\infty} .$$

Putting Theorem (12.7) and Theorem (12.28) together we get:

Theorem 12.29 *Let* $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$ *be a complex matrix. Then*

$$\rho(A) \leq min\{\| A \|_1, \| A \|_{\infty}\}.$$

Of course, since $Spec(A)$ is contained in $\Gamma(A)$ and $\Delta(A)$, it must be contained in $\Gamma(A) \cap \Delta(A)$. We state this as a theorem.

Theorem 12.30 *Let* $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$ *be a complex matrix.*

Then $Spec(A) \subset \Gamma(A) \cap \Delta(A)$.

Other inclusion theorems can be obtained by applying Theorem (12.26) to matrices which are similar to A. The following is an example.

Theorem 12.31 *Let* $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$ *be a complex matrix and* $\begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix}$ *be a positive real* n*-vector. Set* $D_i = \sum_{j \neq i} \frac{d_j}{d_i} |a_{ij}|$. *If* $\lambda \in Spec(A)$ *then there exists* i *such that* λ *is in the disc*

$$\{z \in \mathbb{C} | |z - a_{ii}| \leq D_i\}.$$

Proof *Set* $D = diag\{d_1, \dots, d_n\}$ *and* $B = D^{-1}AD$. *Then* $Spec(B) = Spec(A)$. *Apply Theorem (12.26) to* B.

Theorem (12.26) can be used to obtain a criterion for a matrix to be invertible by comparing diagonal elements to the deleted row sum for the row in which it occurs. Toward that end, we introduce a definition.

Definition 12.18 *Let* $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$ *be a complex matrix.* A *is* **strictly diagonally dominant** *if for every* $i, 1 \leq i \leq n$, *we have*

$$|a_{ii}| > R'_i(A).$$

Theorem 12.32 *Assume the complex matrix* $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$ *is strictly diagonally dominant. Then* A *is invertible.*

Proof *Suppose to the contrary that* A *is not invertible. Then 0 is an eigenvalue. By Theorem (12.26) there exists a* k *such that* $|0 - a_{kk}| = |a_{kk}| \leq R'_k(A)$, *a contradiction.*

Theorem (12.32) also implies Theorem (12.26). Suppose λ is an eigenvalue of A and $|\lambda - a_{kk}| > R'_k(A)$ for all k. Let $\boldsymbol{x} \neq \mathbf{0}_n$ be an eigenvector of A with eigenvaue λ. Then $(\lambda I_n - A)\boldsymbol{x} = \mathbf{0}_n$ so that $B = \lambda I_n - A$ is not invertible. Let b_{ij} denote the (i,j)-entry of B. Note that $R'_k(A) = R'_k(B)$. Then for every k we have $|b_{kk}| = |\lambda - a_{kk}| > R'_k(A) = R'_k(B)$ from which we conclude that B is invertible, a contradiction.

We complete this section with a theorem due to Ky Fan.

Theorem 12.33 *Let* $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$ *be a complex matrix and* $B = \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & \dots & \vdots \\ b_{n1} & \dots & b_{nn} \end{pmatrix}$ *a nonnegative real matrix. Assume* $b_{ij} \geq |a_{ij}|$ *for all* $i \neq j$. *Then for every eigenvalue* λ *of* A *there is an* i *such that* λ *is contained in the disc*

$$\{z \in \mathbb{C} | |z - a_{ii}| \leq \rho(B) - b_{ii}\}.$$

Morover, if $|a_{ii}| > \rho(B) - b_{ii}$ *for all* i *then* A *is invertible.*

Proof *First assume that* B *is a positive matrix. By the strong form of the Perron–theorem, Theorem (12.19), there is a positive vector* $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ *such that* $B\boldsymbol{x} = \rho(B)\boldsymbol{x}$. *Then for each* $i, 1 \leq i \leq n$ *we have*

$$\sum_{j \neq i} |a_{ij}| x_j \leq \sum_{j \neq i} b_{ij} x_j = \rho(B)\boldsymbol{x} - b_{ii} x_i.$$

Dividing both sides of the inequality by $\frac{1}{x_i}$ *we obtain for each* $i, 1 \leq i \leq n$, *that*

$$\frac{1}{x_i} \sum_{j \neq i} |a_{ij}| x_j \leq \rho(B) - b_{ii}.$$

The result now follows from Theorem (12.31) with $\begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix} = \boldsymbol{x}$.

We now treat the general case. Suppose some entry of B *is zero. Let* J *be the* $n \times n$ *matrix all of whose entries are one. Set* $B_\gamma = A + \gamma J$. *The* (i,j)*-entry of* B_γ *is* $b_{ij} + \gamma > b_{ij} \geq |a_{ij}|$ *for* $i \neq j$. *Clearly,* B_γ *is a real positive matrix.*

By what we have shown above, if λ is an eigenvalue of A then there is an i such that λ is in the disc

$$\{z \in \mathbb{C} | |z - a_{ii}| \leq \rho(B_\gamma) - (b_{ii} + \gamma)\}.$$

Now as γ approaches zero, $\rho(B_\gamma) - (b_{ii} + \gamma)$ has the limit $\rho(B) - b_{ii}$.

If $|a_{ii}| > \rho(B) - b_{ii}$ for every i then zero is not in the union of the discs and the last part of the theorem follows.

An excellent reference for the material of this section as well as a source of generalizations is ([21]).

Exercises

1. Assume A is a stochastic matrix and set $\delta = min\{a_{ii} | 1 \leq i \leq n\}$. Prove that $Spec(A)$ is contained in the disc

$$\{z \in \mathbb{C} | |z - \delta| \leq 1 - \delta\}.$$

2. Assume A is a stochastic matrix with diagonal entries all greater than $\frac{1}{2}$. Prove that A is invertible.

3. Let A be a complex $n \times n$ matrix and assume for all $i \neq j$ that $\Gamma_i(A) \cap \Gamma_j(A) = \emptyset$. Prove that A is diagonalizable.

4. Assume A is a real $n \times n$ matrix and for $i \neq j$ that $\Gamma_i(A) \cap \Gamma_j(A) = \emptyset$. Prove that $Spec(A) \subset \mathbb{R}$.

5. Let A be an $n \times n$ complex matrix. Prove that $Spec(A) = \cap_{Q \in GL_n(\mathbb{C})} \Gamma(Q^{-1}AQ)$.

6. Let A be a complex $n \times n$ matrix. Assume the following: a) the characteristic polynomial of $A, \chi_A(x)$, is a real polynomial; b) the diagonal entries of A are real; and c) for $i \neq j, \Gamma_i(A) \cap \Gamma_j(A) = \emptyset$. Prove that $Spec(A) \subset \mathbb{R}$.

7. Let $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$. Set $I = \{i | |a_{ii} > R'_i(A)\}$ and assume $|I| = k$. Prove that $rank(A) \geq k$.

8. Assume the $n \times n$ complex matrix A is strictly diagonally dominant. Prove for at least one j that $|a_{jj}| > C'_j(A)$.

9. Assume A is a real strictly diagonally dominant $n \times n$ matrix with diagonal entries $a_{11}, \dots, a_{nn}$. Prove that

$$det(A) \prod_{i=1}^{n} a_{ii} > 0.$$

An excellent source for this material is ([21]).

12.5 Functions of Matrices

In this section we consider how we might give meaning to $p(A)$ where $p(z)$ is a power series in a complex variable z and A is a square complex matrix. This has applications to the solution of homogeneous linear systems of differential equations as well as to the study of Lie groups. We will also consider possible generalizations over arbitrary fields.

What You Need to Know

Understanding the new material in this section depends on a mastery of the following concepts: normed linear space, matrix norm, Cauchy sequence of matrices, and evaluation of a polynomial at an operator or matrix.

Let A be a $n \times n$ matrix with entries in a field $\mathbb{F}$. Recall if $f(x) = a_d x^d + \cdots + a_1 x + a_0$ is a polynomial with coefficient in $\mathbb{F}$ then we defined $f(A)$ to be $a_d A^d + \cdots + a_1 A + a_0 I_n$. It is our intention to extend this definition to a power series in a single variable. We begin, however, with some lemmas concerning polynomial functions of matrices.

Lemma 12.9 *Let $Q \in GL_n(\mathbb{F})$. Then the following hold:*

i. If $B \in M_{nn}(\mathbb{F})$ and k is a natural number then $(Q^{-1}BQ)^k = Q^{-1}B^kQ$.

ii. If $B_1, B_2 \in M_{nn}(\mathbb{F})$, then $Q^{-1}(B_1 + B_2)Q = Q^{-1}B_1Q + Q^{-1}B_2Q$.

Proof *We leave these as exercises.*

As a consequence of Lemma (12.9) we have the following:

Corollary 12.8 *Let $Q \in GL_n(\mathbb{F}), B \in M_{nn}(\mathbb{F})$ and $f(x) \in \mathbb{F}[x]$. Then $f(Q^{-1}BQ) = Q^{-1}f(B)Q$.*

Now suppose $A \in M_{nn}(\mathbb{F})$ is diagonalizable and $A = Q^{-1}BQ$ where $B = diag\{\lambda_1, \ldots, \lambda_n\}$. Then $f(B) = diag\{f(\lambda_1), \ldots, f(\lambda_n)\}$, a diagonal matrix. Thus, $f(A) = Q^{-1}f(B)Q$ and so $f(A)$ is diagonalizable.

We will now restrict ourselves to matrices with entries in $\mathbb{C}$. In this case an arbitrary matrix A is similar to a matrix J in Jordan canonical form,

$$J = J_{n_1}(\lambda_1) \oplus \cdots \oplus J_{n_s}(\lambda_s) = \begin{pmatrix} J_{n_1}(\lambda_1) & 0 & \ldots \\ & \ddots & \\ 0 & & J_{n_s}(\lambda_s) \end{pmatrix}.$$

Here $J_d(\lambda)$ is the $d \times d$ matrix with diagonal equal to λI_d, ones directly below the main diagonal and all other entries zero. Thus,

$$J_d(\lambda) = \begin{pmatrix} \lambda & 0 & \dots & 0 \\ 1 & \lambda & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & \lambda \end{pmatrix}.$$

If $A = Q^{-1}JQ$ and $f(x) \in \mathbb{F}[x]$ then $f(A) =$

$$f(J_{n_1}(\lambda_1)) \oplus \dots \oplus f(J_{n_s}(\lambda_s)) = \begin{pmatrix} f(J_{n_1}(\lambda_1)) & & \\ & \ddots & \\ & & f(J_{n_s}(\lambda_s)) \end{pmatrix}.$$

We now compute $f(J_d(\lambda))$ for an arbitrary polynomial $f(x) \in \mathbb{C}[x]$. Write $J_d(\lambda)$ as the sum $\lambda I_d + N_d$ where $N_d = J_d(0)$. Note that N is a nilpotent matrix and, in fact, $N^d = \mathbf{0}_{d\times d}$. For convenience we drop the subscript d on I_d and N_d. Since I and N commute, the binomial expansion applies to powers of $J_d(\lambda)$. Thus for a natural number k we have

$$J_s(\lambda)^k = (\lambda I + N)^k = \sum_{i=0}^{min\{k,d-1\}} \binom{k}{i} \lambda^{k-i} N^i.$$

Assume now that $f(x) = a_m x^m + \dots + a_1 x + a_0$. Then

$$f(J_s(\lambda)) = \sum_{j=0}^{m} a_j J_s(\lambda)^j = \sum_{j=0}^{m} a_j \sum_{i=0}^{j} \binom{j}{i} \lambda^{j-1} N^i$$

$$= \sum_{i=0}^{m} \left\{ \sum_{j=i}^{m} \binom{j}{i} a_j \lambda^{j-i} \right\} N^i = \sum_{i=0}^{m} \frac{1}{i!} \left\{ \sum_{j=i}^{m} \frac{j!}{(j-i)!} a_j \lambda^{j-i} \right\} N^i.$$

Note that the expression $\sum_{j=i}^{m} \frac{j!}{(j-i)!} a_j \lambda^{j-i}$ is just the i^{th} derivative of $f(x)$, which we denote by $f^{(i)}(x)$. Thus,

$$\begin{aligned} f(J_d(\lambda)) &= \sum_{i=0}^{m} \frac{1}{i!} f^{(i)}(\lambda) N^i \\ &= \sum_{i=0}^{min\{m,d-1\}} \frac{1}{i!} f^{(i)}(\lambda) N^i. \end{aligned}$$

For example, if we apply a polynomial $f(x)$ to a 4×4 Jordan block centered at λ then we get

$$f(J_4(\lambda)) = \begin{pmatrix} f(\lambda) & 0 & 0 & 0 \\ f'(\lambda) & f(\lambda) & 0 & 0 \\ \frac{1}{2}f''(\lambda) & f'(\lambda) & f(\lambda) & 0 \\ \frac{1}{6}f^{(3)}(\lambda) & \frac{1}{2}f''(\lambda) & f'(\lambda) & f(\lambda) \end{pmatrix}.$$

We now turn our attention to power series. Suppose then that $p(z) = \sum_{k=1}^{\infty} a_k z^k$ is a power series in the complex variable z with radius of convergence R. Let A be a complex matrix with $\| A \| < R$ for some matrix norm $\| \cdot \|$ on $M_{nn}(\mathbb{C})$. Denote by $S_n(z)$ the n^{th} partial sum of $p(z)$,

$$S_n(z) = \sum_{k=0}^{n} a_k z^k.$$

Since $S_n(z)$ is a polynomial the meaning of $S_n(A)$ is unambiguous. Suppose now that $m \leq n$ are natural numbers. Then

$$S_n(A) - S_m(A) = \sum_{k=m+1}^{n} a_k A^k = a_n A^n + \cdots + a_{m+1} A^{m+1}.$$

By the triangle inequality we have

$$\| S_n(A) - S_m(A) \| \leq \sum_{k=m+1}^{n} \| a_k A^k \| = \sum_{k=m+1}^{n} |a_k| \, \| A^k \| .$$

Since the norm is a matrix norm, we have

$$\sum_{k=m+1}^{n} |a_k| \, \| A^k \| \leq \sum_{k=m+1}^{n} |a_k| \, \| A \|^k .$$

Since we are assuming that $\| A \| < R$, it follows that the power series

$$\sum_{k=0}^{\infty} |a_k| \, \| A \|^k$$

converges so that the sequence $\{S_n(A)\}_{n=0}^{\infty}$ is a Cauchy sequence of complex matrices. Since $M_{nn}(\mathbb{C})$ is complete, it follows that this sequence has a unique limit which we denote by $p(A)$.

This can be applied to any function defined as a power series with a positive radius of convergence, in particular to such functions as $sin\ z, cos\ z$, and $exp(z)$. The latter is especially important because of its applications to Lie groups as well as the solution of homogeneous linear systems of differential equations. Thus, for an $n \times n$ complex matrix A we will denote by $exp(A)$ the matrix

$$\sum_{k=0}^{\infty} \frac{1}{k!} A^k$$

and develop its properties.

Theorem 12.34 *Let A and B be commuting $n \times n$ complex matrices. Then $exp(A+B) = (exp(A))(exp(B))$.*

Proof *Since the series that defines the exponential of a matrix is uniformly convergent in any closed and bounded set, we can compute the product $(exp(A))(exp(B))$ by multiplying the terms of $exp(A)$ by the terms of $exp(B)$. Thus,*

$$exp(A)exp(B) = \sum_{i,j=0}^{\infty} \frac{1}{i!j!} A^j B^k.$$

Set $C_k = \sum_{i+j=k} \frac{k!}{i!j!} A^i B^j$.

Since $AB = BA$, the binomial theorem applies to $(A+B)^k$ from which we conclude that $C_k = (A+B)^k$. We then have

$$exp(A)exp(B) = \sum_{k=0}^{\infty} \frac{1}{k!} C_k = \sum_{k=0}^{\infty} \frac{1}{k!} (A+B)^k = exp(A+B).$$

Since A and $-A$ commute for any square complex matrix A and $exp(\mathbf{0}_{nn}) = I_n$, we have the following:

Corollary 12.9 *Let A be an $n \times n$ complex matrix. Then $exp(A)$ is invertible and $exp(A)^{-1} = exp(-A)$.*

Below we make explicit how the exponential of two similar matrices are related but first we need to prove a lemma.

Lemma 12.10 *Let $\| \cdot \|$ be a matrix norm on $M_{nn}(\mathbb{C})$. Assume $\{D_n\}_{n=1}^{\infty}$ is a sequence of matrices which converges to $D, Q \in GL_n(\mathbb{C}), C_n = Q^{-1} D_n Q, C = Q^{-1} D Q$. Then $\{C_n\}_{n=1}^{\infty}$ converges to C.*

Proof *Set $\delta = max\{\parallel Q^{-1} \parallel \cdot \parallel Q \parallel, 1\}$ and let $\epsilon > 0$. We need to show there is a natural number $N(\epsilon)$ such that if $n \geq N(\epsilon)$ then $\parallel C_n - C \parallel < \epsilon$. Now since $\{D_n\}_{n=1}^{\infty}$ converges to D, given $\gamma > 0$ there is an $N(\gamma)$ such that if $n \geq N(\epsilon)$ then $\parallel D_n - D \parallel < \gamma$. Set $\gamma = \frac{\epsilon}{\delta}$ and $N = N(\gamma)$. Suppose $n \geq N$. We then have*

$$\begin{aligned}
\parallel C_n - C \parallel &= \parallel Q^{-1}D_nQ - Q^{-1}DQ \parallel \\
&= \parallel Q^{-1}(D_n - D)Q \parallel \\
&\leq \parallel Q^{-1} \parallel \cdot \parallel D_n - D \parallel \cdot \parallel Q \parallel \\
&= \parallel B_n - B \parallel \cdot (\parallel Q^{-1} \parallel \cdot \parallel Q \parallel) \\
&< \gamma \, (\parallel Q^{-1} \parallel \cdot \parallel Q \parallel) \\
&= \frac{\epsilon}{\delta} \, (\parallel Q^{-1} \parallel \cdot \parallel Q \parallel) \\
&\leq \epsilon.
\end{aligned}$$

We can now prove:

Theorem 12.35 *Assume $A, B \in M_{nn}(\mathbb{C})$ and $A = Q^{-1}BQ$ where $Q \in GL_n(\mathbb{C})$. Then $exp(A) = Q^{-1}exp(B)Q$.*

Proof *Set $D = exp(B), D_n = \sum_{i=0}^{n} \frac{1}{i!}B^i, C = exp(A), C_n = \sum_{i=0}^{n} \frac{1}{i!}A^i$. Here we are using the convention for any $n \times n$ matrix X that $X^0 = I_n$. Then $\{D_n\}_{n=1}^{\infty}$ converges to $D = exp(B)$ and $\{C_n\}_{n=1}^{\infty}$ converges to $exp(A)$. By Corollary (12.8) $C_n = Q^{-1}D_nQ$. By Lemma (12.10) it follows that $exp(A) = C = Q^{-1}DQ = Q^{-1}exp(B)Q$.*

Suppose A is diagonalizable. If the eigenvalues of A are $\lambda_1, \dots, \lambda_n$, then there is an invertible matrix Q such that

$$A = Q^{-1} \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix} Q.$$

Then $exp(A) =$

$$Q^{-1} \begin{pmatrix} e^{\lambda_1} & 0 & \dots & 0 \\ 0 & e^{\lambda_2} & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & e^{\lambda_n} \end{pmatrix} Q.$$

More generally, we can express A as $Q^{-1}BQ$ where B is a Jordan canonical form of A. This can be used to prove the following:

Theorem 12.36 *Let $A \in M_{nn}(\mathbb{C})$. Assume $\chi_A(x) = (x-\lambda_1)\dots(x-\lambda_n)$. Then $\chi_{exp(A)}(x) = (x-e^{\lambda_1})\dots(x-e^{\lambda_n})$.*

Proof *We leave this as an exercise.*

A consequence of Theorem (12.36) is:

Corollary 12.10 *Let $A \in M_{nn}(\mathbb{C})$. Then $det(exp(A)) = exp(Trace(A))$.*

Recall that an $n \times n$ matrix A is nilpotent when $\mu_A(x) = x^k$ for some $k \leq n$. In this case, computing the exponential does not involve limits and is a finite sum:

$$\exp(A) = \sum_{i=1}^{k-1} \frac{1}{i!} A^i.$$

This even applies to matrices with entries in a field with prime characteristic p when the minimal polynomial is x^k for some $k \leq p$. In particular, if $A^2 = \mathbf{0}_{nn}$. Such elements exist in abundance: Any matrix A such that $col(A) \subset null(A)$ satisfies $A^2 = \mathbf{0}_{n\times n}$ and consequently, by the rank-nullity theorem, the rank of such a matrix is at most $\lfloor \frac{n}{2} \rfloor$. For purposes of illustration, and because of the important role they play, we will look at the exponential of those matrices A of rank one such that $A^2 = \mathbf{0}_{n\times n}$. We characterize such matrices in the next result. Before doing so recall that for $1 \leq i, j \leq n$, E_{ij} is the matrix with (i, j)-entry one and all other entries are zero.

Remark 12.10 *Assume $i \neq j$ and $k \neq l$. Then E_{ij} and E_{kl} are similar by a permutation matrix.*

Theorem 12.37 *Let $A \in M_{n\times n}(\mathbb{F})$ have rank one and assume $A^2 = \mathbf{0}_{n\times n}$. Then there is a $Q \in GL_n(\mathbb{F})$ such that $A = Q^{-1}E_{21}Q$.*

Proof *Define $T_A : \mathbb{F}^n \to \mathbb{F}^n$ by $T_A(\boldsymbol{v}) = A\boldsymbol{v}$. Let $\boldsymbol{y} \neq \mathbf{0}_n$ be an element of $Range(T_A) = col(A)$ and let $\boldsymbol{x} \in \mathbb{F}^n$ such that $A\boldsymbol{x} = \boldsymbol{y}$. Since $col(A) \subset null(A)$, in particular, $\boldsymbol{y} \in null(A)$. Extend $\boldsymbol{y}$ to a basis $(\boldsymbol{y} = \boldsymbol{y}_1, \dots, \boldsymbol{y}_{n-1})$ of $null(A)$. Since $\boldsymbol{x} \notin null(A), Span(\boldsymbol{x}) \cap Span(\boldsymbol{y}_1, \dots, \boldsymbol{y}_{n-1}) = \{\mathbf{0}_n\}$ and consequently, $\mathcal{B} = (\boldsymbol{x}, \boldsymbol{y}_1, \dots, \boldsymbol{y}_{n-1})$ is linearly independent and therefore a basis of $\mathbb{F}^n$. Now $\mathcal{M}_{T_A}(\mathcal{B}, \mathcal{B}) = E_{21}$. On the other hand, if $Q = \mathcal{M}_I(\mathcal{S}, \mathcal{B})$ where $\mathcal{S}$ is the standard basis of $\mathbb{F}^n$ then $A = \mathcal{M}_{T_A}(\mathcal{S}, \mathcal{S}) = Q^{-1}\mathcal{M}_{T_A}(\mathcal{B}, \mathcal{B})Q = Q^{-1}E_{21}Q$.*

Now consider $exp(tE_{ij})$ where $t \in \mathbb{F}$. This is equal to $I_n + tE_{21}$, a matrix with ones on the diagonal and one nonzero entry off the diagonal equal to t. This is a transvection. Suppose, more generally, that $A = Q^{-1}E_{21}Q$ where $Q \in GL_n(\mathbb{F})$. Then $exp(tA) = exp(Q^{-1}(tE_{21})Q) = Q^{-1}exp(tE_{21})Q$ which is a transvection. Consequently, if $rank(A) = 1, A^2 = \mathbf{0}_{n\times n}$ then $exp(tA)$ is a transvection. In this way we obtain all the transvections. We therefore have the following result.

Theorem 12.38 *Let G denote the subgroup of $GL_n(\mathbb{F})$ generated by* $\exp(tA)$ *where $t \in \mathbb{F}$, $rank(A) = 1$, and $A^2 = \mathbf{0}_{n\times n}$. Then $G = SL_n(\mathbb{F})$.*

For the reader interested in additional results on this topic see ([11]) and ([19]).

Exercises

1. Prove Lemma (12.9).

2. Prove Corollary (12.8).

3. Prove Theorem (12.36).

4. Prove Corollary (12.10).

For a complex matrix $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$ let $\overline{A}$ be whose (i,j)-entry is $\overline{a_{ij}}$ and let $A^* = \overline{A}^{tr}$.

5. Prove for a complex matrix A that $exp(A)^* = exp(A^*)$.

6. Assume the complex matrix A is Hermitian. Prove $exp(A)$ is Hermitian.

7. Assume the complex matrix A is normal ($AA^* = A^*A$). Prove $exp(A)$ is normal.

This page intentionally left blank

13

Applications of Linear Algebra

CONTENTS

This concluding chapter deals with several common and important applications of linear algebra both to other areas of mathematics as well as to science and technology. In the first section we briefly develop the theory and method of linear least squares which can be used to estimate the parameters of a model to a set of observed data points. In the second section we introduce coding theory which is ubiquitous and embedded in all the digital devices we now take for granted. In our final section we discuss how linear algebra is used to define a page rank algorithm that might be applied in a web search engine.

13.1 Least Squares

In this section we define what is meant by the general linear least squares problem which involves an overdetermined linear system. We derive the normal equations and demonstrate how to use them to find a solution. We then illustrate the method with several examples.

What You Need to Know

Most of the following concepts, which you will need to have mastered in order to make sense of the new material in this section, are introduced in a course in elementary linear algebra: a linear system of equations, inconsistent system of linear equations, null space of a matrix, invertible matrix, transpose of a matrix, column space of a matrix, rank of a matrix. triangular matrix, QR factorization of a matrix, linearly independent sequence of vectors, linearly dependent sequence of vectors, inner product space, orthogonal vectors in an inner product space, orthogonal complement to a subspace of a inner product space, norm of a vector induced by an inner product, orthonormal sequence of vectors, and an orthonormal basis of a subspace of an inner product space.

The General Least Squares Problem

It is trivial to write down a linear system of equations, equivalently, a matrix equation $A\boldsymbol{x} = \boldsymbol{b}$, which is inconsistent. Though inconsistent, one may seek a "best" approximation to a solution. As we will see, this arises in the practice of experimental science when attempting to fit a model to collected data. Finding the best approximate solution to an inconsistent linear system is the basis of a "least squares solution."

Definition 13.1 *Let A be an $m \times n$ complex matrix and $\boldsymbol{b} \in \mathbb{C}^m$ such that $\boldsymbol{b} \notin col(A)$. A vector $\boldsymbol{x} \in \mathbb{C}^n$ is said to be a* **least squares solution** *if $\parallel A\boldsymbol{x} - \boldsymbol{b} \parallel \leq \parallel A\boldsymbol{y} - \boldsymbol{b} \parallel$ for all $\boldsymbol{y} \in \mathbb{C}^n$.*

For any vector $\boldsymbol{x} \in \mathbb{C}^n$, the vector $A\boldsymbol{x}$ is in the column space of A. The first step in the solution to this problem is to identify the vector $A\boldsymbol{x}$. Immediately relevant to this is Theorem (5.16), which we proved in Section (5.4). Here is the statement:

Theorem (5.16) Let W be a subspace of $\mathbb{C}^n$ and $\boldsymbol{u}$ a complex $n-$vector. Then for any vector $\boldsymbol{w} \in W, \boldsymbol{w} \neq Proj_W(\boldsymbol{u})$, $\parallel \boldsymbol{u} - Proj_W(\boldsymbol{u}) \parallel < \parallel \boldsymbol{u} - \boldsymbol{w} \parallel$.

Finding the General Least Squares Solutions

Given an $m \times n$ complex matrix A and $\boldsymbol{b} \in \mathbb{C}^m$, set $W = col(A)$ and $\boldsymbol{b}' = Proj_W(\boldsymbol{b})$. Assume that $\boldsymbol{x}$ is a vector such that $A\boldsymbol{x} = \boldsymbol{b}'$.

Recall that the vector $\boldsymbol{b} - \boldsymbol{b}' = \boldsymbol{b} - A\boldsymbol{x}$ is in $W^{\perp}$, the orthogonal complement to $W = col(A)$. This means that the vector $\boldsymbol{b} - \boldsymbol{b}' = \boldsymbol{b} - A\boldsymbol{x}$ is orthogonal to every column of the matrix A and therefore is in the null space of the adjoint of $A, A^* = \overline{A^{tr}}$. This means that

$$A^*(\boldsymbol{b} - \boldsymbol{b}') = A^*(\boldsymbol{b} - A\boldsymbol{x}) = \boldsymbol{0}_n. \tag{13.1}$$

An immediate consequence of (13.1) is that a vector $\boldsymbol{x}$ for which $A\boldsymbol{x} = \boldsymbol{b}' = Proj_W(\boldsymbol{b})$ satisfies the equation

$$A^*A\boldsymbol{x} = A^*\boldsymbol{b}. \tag{13.2}$$

The equations of the linear system equivalent to the matrix equation shown in (13.2) are referred to as the ***normal equations*** of $A\boldsymbol{x} = \boldsymbol{b}$.

We have thus shown that every least squares solution satisfies the normal equations. The converse is also true:

Theorem 13.1 *Assume that $\boldsymbol{x}$ satisfies the $A^*A\boldsymbol{x} = A^*\boldsymbol{b}$. Then $\boldsymbol{x}$ is a least squares solution to $A\boldsymbol{x} = \boldsymbol{b}$.*

Proof *Assume that $\boldsymbol{x}$ satisfies $A^*A\boldsymbol{x} = A^*\boldsymbol{b}$. Then*

$$A^*A\boldsymbol{x} - A^*\boldsymbol{b} = A^*(A\boldsymbol{x} - \boldsymbol{b}) = \boldsymbol{0}_n. \tag{13.3}$$

A consequence of (13.3) is that the vector $A\boldsymbol{x} - \boldsymbol{b}$ is in the null space of A^* and therefore orthogonal to every row of A^{tr}, equivalently, every column of A. Since $A\boldsymbol{x} - \boldsymbol{b}$ is orthogonal to every column of A, it follows that $A\boldsymbol{x} - \boldsymbol{b}$ is in the orthogonal complement of the column space of A.

On the other hand, assume $A\boldsymbol{x}$ is in the column space of A and $\boldsymbol{b} = A\boldsymbol{x} + (\boldsymbol{b} - A\boldsymbol{x})$, the sum of a vector in $col(A)$ and a vector in $col(A)^\perp$. From Theorem (5.12) there are unique vectors $\boldsymbol{w} \in col(A)$ and $\boldsymbol{z} \in col(A)^\perp$ such that $\boldsymbol{b} = \boldsymbol{w} + \boldsymbol{z}$. Moreover, the vector $\boldsymbol{w} = Proj_{col(A)}(\boldsymbol{b})$. Thus, $A\boldsymbol{x} = Proj_{col(A)}(\boldsymbol{b})$ and is therefore a least squares solution to $A\boldsymbol{x} = \boldsymbol{b}$.

We now determine when a unique solution exists. Of course, this occurs precisely when the matrix A^*A is invertible.

Theorem 13.2 *Let A be an $m \times n$ complex matrix and $\boldsymbol{b} \in \mathbb{C}^m, \boldsymbol{b} \notin col(A)$ so that the matrix equation $A\boldsymbol{x} = \boldsymbol{b}$ has no solutions. Then a least squares solution for the system $A\boldsymbol{x} = \boldsymbol{b}$ is unique if and only if the sequence of columns of the matrix A is linearly independent. In this case the unique solution is given by $\boldsymbol{x} = (A^*A)^{-1}A^*\boldsymbol{b}$.*

Proof *First assume that there is a unique solution. Then A^*A is an invertible matrix, which implies that the rank of A^*A is n. However, $rank(A^*) = rank(A)$ and $rank(A^*A) \leq min\{rank(A), rank(A^*)\}$. It must therefore be the case that $rank(A) = n$ and since A has n columns, the sequence of columns of A must be linearly independent.*

Conversely, assume that the sequence of columns of A is linearly independent. This implies that the null space of A consists of only the zero vector, $null(A) = \{\mathbf{0}_n\}$. We will show that $null(A^*A) = \{\mathbf{0}_n\}$ from which it will follow that A^*A is an invertible matrix.

Assume $\boldsymbol{x} \in null(A^*A)$. Then $A^*A\boldsymbol{x} = \mathbf{0}_n$. Then $0 = \overline{\boldsymbol{x}^{tr}}(A^*A\boldsymbol{x}) = \overline{\boldsymbol{x}^{tr}A^{tr}}(A\boldsymbol{x}) = \langle A\boldsymbol{x}, A\boldsymbol{x}\rangle$, so that by positive definiteness we have $A\boldsymbol{x} = \mathbf{0}_m$. Since the sequence of columns of A are linearly independent, $null(A) = \{\mathbf{0}_n\}$ so that $\boldsymbol{x} = \mathbf{0}_n$.

Remark 13.1 *Note that when A is a complex $m \times n$ matrix of rank n and $A\boldsymbol{x} = \boldsymbol{b}$ is inconsistent, the unique least square solution is equal to $A^\dagger\boldsymbol{b}$, where $A^\dagger$ is the pseduoinverse of A. This will make an appearance again when we consider the situation where $rank(A) < n$ and we characterize all the least square solutions.*

In the next definition we introduce a weak notion of pseudoinverse of a matrix.

Definition 13.2 *Let A be an $m \times n$ complex matrix. An $n \times m$ matrix X is a* $\{1,3\}$**-inverse** *of A if the following hold:*

(PI1) $AXA = A$; and

(PI3) $(AX)^* = AX$.

In the next lemma we establish some properties of a $\{1,3\}$-inverse of a matrix.

Lemma 13.1 *Let A be an $m \times n$ complex matrix and X a $\{1,3\}$-inverse of A. Then the following hold:*

i) $AX = AA^\dagger$.

ii) $I_m - AX$ is the projection map onto $col(A)^\perp$.

Proof *i) Since $AA^\dagger A = A$ we have*

$$\begin{aligned} AX &= AA^\dagger AX \\ &= (AA^\dagger)^*(AX)^* \\ &= (A^\dagger)^*(A^*X^*A^*) \\ &= (A^\dagger)^*(AXA)^* \\ &= (A^\dagger)^*A^* \\ &= (AA^\dagger)^* = AA^\dagger. \end{aligned}$$

ii) This follows from Theorem (12.12).

We leave the following corollary as an exercise.

Corollary 13.1 *Let A be an $m \times n$ complex matrix. Then X is a $\{1,3\}$-inverse of A if and only if $AX = AA^\dagger$.*

Assume A is a complex $m \times n$ matrix, $\boldsymbol{b} \in \mathbb{C}^m$, and $\boldsymbol{b} \notin col(A)$. The next result obtains least square solutions to an inconsistent system $A\boldsymbol{x} = \boldsymbol{b}$ in terms of a $\{1,3\}$-inverse of A.

Theorem 13.3 *Assume X is a $\{1,3\}$-inverse of A. Then $X\boldsymbol{b}$ is a least square solution to $A\boldsymbol{x} = \boldsymbol{b}$.*

Proof *Set $\boldsymbol{z} = X\boldsymbol{b}$. We need to show that for an arbitrary $\boldsymbol{y} \in \mathbb{C}^n$ that $\parallel A\boldsymbol{y} - \boldsymbol{b} \parallel^2 \geq \parallel A\boldsymbol{z} - \boldsymbol{b} \parallel^2$. Now*

$$\begin{aligned} \parallel A\boldsymbol{y} - \boldsymbol{b} \parallel^2 &= \parallel (A\boldsymbol{y} - A\boldsymbol{z}) + (A\boldsymbol{z} - \boldsymbol{b}) \parallel^2 \\ &= \parallel (A\boldsymbol{y} - AX\boldsymbol{b}) + (AX\boldsymbol{b} - \boldsymbol{b}) \parallel^2 \\ &= \parallel (A\boldsymbol{y} - AA^\dagger\boldsymbol{b}) + (AA^\dagger\boldsymbol{b} - \boldsymbol{b}) \parallel^2 \\ &= \parallel A(\boldsymbol{y} - A^\dagger\boldsymbol{b}) + (AA^\dagger\boldsymbol{b} - \boldsymbol{b}) \parallel^2 . \end{aligned}$$

By part ii) of Theorem (13.1), $I_m - AA^\dagger$ is the projection onto $col(A)^\perp$ so, in particular, $AA^\dagger\boldsymbol{b} - \boldsymbol{b} = (AA^\dagger - I_m)\boldsymbol{b}$ is in $col(A)^\perp$. On the other hand, $A(\boldsymbol{y} - A^\dagger\boldsymbol{b}) \in col(A)$ so we can conclude that

$$\langle A(\boldsymbol{y} - A^\dagger\boldsymbol{b}), (AA^\dagger - I_m)\boldsymbol{b}\rangle = 0.$$

Consequently, by the Pythagorean theorem, Theorem (5.3),

$$\begin{aligned} \| A(\boldsymbol{y} - A^\dagger \boldsymbol{b}) + (AA^\dagger \boldsymbol{b} - \boldsymbol{b}) \|^2 &= \| A(\boldsymbol{y} - A^\dagger \boldsymbol{b}) \|^2 + \| AA^\dagger \boldsymbol{b} - \boldsymbol{b} \|^2 \\ &\geq \| AA^\dagger \boldsymbol{b} - \boldsymbol{b} \|^2 \\ &= \| AX\boldsymbol{b} - \boldsymbol{b} \|^2 . \end{aligned}$$

Note that we get equality if and only if $\| A(\boldsymbol{y} - A^\dagger \boldsymbol{b}) \|^2 = 0$, *if and only if* $\boldsymbol{y} - A^\dagger \boldsymbol{b}$ *is in the null space of* A.

The next two results characterize the least squares solution to $A\boldsymbol{x} = \boldsymbol{b}$ in terms of a given $\{1,3\}$-inverse to A.

Theorem 13.4 *Let* A *be an* $m \times n$ *matrix,* $\boldsymbol{b} \in \mathbb{C}^n, \boldsymbol{b} \notin col(A)$. *Assume* X *is a* $\{1,3\}$*-inverse to* A. *Set* $\boldsymbol{z} = X\boldsymbol{b}$. *Then* $\boldsymbol{y}$ *is a least square solution to* $A\boldsymbol{x} = \boldsymbol{b}$ *if and only if* $\| A\boldsymbol{y} - \boldsymbol{b} \| = \| A\boldsymbol{z} - \boldsymbol{b} \|$.

Proof *We leave this as an exercise.*

Theorem 13.5 *Let* A *be an* $m \times n$ *matrix,* $\boldsymbol{b} \in \mathbb{C}^n$, *and* $\boldsymbol{b} \notin col(A)$. *Assume* X *is a* $\{1,3\}$*-inverse to* A *and* $\boldsymbol{y} \in \mathbb{C}^n$. *Then* $\boldsymbol{y}$ *is a least squares solution to* $A\boldsymbol{x} = \boldsymbol{b}$ *if and only if* $A\boldsymbol{y} = AX\boldsymbol{b} = (AA^\dagger)\boldsymbol{b}$.

Proof *Set* $\boldsymbol{z} = AX\boldsymbol{b} = (AA^\dagger)\boldsymbol{b}$. *We first show that the matrix equation* $A\boldsymbol{v} = \boldsymbol{z}$ *has a solution. Since* $AX = AA^\dagger$ *is the orthogonal projection onto* $col(A)$, *it follows that* $(AX)^2 = AX$. *Therefore* $(AX)\boldsymbol{z} = (AX)(AX\boldsymbol{b}) = (AX)^2\boldsymbol{b} = AX\boldsymbol{b} = \boldsymbol{z}$. *Thus,* $A[XAX\boldsymbol{b}] = \boldsymbol{z}$ *as required.*

Assume now that $\boldsymbol{y}$ *is a least squares solution to* $A\boldsymbol{x} = \boldsymbol{b}$. *Then* $\| A\boldsymbol{y} - \boldsymbol{b} \| = \| AX\boldsymbol{b} - \boldsymbol{b} \|$ *by Theorem (13.4). However,*

$$\begin{aligned} \| A\boldsymbol{y} - \boldsymbol{b} \|^2 &= \| (A\boldsymbol{y} - AA^\dagger \boldsymbol{b}) + (AA^\dagger \boldsymbol{b} - \boldsymbol{b} \|^2 \\ &= \| A\boldsymbol{y} - AA^\dagger \boldsymbol{b} \|^2 + \| AA^\dagger \boldsymbol{b} - \boldsymbol{b} \|^2 . \end{aligned}$$

It follows that $\| A\boldsymbol{y} - AX\boldsymbol{b} \|^2 = 0$, *so by positive definiteness,* $A\boldsymbol{y} = AX\boldsymbol{b}$.

Conversely, assume $A\boldsymbol{y} = AX\boldsymbol{b}$. *Then* $A\boldsymbol{y} - AX\boldsymbol{b} = \boldsymbol{0}_m$, *from which we conclude that* $\| A\boldsymbol{y} - \boldsymbol{b} \|^2 = \| AX\boldsymbol{b} - \boldsymbol{b} \|$. *By Theorem (13.4),* $\boldsymbol{y}$ *is a least squares solution to* $A\boldsymbol{x} = \boldsymbol{b}$.

Finally, we can describe all least square solutions to $A\boldsymbol{x} = \boldsymbol{b}$.

Theorem 13.6 *Assume X is a $\{1,3\}$-inverse of A. Set $\boldsymbol{v} = X\boldsymbol{b}$. Then the set of least square solutions to $A\boldsymbol{x} = \boldsymbol{b}$ is $\boldsymbol{v} + col(I_n - XA)$.*

Proof *Let $\boldsymbol{z} \in \mathbb{C}^n$ and set $\boldsymbol{u} = (I_n - XA)\boldsymbol{z}$ and $\boldsymbol{y} = \boldsymbol{v} + \boldsymbol{u}$. Then*

$$\begin{aligned} A\boldsymbol{y} &= A(\boldsymbol{v} + \boldsymbol{u}) \\ &= A\boldsymbol{v} + A\boldsymbol{u} \\ &= AX\boldsymbol{b} + A(I_n - XA)\boldsymbol{z} \\ &= AX\boldsymbol{b} + (A - AXA)\boldsymbol{z} \\ &= AX\boldsymbol{b}, \end{aligned}$$

since X is $\{1,3\}$-inverse of A, whence $AXA = A$. By Theorem (13.5) it follows that $\boldsymbol{y}$ is a least squares solution to $A\boldsymbol{x} = \boldsymbol{b}$.

Conversely, assume $\boldsymbol{y}$ is a least squares solution to $A\boldsymbol{x} = \boldsymbol{b}$. Set $\boldsymbol{u} = \boldsymbol{y} - X\boldsymbol{b}$. Then $A\boldsymbol{u} = A(\boldsymbol{y} - X\boldsymbol{b}) = A\boldsymbol{y} - AX\boldsymbol{b} = \boldsymbol{0}_m$ by Theorem (13.5). Now $(I - XA)\boldsymbol{u} = \boldsymbol{u} - XA\boldsymbol{u} = \boldsymbol{u} - \boldsymbol{0}_m = \boldsymbol{u}$ so that $\boldsymbol{u} \in col(I_n - XA)$ and we are done.

In our final result, before we turn to some examples, we consider the situation where $rank(A) < n$ and determine among all least squares solutions to $A\boldsymbol{x} = \boldsymbol{b}$ one of minimal norm. As we will see the pseudoinverse of A makes an appearance.

Theorem 13.7 *Set $\boldsymbol{z} = A^\dagger \boldsymbol{b}$ and assume $\boldsymbol{y}$ is a least squares solution to $A\boldsymbol{x} = \boldsymbol{b}$. Then $\parallel \boldsymbol{z} \parallel \leq \parallel \boldsymbol{y} \parallel$.*

Proof *By Theorem (13.6) there exists $\boldsymbol{u} = col(I_n - A^\dagger A)$ so that $\boldsymbol{y} = \boldsymbol{z} + \boldsymbol{u}$. Note that $(I_n - A^\dagger A)^* = (I_n - A^\dagger A)$ and therefore*

$$(I_n - A^\dagger A)^* A^\dagger = (I_n - A^\dagger A)A^\dagger =$$

$$A^\dagger - A^\dagger A A^\dagger = A^\dagger - A^\dagger = \boldsymbol{0}_{n\times m}.$$

It follows that every vector in $col(I_n - A^\dagger A)$ is orthogonal to $A^\dagger \boldsymbol{b}$. Then by Theorem (5.3)

$$\parallel \boldsymbol{y} \parallel^2 = \parallel \boldsymbol{z} + \boldsymbol{u} \parallel^2 = \parallel \boldsymbol{z} \parallel^2 + \parallel \boldsymbol{u} \parallel^2 \geq \parallel \boldsymbol{z} \parallel^2 .$$

We now do several examples to illustrate how least squares are practically used. In all cases the matrix A will be real so that $A^* = A^{tr}$.

Example 13.1 *Find all the least square solutions for the inconsistent linear system* $A\boldsymbol{x} = \boldsymbol{b}$ *where*

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 2 \end{pmatrix}, \boldsymbol{b} = \begin{pmatrix} 14 \\ 22 \\ 6 \\ 7 \end{pmatrix}$$

$$A^{tr}A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 3 \\ 3 & 6 \end{pmatrix}$$

$$A^{tr}\boldsymbol{b} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} 14 \\ 22 \\ 6 \\ 7 \end{pmatrix} = \begin{pmatrix} 27 \\ 42 \end{pmatrix}.$$

The matrix $A^{tr}A$ *is invertible so there is a unique solution*

$$\frac{1}{9}\begin{pmatrix} 6 & -3 \\ -3 & 3 \end{pmatrix}\begin{pmatrix} 27 \\ 42 \end{pmatrix} = \begin{pmatrix} 4 \\ 5 \end{pmatrix}.$$

Using Least Squares to Fit a Function to Data

It is a common feature of nearly all scientific domains to collect data among variables and then to find a functional relationship amongst the variables that best fits the data. In the simplest case one uses a linear function. Geometrically, this amounts to finding the line which best fits the data points when graphed in a coordinate plane.

More specifically, suppose we want to fit the experimentally obtained n data points $(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)$ by a linear function $y = f(x) = a + bx$.

If the points were all collinear and on the graph of this linear function then all equations

$$\begin{aligned} y_1 &= a + bx_1 \\ y_2 &= a + bx_2 \\ &\vdots \\ y_n &= a + bx_n \end{aligned}$$

would be satisfied. This can be written as a matrix equation

$$\begin{pmatrix} 1 & x_1 \\ 1 & x_2 \\ \vdots & \vdots \\ 1 & x_n \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n . \end{pmatrix} \tag{13.4}$$

If we let $A = \begin{pmatrix} 1 & x_1 \\ 1 & x_2 \\ \vdots & \vdots \\ 1 & x_n \end{pmatrix}$, $\boldsymbol{y} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$ and $\boldsymbol{m} = \begin{pmatrix} a \\ b \end{pmatrix}$ then (13.4) can be written as

$$\boldsymbol{y} = A \begin{pmatrix} a \\ b \end{pmatrix}. \tag{13.5}$$

If the data points are not collinear then there will be no a and b satisfying these equations and the system represented by (13.5) is inconsistent. In this situation, approximating y_i by $y_i' = a + bx_i$ results in an error $e_i = y_i - y_i'$.

Now set $\boldsymbol{e} = \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} y_1 - y_1' \\ y_2 - y_2' \\ \vdots \\ y_n - y_n' \end{pmatrix}$. Now the equations become

$$\boldsymbol{y} = A \begin{pmatrix} a \\ b \end{pmatrix} + \boldsymbol{e}, \boldsymbol{y} - A \begin{pmatrix} a \\ b \end{pmatrix} = \boldsymbol{e}. \tag{13.6}$$

The least squares solution determines the a and b such that $\parallel \boldsymbol{e} \parallel$ is minimized and is given by

$$\begin{pmatrix} a \\ b \end{pmatrix} = (A^{tr}A)^{-1}(A^{tr}\boldsymbol{y}).$$

The line given by the least squares solution is called the ***line of best fit*** or the ***regression line*** of the data. The norm of the error vector $\boldsymbol{e}$ is the ***least squares error***.

Example 13.2 *A significant sample was taken of the heights of boys, ages 11–17. The average heights by age group are given in the following table:*

Age (years)	*Height (inches)*
11	*55.1*
12	*57.6*
13	*60.8*
14	*63.3*
15	*66.2*
16	*68.1*
17	*69.1*

We will find the regression line of this data.

Let $A = \begin{pmatrix} 1 & 11 \\ 1 & 12 \\ 1 & 13 \\ 1 & 14 \\ 1 & 15 \\ 1 & 16 \\ 1 & 17 \end{pmatrix}$ *and* $\boldsymbol{y} = \begin{pmatrix} 55.1 \\ 57.6 \\ 60.8 \\ 63.3 \\ 66.2 \\ 68.1 \\ 69.1 \end{pmatrix}$. *Then* $A^{tr}A = \begin{pmatrix} 7 & 98 \\ 98 & 1400 \end{pmatrix}$ *and*

$A^{tr}\boldsymbol{y} = \begin{pmatrix} 440.2 \\ 6231.2. \end{pmatrix}$

The reduced echelon form of $\begin{pmatrix} 7 & 98 & | & 440.2 \\ 98 & 1400 & | & 6231.2 \end{pmatrix}$ *is*

$\begin{pmatrix} 1 & 0 & | & 28.74 \\ 0 & 1 & | & 2.44. \end{pmatrix}$

Therefore the regression line has equation $y = 28.74 + 2.44x$. *The least square error is 1.6.*

Fitting Data to a Polynomial

Suppose you hypothesize that a set of data $(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)$ is best modeled by a k-degree polynomial $y = f(x) = a_0 + a_1x + \cdots + a_kx^k$. We know there is a unique polynomial of degree $n-1$ whose graph contains all the points so we may assume that $k < n-1$. If the data points were all on the graph of this polynomial then for each i the equation

$$y_i = f(x_i) = a_0 + a_1x_i + a_2x_i^2 + \cdots + a_kx_i^k \tag{13.7}$$

would be satisfied.

Set $A = \begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^k \\ 1 & x_2 & x_2^2 & \dots & x_2^k \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^k \end{pmatrix}, \boldsymbol{y} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}, \boldsymbol{m} = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_k \end{pmatrix}$

The equations (13.7) can be represented by the single matrix equation

$$\boldsymbol{y} = A\boldsymbol{m}. \tag{13.8}$$

If the points do not all lie on some polynomial of degree at most k then the system will have no solution. In this case, we find a best fit using the least squares method.

Note that the matrix obtained by taking the first $k+1$ rows of A,

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^k \\ 1 & x_2 & x_2^2 & \dots & x_2^k \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & x_{k+1} & x_{k+1}^2 & \dots & x_{k+1}^k \end{pmatrix},$$

is a Vandermonde matrix. This matrix has determinant $\prod_{i<j}(x_j - x_i) \neq 0$. Therefore, the rank of A is $k+1$ and the least squares solution is unique and equal to

$$(A^{tr}A)^{-1}(A^{tr}\boldsymbol{y}). \tag{13.9}$$

We illustrate with some examples.

Example 13.3 *Find the quadratic polynomial which is the best fit to the five points (1, -2), (2,0.2), (3,3.9), (4,10), (5, 17.9).*

Set $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \\ 1 & 4 & 16 \\ 1 & 5 & 25 \end{pmatrix}, \boldsymbol{y} = \begin{pmatrix} -2 \\ 0.2 \\ 3.9 \\ 10 \\ 17.9 \end{pmatrix}$

Then $f(x) = a_0 + a_1x + a_2x^2$ *where*

$$\begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} = (A^{tr}A)^{-1}(A^{tr}\boldsymbol{y}).$$

$A^{tr}A = \begin{pmatrix} 5 & 15 & 55 \\ 15 & 55 & 225 \\ 55 & 225 & 979 \end{pmatrix}, A^{tr}\boldsymbol{y} = \begin{pmatrix} 30 \\ 139.6 \\ 641.4 \end{pmatrix}.$

The reduced echelon form of the matrix $\begin{pmatrix} 5 & 15 & 55 & | & 30 \\ 15 & 55 & 225 & | & 139.6 \\ 55 & 225 & 979 & | & 641.4 \end{pmatrix}$ *is*

$$\begin{pmatrix} 1 & 0 & 0 & \mid & -1.98 \\ 0 & 1 & 0 & \mid & -0.95 \\ 0 & 0 & 1 & \mid & 0.99 \end{pmatrix}.$$

Therefore the quadratic polynomial which best fits these five points is

$$f(x) = -1.98 - 0.95x + 0.99x^2$$

Using this quadratic we compute the vector $\boldsymbol{y}' = \begin{pmatrix} f(1) \\ f(2) \\ f(3) \\ f(4) \\ f(5) \end{pmatrix} = \begin{pmatrix} -1.95 \\ 0.05 \\ 4.03 \\ 9.97 \\ 17.89 \end{pmatrix}$. *The error vector is* $\boldsymbol{e} = \boldsymbol{y} - \boldsymbol{y}' = \begin{pmatrix} -0.05 \\ 0.15 \\ -0.13 \\ 0.03 \\ 0.01 \end{pmatrix}$. *The least square error is* $\parallel \boldsymbol{e} \parallel = 0.04$.

Example 13.4 *Find the cubic polynomial which is the best fit to the five points* $(-2, -5), (-1, 1), (0, -1), (1, -1), (2, 6)$.

Set $A = \begin{pmatrix} 1 & -2 & 4 & -8 \\ 1 & -1 & 1 & -1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 \end{pmatrix}, \boldsymbol{y} = \begin{pmatrix} -5 \\ 1 \\ -1 \\ -1 \\ 6 \end{pmatrix}$.

If $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3$ *is the cubic polynomial of best fit then* $\boldsymbol{m} = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}$ *is the solution to* $(A^{tr}A)\boldsymbol{m} = (A^{tr}\boldsymbol{y})$.

Direct computation gives $A^{tr}A = \begin{pmatrix} 5 & 0 & 10 & 0 \\ 0 & 10 & 0 & 34 \\ 10 & 0 & 34 & 0 \\ 0 & 34 & 0 & 130 \end{pmatrix}, A^{tr}\boldsymbol{y} = \begin{pmatrix} 0 \\ 20 \\ 4 \\ 87 \end{pmatrix}$.

The reduced echelon form of $\begin{pmatrix} 5 & 0 & 10 & 0 & \mid & 0 \\ 0 & 10 & 0 & 34 & \mid & 20 \\ 10 & 0 & 34 & 0 & \mid & 4 \\ 0 & 34 & 0 & 130 & \mid & 87 \end{pmatrix}$ *is the matrix*

$$\begin{pmatrix} 1 & 0 & 0 & 0 & | & -0.57 \\ 0 & 1 & 0 & 0 & | & -2.25 \\ 0 & 0 & 1 & 0 & | & 0.29 \\ 0 & 0 & 0 & 1 & | & 1.25 \end{pmatrix}.$$

Therefore the cubic polynomial which is the best fit to this data is

$$g(x) = -0.57 - 2.25x + 0.29x^2 + 1.25x^2.$$

Using this cubic we compute the vector $\boldsymbol{y}' = \begin{pmatrix} g(-2) \\ g(-1) \\ g(0) \\ g(1) \\ g(2) \end{pmatrix} = \begin{pmatrix} -4.93 \\ 0.71 \\ -0.57 \\ -1.29 \\ 6.07 \end{pmatrix}$. *The error vector is* $\boldsymbol{e} = \boldsymbol{y} - \boldsymbol{y}' = \begin{pmatrix} -0.07 \\ 0.29 \\ -0.43 \\ 0.29 \\ -0.07 \end{pmatrix}$. *The least square error is* $\parallel \boldsymbol{e} \parallel = 0.60$.

Fitting Data to an Exponential Function

Sometimes the graph of some data or the context in which it is collected suggests that the most appropriate approximation for the data is by an exponential function; for example, growth of the national income or the amount of a radioactive material present at given time intervals.

Thus, given some points $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$ we wish to approximate this data by a function $y = Ce^{kt}$ for some constants C and k.

Note that for such a function, $ln\ y = ln\ C + kt$ is a linear function of t. We can therefore use the least squares method for finding $ln\ C$ and k from the data $(x_1, ln\ y_1), (x_2, ln\ y_2), \ldots, (x_n, ln\ y_n)$.

Example 13.5 *Find the exponential function* $y = Ce^{kt}$ *which best approximates the following 6 data points:*

$$(-2, .14), (-1, .32), (0, .55), (1, 1.24), (2, 2.44), (3, 4.75).$$

Taking the natural logs of the y-values we get the data points:

$$(-2, -1.97), (-1, -1.14), (0, -.60), (1, .22), (2, .89), (3, 1.56).$$

We now need to find the least squares solution to $A\boldsymbol{x} = \boldsymbol{b}$ *where* $A = \begin{pmatrix} 1 & -2 \\ 1 & -1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 2 \\ 1 & 3 \end{pmatrix}$ *and* $\boldsymbol{b} = \begin{pmatrix} -1.97 \\ -1.14 \\ -.60 \\ .22 \\ .89 \\ 1.56 \end{pmatrix}$. *The matrix form of the normal equations for this least squares problem is as follows:*

$$A^{tr}A\boldsymbol{x}' = A^{tr}\boldsymbol{b}, \begin{pmatrix} 6 & 3 \\ 3 & 19 \end{pmatrix} \boldsymbol{x}' = \begin{pmatrix} 1.04 \\ 11.76. \end{pmatrix}$$

The solution to this is $\boldsymbol{x}' = \begin{pmatrix} -.524 \\ .702 \end{pmatrix}$. *Then* $C = e^{-.524} = .59, k = .702$. *Since* $e^{.702} \sim 2.02$, *the data is approximated by the function* $h(x) = .59(2.02)^t$. *We compute*

the vector $\boldsymbol{y}' = \begin{pmatrix} h(-2) \\ h(-1) \\ h(0) \\ h(1) \\ h(2) \\ h(3) \end{pmatrix} = \begin{pmatrix} 0.14 \\ 0.29 \\ 0.59 \\ 1.19 \\ 2.41 \\ 4.86 \end{pmatrix}$. *The error vector is* $\boldsymbol{e} = \boldsymbol{y} - \boldsymbol{y}' = \begin{pmatrix} 0 \\ 0.03 \\ -0.04 \\ 0.05 \\ 0.03 \\ -0.11 \end{pmatrix}$. *The least square error is* $\parallel \boldsymbol{e} \parallel = 0.13$.

The QR Computation of Least Squares Solutions

Let A be a real $m \times n$ matrix, $\boldsymbol{b} \in \mathbb{R}^n, \boldsymbol{b} \notin col(A)$. It is sometimes the case that the entries in A are highly sensitive to small changes, that is, small errors in the calculation of the entries in $A^{tr}A$ can cause significant errors in the solution of $\boldsymbol{x}'$. When the matrix $A^{tr}A$ is invertible, it is therefore sometimes better to calculate the least squares solution using the QR factorization of the matrix A.

We recall that if A is an $m \times n$ real matrix then there is an $m \times n$ matrix Q whose columns form an orthonormal sequence (and a basis for $col(A)$) and an invertible $n \times n$ upper triangular matrix R such that $A = QR$.

In this case the matrix form of the normal equations, $(A^{tr}A)\boldsymbol{x}' = A^{tr}\boldsymbol{b}$, becomes

$$[(QR)^{tr}(QR)]\boldsymbol{x}' = (QR)^{tr}\boldsymbol{b}. \tag{13.10}$$

Using the fact that $(BC)^{tr} = C^{tr}B^{tr}$, (13.10) becomes

$$[R^{tr}(Q^{tr}Q)R]\boldsymbol{x}' = R^{tr}Q^{tr}\boldsymbol{b} \tag{13.11}$$

Here we have made use of the fact that Q is an orthogonal matrix to conclude that $Q^{tr}Q = I_n$. Also, since R is invertible, so is R^{tr}, and therefore it can be canceled from both sides. Making use of these two conditions (13.11) now becomes

$$R\boldsymbol{x}' = Q^{tr}\boldsymbol{b}, \boldsymbol{x}' = R^{-1}(Q^{tr}\boldsymbol{b}). \tag{13.12}$$

Example 13.6 *Find the least squares solution to the inconsistent system* $A\boldsymbol{x} = \boldsymbol{b}$ *where* $A = \begin{pmatrix} 1 & 3 & 4 \\ 1 & 3 & 2 \\ 1 & -1 & 2 \\ 1 & -1 & 0 \end{pmatrix}$ *and* $\boldsymbol{b} = \begin{pmatrix} 2 \\ 8 \\ 4 \\ 6 \end{pmatrix}$.

The Gram–Schmidt process yields the following orthonormal basis for $col(A)$:

$$\{\begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}, \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \\ -\frac{1}{2} \end{pmatrix}, \begin{pmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{pmatrix}\}.$$

Set $Q = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}$. *Q is an orthonormal matrix and* $col(Q) = col(A)$. *If we set* $R = Q^{tr}A = \begin{pmatrix} 2 & 2 & 4 \\ 0 & 4 & 2 \\ 0 & 0 & 2 \end{pmatrix}$ *then* $A = QR$. $R^{-1} = \begin{pmatrix} \frac{1}{2} & -\frac{1}{4} & -\frac{3}{4} \\ 0 & \frac{1}{4} & -\frac{1}{4} \\ 0 & 0 & \frac{1}{2} \end{pmatrix}$, $Q^{tr}\boldsymbol{b} = \begin{pmatrix} 10 \\ 0 \\ -4 \end{pmatrix}$ *and* $\boldsymbol{x}' = R^{-1}(Q^{tr}\boldsymbol{b}) = \begin{pmatrix} 8 \\ 1 \\ -2 \end{pmatrix}$.

An excellent source for real-world applications of least squares is ([10]).

Exercises

1. Prove Corollary (13.1).

2. Prove Theorem (13.4).

3. Assume A is a complex $m \times n$ matrix and $A = BC$ is a full rank factorization of A. Let $\boldsymbol{b} \in \mathbb{C}^m$. Prove that the matrix version, $A^*A\boldsymbol{x} = A^*\boldsymbol{b}$, of the normal equations is equivalent to the matrix equation $B^*A\boldsymbol{x} = B^*\boldsymbol{b}$.

In Exercises 4–7 show that the given vector $\boldsymbol{b}$ is not in the column space of the given matrix A. Verify that the columns of A are linearly independent. Write down the normal equations least squares solution to the linear system $A\boldsymbol{x} = \boldsymbol{b}$ and find the unique least square solution $\boldsymbol{x}'$.

4. $A = \begin{pmatrix} 1 & 1 \\ 1 & -3 \\ -2 & 2 \end{pmatrix}, \boldsymbol{b} = \begin{pmatrix} 9 \\ 3 \\ -6 \end{pmatrix}$

5. $A = \begin{pmatrix} 1 & 2 \\ 1 & 1 \\ 1 & 3 \end{pmatrix}, \boldsymbol{b} = \begin{pmatrix} 1 \\ -2 \\ 7 \end{pmatrix}$

6. $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & -1 \end{pmatrix}, \boldsymbol{b} = \begin{pmatrix} 2 \\ 1 \\ 3 \\ 18 \end{pmatrix}$

7. $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & -1 \\ 1 & -1 & 1 \end{pmatrix}, \boldsymbol{b} = \begin{pmatrix} 1 \\ 2 \\ 0 \\ 0 \end{pmatrix}$

In Exercises 8 and 9, show that the given vector $\boldsymbol{b}$ is not in the column space of the given matrix A. Verify that the columns of A are linearly dependent. Write down the normal equations for the least squares solution to the linear system $A\boldsymbol{x} = \boldsymbol{b}$ and find the general least square solution $\boldsymbol{x}'$.

8. $A = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & -1 \\ 1 & 2 & 0 \\ 2 & 1 & 3 \end{pmatrix} . \boldsymbol{b} = \begin{pmatrix} 1 \\ -1 \\ -1 \\ 0 \end{pmatrix}.$

9. $A = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & -1 & 2 \\ 1 & 3 & 1 & 2 \\ -1 & -2 & -1 & -1 \\ -2 & -4 & 0 & -3 \end{pmatrix}, \boldsymbol{b} = \begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$

In Exercises 10 and 11, verify that the given orthonormal sequence is a basis for the column space of the given matrix A. Use this to obtain a QR factorization for A and apply this to find the least square solution to the inconsistent linear system $A\boldsymbol{x} = \boldsymbol{b}$ for the given vector $\boldsymbol{b}$.

10. $A = \begin{pmatrix} 1 & 1 \\ 2 & 8 \\ -2 & -5 \end{pmatrix}, \mathcal{O} = \{ \begin{pmatrix} \frac{1}{3} \\ \frac{2}{3} \\ -\frac{2}{3} \end{pmatrix}, \begin{pmatrix} -\frac{2}{3} \\ \frac{2}{3} \\ \frac{1}{3} \end{pmatrix} \}, \boldsymbol{b} = \begin{pmatrix} 2 \\ 7 \\ 5 \end{pmatrix}.$

11. $A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 2 \\ 1 & -3 & -1 \\ 1 & -3 & -2 \end{pmatrix}, \mathcal{O} = \{ \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}, \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \\ -\frac{1}{2} \end{pmatrix}, \begin{pmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{pmatrix} \}, \boldsymbol{b} = \begin{pmatrix} -1 \\ 1 \\ 2 \\ 4 \end{pmatrix}.$

In Exercises 12 and 13, find the regression line and the least squares error for the given data.

12. $(-2, -3.8), (-1, -1.1), (0, 1.9), (1, 5.2), (2, 8.1)$

13. $(-1, 3.3), (0, 1.6), (1, -.8), (2, -2.5), (3, -4.4)$

In Exercises 14 and 15, find the quadratic polynomial which best approximates the given data.

14. $(-1, 4.1), (0, 2.3), (1, 2.6), (2, 4.2), (3, 8.2)$

15. $(-1, 1.0), (0, .7), (1, 1.2), (2, 2.5), (3, 5.0), (4, 8.7)$

In Exercises 16 and 17, find the exponential function $y = Ce^{kt}$ which best approximates the given data.

16. $(-1, .2), (0, .7), (1, 1.5), (2, 8.5), (3, 36.4)$

17. $(-2, 3.1), (-1, 2.8), (1, 2.3), (2, 2.0), (4, 1.6)$

13.2 Error Correcting Codes

In this section we demonstrate how finite dimensional vector spaces over a finite field can be used to construct error correcting codes.

What You Need to Know

To be successful in understanding the material of this section you should already have gained mastery of the following concepts: a field, vector space over a field, span of a sequence of vectors, spanning sequence of a vector space, a sequence of vectors is linearly independent, basis of a vector space, dimension of a vector space, and a finite field.

Error correcting codes are used whenever a message is transmitted in a digital format over a "noisy" communication channel. This could be a phone call over a land line or wireless, email between two computers, a picture sent from outer space, an MP3 player interpreting digital music in a file, a computer memory system, and many others. The "noise" could be as a result of human error, lightning, solar flares, imperfections in equipment, deterioration of a computer's memory, and so on, which might introduce errors by exchanging some of the digits of the message for other, incorrect digits.

The basic idea is to introduce redundancy into the message. This is a delicate task since one needs to insure that there is enough redundancy so that there is a high probability that errors can be detected and corrected, but not so much redundancy that one has to send messages which are long relative to what we wish to transmit, consequently reducing the "information rate" and making the transmission too costly.

There are six elements to a digital communication system. It begins with a message, which is a string of symbols. This is input to an encoder which adds redundancy (for example it could repeat the message) and creates a codeword. The codeword is sent over the noisy communication channel, which randomly introduces errors (but with low probability for each symbol). Out the other end comes a received string of symbols. This is input to a decoder which detects whether any errors have occurred. In a simple system which only detects errors, if an error has occurred the sender is informed of this and asked to resend the message. In a more complicated scheme, the decoder corrects errors as well as detects them and then sends the message on to the intended recipient. This is pictured schematically in Figure (13.1).

Definition 13.3 *By a* **message** *we will mean a string of symbols in some* **finite alphabet**. *The message is* **binary** *if the alphabet has only two symbols. It is said to be* **q-ary**, *with q some natural number, if the alphabet has q elements. Typically, the alphabet is a finite field, $\mathbb{F}_q$, and consequently q is usually a prime power.*

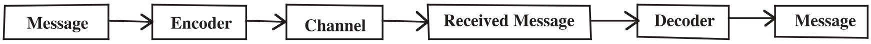

FIGURE 13.1
Sending a Mmessage over a noisy channel.

We ordinarily assume the channel satisfies the following properties:

1) the probability that a symbol α from the alphabet is transmitted and α is received is independent of α; and

2) the probability that a symbol α is sent and $\beta \neq \alpha$ is received is independent of α and β.

Suppose the alphabet has q symbols and the probability that α is sent and received is p. Then the probability that α is sent but α is not received is $1-p$. Since there are $q-1$ possibilities for the received symbols and each is equally likely, by assumption 2) it follows that the probability that α is sent and a fixed $\beta \neq \alpha$ is received is $\frac{1-p}{q-1}$.

It is also assumed that the channel, though noisy, is pretty good, meaning that p is close to one and, therefore, $1-p$ is small.

Example 13.7 *We want to send a message about how to color pixels (in some given order). At any location one can color it "nothing" or white, red, blue, or yellow. In binary, these can be encoded in the following way where we treat 0 and 1 as the elements of the finite field $\mathbb{F}_2$:*

$$white = (0,0), red = (1,0), blue = (0,1), yellow = (1,1). \tag{13.13}$$

These are the message digits that we wish to send but in the present form it is not particularly useful since if an error occurs, we cannot tell since it simply transforms one valid message into another valid message.

We can improve this by adding **redundancy** *in the form of a* **check digit** *–adding a third digit to each message so that the number of ones is even, or the same thing, the sum of the digits is zero (remember our digits are elements of the field $\mathbb{F}_2$). With the introduction of this redundancy, the expressions we use to communicate the colors become*

$$white = (0,0,0), red = (1,0,1), blue = (0,1,1), yellow = (1,1,0). \quad (13.14)$$

Now if one error occurs it can be detected. This information could be communicated and a request made for resending the message, which is, of course, costly and time consuming; if we want to detect and correct errors then more redundancy is needed.

We can systematically add greater redundancy in the following way: If $\boldsymbol{w}$ *is one of the four pairs of (13.13), follow* $\boldsymbol{w}$ *with a check digit and then with* $\boldsymbol{w}$ *again. Thus,*

$$(0,0) \to (0,0,0,0,0), (1,0) \to (1,0,1,1,0)$$

$$(0,1) \to (0,1,1,0,1), (1,1) \to (1,1,0,1,1). \quad (13.15)$$

Now if a single error occurs we can not only detect it but we can correct it by decoding the received vector as the one among the four vectors of (13.15) which is "closest" to it, in the sense that they differ in the minimum number of digits.

For example, if a received vector has a single one and four zeros then it differs from (0,0,0,0,0) in only one place but from all the others in two or more places. Therefore we would decode it as (0,0,0,0,0) = white.

To make the ideas of Example (13.7) more precise requires that we introduce some definitions.

Definition 13.4 *Let* $\mathbb{F}_q$ *be a finite field. By a* **q-ary word of length n** *we will mean an element of the vector space* $\mathbb{F}_q^n$ *written as a row.*

Definition 13.5 *Let* $\boldsymbol{x} = (a_1\ a_2 \ldots\ a_n)$ *be a q-ary word of length n. Then the* **weight** *of* $\boldsymbol{x}$*, denoted by* $wt(\boldsymbol{x})$*, is the number of* i *such that* $a_i \neq 0$.

The following property of the weight function is fundamental. We leave it as an exercise.

Theorem 13.8 *Let* $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$*. Then* $wt(\boldsymbol{x}+\boldsymbol{y}) \leq wt(\boldsymbol{x}) + wt(\boldsymbol{y})$.

Making use of the weight function we can introduce a concept of distance between words first formulated by the coding theory pioneer Richard Hamming.

Definition 13.6 *Let $\boldsymbol{x} = (a_1\ a_2 \ldots\ a_n)$ and $\boldsymbol{y} = (b_1\ b_2 \ldots\ b_n)$ be two q-ary words of length n. Then the* **Hamming distance** *between $\boldsymbol{x}$ and $\boldsymbol{y}$, denoted by $d(\boldsymbol{x}, \boldsymbol{y})$, is the number of i such that $a_i \neq b_i$.*

Note that if $\boldsymbol{x} = (a_1 \ldots a_n), \boldsymbol{y} = (b_1 \ldots b_n)$ are q-ary words then $a_i \neq b_i$ if and only if the i^{th} component of $\boldsymbol{x} - \boldsymbol{y}$ is non-zero. Consequently, we have the following:

Theorem 13.9 *Let $\boldsymbol{x}, \boldsymbol{y}$ be words from $\mathbb{F}_q^n$. Then $d(\boldsymbol{x}, \boldsymbol{y}) = wt(\boldsymbol{x} - \boldsymbol{y})$. In particular, $d(\boldsymbol{x}, \boldsymbol{0}_n) = wt(\boldsymbol{x})$.*

In our next result we collect some properties of the Hamming distance function.

Theorem 13.10 *i) For any vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n, d(\boldsymbol{x}, \boldsymbol{y}) \geq 0$ with equality if and only if $\boldsymbol{x} = \boldsymbol{y}$.*

ii) For vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ in $\mathbb{F}_q, d(\boldsymbol{x}, \boldsymbol{y}) = d(\boldsymbol{y}, \boldsymbol{x})$.

iii) The "triangle inequality holds": For vectors $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in \mathbb{F}_q$ $d(\boldsymbol{x}, \boldsymbol{z}) \leq d(\boldsymbol{x}, \boldsymbol{y}) + d(\boldsymbol{y}, \boldsymbol{z})$.

The first and second should be clear. The third is left as an exercise.

An important concept, for both conceptual and theoretic purposes, is the notion of a ball of radius r about a vector $\boldsymbol{w}$.

Definition 13.7 *Let $\boldsymbol{w}$ be a word in $\mathbb{F}_q^n$ and r a natural number. The* **ball of radius** r **with center** $\boldsymbol{w}$*, denoted by $B_r(\boldsymbol{w})$, consists of all the q-ary words of length n whose Hamming distance from $\boldsymbol{w}$ is less than or equal to r :*

$$B_r(\boldsymbol{w}) = \{\boldsymbol{x} \in \mathbb{F}_q^n : d(\boldsymbol{w}, \boldsymbol{x}) \leq r\}.$$

Example 13.8 *The ball of radius one with center at (0,0,0,0,0) in $\mathbb{F}_2$ consists of (0,0,0,0,0) and all the words of weight one. For $\boldsymbol{w} = (1, 0, 1, 1, 0)$,*

$$B_1(\boldsymbol{w}) = \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}^{tr}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}^{tr}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}^{tr}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}^{tr}, \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}^{tr}, \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} \right\}.$$

The balls of radius one centered at the four words shown in (13.15) do not intersect.

One can easily count the number of vectors in a ball of radius r. We state the result and leave it as a exercise.

Theorem 13.11 *Let $\boldsymbol{w} \in \mathbb{F}_q^n$.*

i) Let t be a nonnegative integer. Then the number of $\boldsymbol{x} \in \mathbb{F}_q^n$ such that $d(\boldsymbol{w}, \boldsymbol{x}) = t$ is $\binom{n}{t}(q-1)^t$.

ii) Let r be a nonnegative integer. Then the number of vectors in $B_r(\boldsymbol{w})$ is

$$1 + n(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{r}(q-1)^r.$$

We are now ready to define what we mean by a code with alphabet $\mathbb{F}_q$, where q is a power of a prime.

Definition 13.8 *A* **code** *is a subset $\mathcal{C}$ of some finite vector space $\mathbb{F}_q^n$. The* **length** *of the code is n. If the number of elements in $\mathcal{C}$ is K then we say that $\mathcal{C}$ is an* **(n,K)-code** *over $\mathbb{F}_q$.*

A code $\mathcal{C}$ of length n is said to be a **linear code over** *$\mathbb{F}_q$, if $\mathcal{C}$ is a subspace of $\mathbb{F}_q^n$. If the dimension of $\mathcal{C}$ is k, then we say that $\mathcal{C}$ is an* **(n,k)-linear code** *over $\mathbb{F}_q$.*

Example 13.9 *The collection of four vectors in (13.15) is a (5,2)-linear code over $\mathbb{F}_2$.*

In Example (13.7) we added sufficient redundancy so that the Hamming distance between any pairs of code words is always large enough so that we could detect and correct single errors. Making this rigorous requires some further definitions.

Definition 13.9 *Let $\mathcal{C}$ be a code of length n over $\mathbb{F}_q$. The* **minimum distance** *of $\mathcal{C}$ is*

$$d(\mathcal{C}) = min\{d(\boldsymbol{x}, \boldsymbol{y}) : \boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}, \boldsymbol{x} \neq \boldsymbol{y}\}.$$

In other words, it is the minimum distance obtained between any two distinct codewords from $\mathcal{C}$.

The importance of the minimum distance of a code is indicated by the following result:

Theorem 13.12 *Let $\mathcal{C}$ be an (n,K)-code over $\mathbb{F}_q$ and assume that $d(\mathcal{C}) = d$. Then the following hold:*

i) $\mathcal{C}$ can detect up to e errors as long as $d \geq e + 1$.

ii) $\mathcal{C}$ can correct up to c errors as long as $d \geq 2c + 1$.

Conceptually, i) holds because the ball of radius $d - 1$ centered at a codeword does not contain any other codewords. Also, ii) holds because two balls with radius c such that $2c + 1 \leq d$ and centered at distinct codewords are disjoint.

Proof *i) Suppose that a codeword $\boldsymbol{w}$ is transmitted, the word $\boldsymbol{x}$ is received, and there are e errors with $e < d$. The number of errors is simply $d(\boldsymbol{w}, \boldsymbol{x})$. Since $d(\boldsymbol{w}, \boldsymbol{x}) = e < d$ it cannot be that $\boldsymbol{x}$ is another codeword and, consequently, we can detect that an error occurred.*

ii) Suppose $\boldsymbol{w}$ is transmitted and $\boldsymbol{x}$ is received with c errors, where $2c + 1 \leq d$. We claim that for any codeword $\boldsymbol{w}' \neq \boldsymbol{w}$ that $d(\boldsymbol{x}, \boldsymbol{w}') > c$ and therefore amongst $\mathcal{C}, \boldsymbol{w}$ is the unique nearest neighbor to $\boldsymbol{x}$. To see this claim, assume to the contrary that $d(\boldsymbol{x}, \boldsymbol{w}') \leq c$ for some codeword $\boldsymbol{w}' \neq \boldsymbol{w}$. Then

$$d \leq d(\boldsymbol{w}, \boldsymbol{w}') \leq d(\boldsymbol{w}, \boldsymbol{x}) + d(\boldsymbol{x}, \boldsymbol{w}') \leq c + c = 2c < d \tag{13.16}$$

by the triangle inequality and the definition of d. We therefore have a contradiction.

There are many advantages to working with linear codes as contrasted with more general codes. One is that they can be constructed using matrix multiplication. Another is that the computation of the minimum distance of the code is simplified and does not require computing the distances between every pair of vectors in the code. Before showing this we require another definition.

Definition 13.10 *Let $\mathcal{C}$ be an (n,k)-linear code over $\mathbb{F}_q$. The* **minimum weight** *of $\mathcal{C}$, denoted by $m(\mathcal{C})$, is*

$$min\{wt(\boldsymbol{w}) : \boldsymbol{w} \in \mathcal{C}, \boldsymbol{w} \neq \mathbf{0}_n\}.$$

This next theorem indicates the relationship between $d(\mathcal{C})$ and $m(\mathcal{C})$ for a linear code.

Theorem 13.13 *Let $\mathcal{C}$ be an (n,k)-linear code over $\mathbb{F}_q$. Then $d(\mathcal{C}) = m(\mathcal{C})$.*

Proof *By the definition of minimal distance, $d(\mathcal{C}) = min\{d(\boldsymbol{x}, \boldsymbol{y}) : \boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}, \boldsymbol{x} \neq \boldsymbol{y}\}$. Since $d(\boldsymbol{x}, \boldsymbol{y}) = wt(\boldsymbol{x} - \boldsymbol{y})$, it therefore follows that $d(\mathcal{C}) = min\{wt(\boldsymbol{x} - \boldsymbol{y}) : \boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}, \boldsymbol{x} \neq \boldsymbol{y}\}$. Since $\mathcal{C}$ is a linear code, as $(\boldsymbol{x}, \boldsymbol{y})$ runs over all pairs from $\mathcal{C}$ with $\boldsymbol{x} \neq \boldsymbol{y}$, $\boldsymbol{x} - \boldsymbol{y}$ runs over all nonzero vectors in $\mathcal{C}$. Thus, $min\{wt(\boldsymbol{x} - \boldsymbol{y}) : \boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}, \boldsymbol{x} \neq \boldsymbol{y}\} = m(\mathcal{C})$ as claimed.*

As we shall see, linear codes can be constructed with a designed minimum weight and in this way no computation will be required to determine the minimum distance and, therefore, the error detecting and error correcting capacity of the code. In the next example we show how the code of (13.15) can be constructed from the original message by matrix multiplication.

Example 13.10 *Let $G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$. Then*

$$(0,0)G = (0,0,0,0,0), (1,0)G = (1,0,1,1,0)$$

$$(0,1)G = (0,1,1,0,1), (1,1)G = (1,1,0,1,1).$$

Notice that the sequence of rows of the matrix G of Example (13.10) is a basis for this linear code. This is an example of a generator matrix for a code.

Definition 13.11 *Let $\mathcal{C}$ be an (n,k)-linear code over $\mathbb{F}_q$. Any $k \times n$ matrix G whose rows consists of a basis for $\mathcal{C}$ is a* **generator matrix of** $\mathcal{C}$. *The matrix G is said to be* **systematic** *if G has the form $(I_k B)$ where B is a $k \times (n-k)$ matrix.*

Note that since the rows of G are a basis, the rank of G is equal to k.

We can use a generator matrix to encode a message of length k by matrix multiplication: Given a message $\boldsymbol{m} = (a_1, a_1, \ldots, a_k)$, encode this as $\boldsymbol{m}G$. If G is systemic then the first k digits of the codeword $\boldsymbol{m}G$ will be the message $\boldsymbol{m}$.

In addition to encoding messages on the transmission end, we need a decoder on the receiving end to detect whether errors have occurred, correct them, if possible, and deliver the original message to the user. The parity check matrix will fulfill this purpose. First, some more definitions.

Definition 13.12 *Let $\boldsymbol{x} = (a_1\ a_2 \ldots\ a_n)$ and $\boldsymbol{y} = (b_1\ b_2 \ldots\ b_n)$ be two vectors in $\mathbb{F}_q^n$. Then the* **dot product** *of $\boldsymbol{x}$ and $\boldsymbol{y}$, denoted by $\boldsymbol{x} \boldsymbol{\cdot} \boldsymbol{y}$, is map from $\mathbb{F}_q^n \times \mathbb{F}_q^n$ to $\mathbb{F}$ given by*

$$a_1b_1 + a_2b_2 + \ldots a_nb_n.$$

The following summarizes the fact that the dot product is a symmetric bilinear form on $\mathbb{F}_q^n$.

Theorem 13.14 *Let $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ be vectors in $\mathbb{F}_q^n$ and $c \in \mathbb{F}_q$. Then the following hold:*

i) $\boldsymbol{x} \centerdot \boldsymbol{y} = \boldsymbol{y} \centerdot \boldsymbol{x}$.

ii) $\boldsymbol{x} \centerdot [\boldsymbol{y} + \boldsymbol{z}] = \boldsymbol{x} \centerdot \boldsymbol{y} + \boldsymbol{x} \centerdot \boldsymbol{z}$.

iii) $c[\boldsymbol{x} \centerdot \boldsymbol{y}] = (c\boldsymbol{x}) \centerdot \boldsymbol{y} = \boldsymbol{x} \centerdot (c\boldsymbol{y})$.

Proof *i) This holds since the multiplication in $\mathbb{F}_q$ is commutative: If $\boldsymbol{x} = (x_1 \ \ldots \ x_n), \boldsymbol{y} = (y_1 \ \ldots \ y_n)$ then for each $i, x_iy_i = y_ix_i$.*

ii) This holds since the distributive property holds in $\mathbb{F}_q$: If also $\boldsymbol{z} = (z_1 \ \ldots \ z_n)$ then for each i we have

$$x_i(y_i + z_i) = x_iy_i + x_iz_i.$$

iii) This holds because the multiplication in $\mathbb{F}_q$ is associative and commutative: For each i

$$c(x_iy_i) = (cx_i)y_i = (x_ic)y_i = x_i(cy_i).$$

We will say that q-ary words $\boldsymbol{x}$ and $\boldsymbol{y}$ are **orthogonal** if $\boldsymbol{x} \cdot \boldsymbol{y} = 0$.

Definition 13.13 *Let $\mathcal{C}$ be a subspace (linear code) of $\mathbb{F}_q^n$. The* **orthogonal complement** *to $\mathcal{C}$, denoted by $\mathcal{C}^{\perp}$, is $\{\boldsymbol{y} \in \mathbb{F}_q^n | \boldsymbol{x} \cdot \boldsymbol{y} = 0$ for all $\boldsymbol{y} \in \mathcal{C}\}$. When $\mathcal{C}$ is considered a linear code we refer to $\mathcal{C}^{\perp}$ as the* **dual code**.

Theorem 13.15 *Assume $\mathcal{C}$ is an (n,k)-linear code over $\mathbb{F}_q$. Then the dual code $\mathcal{C}^{\perp}$ is an (n,n-k) linear code.*

Proof *Since the dot product is a symmetric bilinear form, it follows that $\mathcal{C}^{\perp}$ is a subspace of $\mathbb{F}_q^n$, so it remains to prove that $dim(\mathcal{C}^{\perp}) = n - k$.*

Let A be the matrix whose i^{th} row is $\boldsymbol{x}_i$. It then follows that $\boldsymbol{y} \in \mathcal{C}^{\perp}$ if and only if $\boldsymbol{y}^{tr}$ is in the null space of A. By the rank-nullity theorem for matrices, it follows that $dim(\mathcal{C}) + dim(\mathcal{C}^{\perp}) = n$, so that $dim(\mathcal{C}^{\perp}) = n - k$.

Example 13.11 *For the code* $\mathcal{C} = Span\,((1,0,1,1,0),(0,1,1,0,1))$ *the dual code is* $Span\,((1,0,0,1,0),(0,1,0,0,1),(1,1,1,0,0))$ *which consists of the eight vectors*

$$(0,0,0,0,0),(1,0,0,1,0),(0,1,0,0,1),(1,1,1,0,0)$$

$$(1,1,0,1,1),(0,1,1,1,0),(1,0,1,0,1),(0,0,1,1,1).$$

We can now define what is meant by a parity check matrix for an linear code $\mathcal{C}$ over $\mathbb{F}_q$.

Definition 13.14 *Let* $\mathcal{C}$ *be an* (n,k)*-linear code over* $\mathbb{F}_q$*. Any generator matrix* H *for the dual code* $\mathcal{C}^{\perp}$ *of* $\mathcal{C}$ *is a* **parity check matrix for** $\mathcal{C}$*.*

Example 13.12 *From Example (13.11) the matrix*

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix},$$

is a parity check matrix for the binary code

$$\mathcal{C} = \{(0,0,0,0,0),(1,0,1,1,0),(0,1,1,0,1),(1,1,0,1,1)\}.$$

In part, the importance of the parity check matrix is indicated by the following:

Theorem 13.16 *Let* $\mathcal{C}$ *be an* (n,k)*-linear code over* $\mathbb{F}_q$ *and* H *a parity check matrix. Then* $\boldsymbol{w} \in \mathbb{F}_q^n$ *is a codeword if and only if* $H\boldsymbol{w}^{tr} = \mathbf{0}_{n-k}$*.*

Proof *Suppose* $\boldsymbol{w} \in \mathcal{C}$*. Then* $\boldsymbol{w}$ *is perpendicular to every row of* H *by the definition of* H*. In particular, the product of* $\boldsymbol{w}$ *with each row of* H^{tr} *is zero and therefore* $H\boldsymbol{w}^{tr} = \mathbf{0}_{n-k}$*.*

Conversely, the rank of H *is* $n-k$ *since its rows are linearly independent. Therefore the null space of* H *has dimension* $n-(n-k) = k$*. However,* $null(H)$ *contains* $\{\boldsymbol{w}^{tr} : \boldsymbol{w} \in \mathcal{C}\}$*, which has dimension* k *and therefore this is all of* $null(H)$*.*

It is especially easy to obtain a parity check matrix for a linear code $\mathcal{C}$ from a systematic generator matrix $G = (I_k B)$ for $\mathcal{C}$. This is made explicit in the next result.

Theorem 13.17 *Assume that $G = (I_kB)$ is a systematic generator matrix for an (n,k)-linear code $\mathcal{C}$ over $\mathbb{F}_q$. Then $H = (-B^{tr}I_{n-k})$ is a partity check matrix for $\mathcal{C}$.*

Proof *H is an $(n-k)\times n$ matrix and the last $n-k$ columns are a basis for $\mathbb{F}_q^{n-k}$. Therefore, H has rank $n-k$. By Theorem (13.16) we will be done if we can show that $HG^{tr} = \mathbf{0}_{(n-k)\times k}$. We compute this product:*

$$HG^{tr} = (-B^{tr}I_{n-k})\begin{pmatrix} I_k \\ B^{tr}\end{pmatrix} = -B^{tr}I_k + I_{n-k}B^{tr} = -B^{tr} + B^{tr} = \mathbf{0}_{(n-k)\times k}.$$

Example 13.13 *The matrix $G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1\end{pmatrix}$ is a systematic generator matrix for the code $\mathcal{C} = Span\,((1,0,1,1,0),(0,1,1,0,1))$. The parity check matrix we obtain from this is $H' = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1\end{pmatrix}$.*

In our next result we indicate how a parity check matrix H for a linear code $\mathcal{C}$ can be used to determine the minimum weight of $\mathcal{C}$.

Theorem 13.18 *Let H be a parity check matrix for an (n,k)-code $\mathcal{C}$ over $\mathbb{F}_q$. Assume that every sequence of $d-1$ columns of H is linearly independent but some sequence of d columns is linearly dependent. Then $m(\mathcal{C}) = d$.*

Proof *Denote by $\mathbf{c}_j, 1 \le j \le n$, the columns of H. Suppose for the sake of the proof that the sequence of the first d columns, $S = (\boldsymbol{c}_1, \dots, \boldsymbol{c}_d)$ of H, is linearly dependent. Let*

$$a_1\boldsymbol{c}_1 + a_2\boldsymbol{c}_2 + \cdots + a_d\mathbf{c}_d = \mathbf{0}_n$$

be a non-trivial dependence relation of S. Then the vector $\boldsymbol{x} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_d \\ 0 \\ \vdots \\ 0\end{pmatrix}$ satisfies

$H\boldsymbol{x} = \mathbf{0}_{n-k}$ and therefore $\boldsymbol{w} = \boldsymbol{x}^{tr} \in \mathcal{C}$ by Theorem (13.16). Since $wt(\boldsymbol{w}) = d$, we conclude that $m(\mathcal{C}) \leq d$.

On the other hand, suppose $\boldsymbol{y}$ is a vector with weight less than d and $H\boldsymbol{y}^{tr} = \mathbf{0}_{n-k}$. Suppose $\boldsymbol{y}$ is nonzero and let the nonzero entries in $\boldsymbol{y}$ be $b_{i_1}, b_{i_2}, \ldots, b_{i_t}$ where $t < d$. Since $H\boldsymbol{y}^{tr} = \mathbf{0}_{n-k}$, we conclude that

$$b_{i_1}\boldsymbol{c}_{i_1} + b_{i_2}\boldsymbol{c}_{i_2} + \cdots + b_{i_t}\boldsymbol{c}_{i_t} = \mathbf{0}_{n-k}.$$

This implies that the sequence of columns $(\boldsymbol{c}_{i_1}, \boldsymbol{c}_{i_2}, \ldots, \boldsymbol{c}_{i_t})$ is linearly dependent. Since $t < d$, this contradicts our hypothesis. Thus, no nonzero vector in $\mathcal{C}$ has weight less than d and the minimum weight of $\mathcal{C}$ is exactly d.

If the columns of a parity check matrix H of a linear code $\mathcal{C}$ are all distinct then from Theorem (13.18) we can conclude that the minimum weight is at least two and we can detect a single error. If no two columns of H are multiples of one another, that is, every pair of columns of H is linearly independent then the minimum weight of the code is greater than equal to three and we can correct single errors. Note that for binary codes, a pair of nonzero vectors is linearly independent if and only if they are distinct.

Example 13.14 *Let H be the matrix whose columns are all the nonzero vectors in $\mathbb{F}_2^3$. We use H as the parity check matrix of a code. We will treat the vectors in $\mathbb{F}_2^3$ as a binary expression for a natural number where $\begin{pmatrix}1\\0\\0\end{pmatrix} = 1, \begin{pmatrix}0\\1\\0\end{pmatrix} = 2, \begin{pmatrix}0\\0\\1\end{pmatrix} = 4$. This will be of use in our decoding scheme.*

We order the columns from 1 to 7. Thus, $H = \begin{pmatrix}1&0&1&0&1&0&1\\0&1&1&0&0&1&1\\0&0&0&1&1&1&1\end{pmatrix}$.

Since the sequence of standard basis vectors of $\mathbb{F}_2^3$ is a subsequence of the columns of H, it follows that H has rank three. Let $\mathcal{H}(3,2)$ denote the code that is dual to the row space of H. In this notation the (3,2) indicates that the columns of the parity check matrix H are the 3-vectors over $\mathbb{F}_2$. This resulting code is referred to as a binary Hamming code. It is a linear (7,4)-code over $\mathbb{F}_2$.

Since the columns of H are all distinct and this is a binary matrix, the minimum weight of $\mathcal{H}(3,2)$ is at least 3. On the other hand, the sum of the first three columns of H is the zero vector and therefore the minimum weight is exactly 3. Thus, $\mathcal{H}(3,2)$ is a 1-error correcting code.

Notice that a ball of radius one centered at a word contains 1 + 7 = 8 words. If we consider the balls of radius one around the 16 codewords then these are disjoint and so the number of words they jointly cover is $16 \times 8 = 128 = 2^7$. That, is, each word is contained in exactly one of these balls.

Let $\boldsymbol{e}_i, i = 1, 2, \ldots, 7$ *denote the standard basis of* $\mathbb{F}_2^7$*. Now suppose some codeword* $\boldsymbol{w}$ *is sent,* $\boldsymbol{x}$ *is received, and one error occurred, say in the* i^{th} *position. Then by the definition of* $\boldsymbol{e}_i, \boldsymbol{x} = \boldsymbol{w} + \boldsymbol{e}_i$*. We can deduce that an error has occurred since* $H\boldsymbol{x}^{tr} \neq \mathbf{0}_3$*. But we get more information. The nonzero vector* $H\boldsymbol{x}^{tr}$ *is called the* **syndrome** *of* $\boldsymbol{x}$*, and is denoted by* $S(\boldsymbol{x})$*. In this example, it will tell us precisely where the error occurred.*

Since $\boldsymbol{x} = \boldsymbol{w} + \boldsymbol{e}_i, S(\boldsymbol{x}) = H\boldsymbol{x}^{tr} = H(\boldsymbol{w}^{tr} + \boldsymbol{e}_i^{tr}) = H\boldsymbol{w}^{tr} + H\boldsymbol{e}_i^{tr} = H\boldsymbol{e}_i^{tr}$ *because* $\boldsymbol{w}$ *is in the code and therefore* $H\boldsymbol{w}^{tr} = \mathbf{0}_3$*.*

Since $\boldsymbol{e}_i$ *is the* i^{th} *standard basis vector of* $\mathbb{F}_2^7, H\boldsymbol{e}_i^{tr}$ *is the* i^{th} *column of* H*. This gives us a decoding scheme:*

Take the received word $\boldsymbol{x}$ *and compute its syndrome* $S(\boldsymbol{x}) = H\boldsymbol{x}^{tr}$*. If* $S(\boldsymbol{x}) = \mathbf{0}_3$ *then* $\boldsymbol{x}$ *is codeword and the intended message can be obtained from the received word* $\boldsymbol{x}$ *(though how depends on the encoder used). If* $S(\boldsymbol{x}) = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \neq \mathbf{0}_3$ *then let* i *be the natural number with binary expansion* $a_3a_2a_1$*. Set* $\boldsymbol{w} = \boldsymbol{x} + \boldsymbol{e}_i$*. This will be a codeword (the unique one at distance one from* $\boldsymbol{x}$*) and we decode as* $\boldsymbol{w}$*.*

As a concrete example, suppose the word $\boldsymbol{x} = (0111110)$ *is received. Then the syndrome of this vector is*

$$S(\boldsymbol{x}) = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} =$$

$$\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}.$$

The vector $\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$ *is binary for 6. Thus, if one error occurred it was in the sixth position. Therefore the codeword sent was (0111100).*

The code of Example (13.14) is one in a family of 1-error correcting codes where the balls of radius one centered at the codewords cover all the words. Such codes are said to be ***perfect 1-error correcting codes***. We define these below.

Definition 13.15 *Assume $\mathcal{C}$ is a subspace of $\mathbb{F}_q^n$ is a d-error correcting codes. If $\{B_d(\boldsymbol{w})|\boldsymbol{w} \in \mathcal{C}\}$ is a partition of $\mathbb{F}_q^n$ then $\mathcal{C}$ is said to be a* **perfect d-error correcting code**.

Hamming Codes

Definition 13.16 *Let q be a prime power and $n \geq 2$ a natural number. The number of one-dimensional subspaces of $\mathbb{F}_q^n$ is $t = \frac{q^n-1}{q-1}$. For each one dimensional subspace W of $\mathbb{F}_q^n$, choose the vector $\boldsymbol{w}$ such that $Span(\boldsymbol{w}) = W$ and such that the first nonzero entry in $\boldsymbol{w}$ is one. Put these vectors into lexicographical order and label them as $\boldsymbol{w}_1, \dots, \boldsymbol{w}_t$. Let $H(n,q)$ be the matrix whose columns are the vectors $\boldsymbol{w}_1, \dots, \boldsymbol{w}_t$. Let $\mathcal{H}(n,q)$ be the linear code with parity check matrix $H(n,q)$. This is referred to as the Hamming (n,q)-code.*

In the next result we state some of the properties of the Hamming codes and leave the proofs as an exercise.

Theorem 13.19 *The code $\mathcal{H}(n.q)$ has length $t = \frac{q^n-1}{q-1}$ and dimension $t - n$. It has minimum distance 3. It is a perfect one-error correcting code.*

Clearly, one needs to do better than be able to correct one error and it is not difficult to define such codes using Theorem (13.18). We show how to construct linear codes with a designed minimum weight.

BCH-codes

Let $\alpha_1, \alpha_2, \dots, \alpha_{q-1}$ be the nonzero elements of the finite field $\mathbb{F}_q$ and let t be a natural number, $t \leq q-1$.

Let H be the following matrix

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_{q-1} \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_{q-1}^2 \\ \vdots & \vdots & \dots & \vdots \\ \alpha_1^{t-1} & \alpha_2^{t-1} & \dots & \alpha_{q-1}^{t-1} \end{pmatrix}.$$

We will show that any t columns from H are linearly independent. Suppose $\beta_1, \beta_2, \dots, \beta_t$ is a subset of $\{\alpha_1, \alpha_2, \dots, \alpha_{q-1}\}$. Consider the square matrix made from the columns $\begin{pmatrix} 1 \\ \beta_i \\ \beta_i^2 \\ \vdots \\ \beta_i^{t-1} \end{pmatrix}$. This matrix is $\begin{pmatrix} 1 & 1 & \dots & 1 \\ \beta_1 & \beta_2 & \dots & \beta_t \\ \beta_1^2 & \beta_2^2 & \dots & \beta_t^2 \\ \vdots & \vdots & \dots & \vdots \\ \beta_1^{t-1} & \beta_2^{t-1} & \dots & \beta_t^{t-1} \end{pmatrix}$.

This is a Vandermonde matrix which is invertible with determinant $\Pi_{1\leq i<j\leq t}(\beta_j - \beta_i)$. Consequently, any sequence of t columns is linearly independent. Since there are only t rows, the rank of H is exactly t and a sequence of any $t+1$ columns is linearly dependent.

From what we have shown, if $\mathcal{C}$ is the code with parity check matrix H then $\mathcal{C}$ is a (q-1, q-t-1) linear code with minimum weight $t+1$. Therefore, if $2e+1 \leq t$ this code can be used to correct e errors.

To be useful, that is, actually implemented, requires the existence of an algorithm to do the encoding and decoding. Any generator matrix can be used for the encoding. An algorithm for decoding exists for these codes, based on ideas from number theory developed by the Indian mathematician Ramanujan. The codes are known as BCH codes. They were invented in 1959 by Hocquenghem and independently by Bose and Ray-Chaudhuri and they have been used fairly extensively.

Example 13.15 *Denote the elements of* $\mathbb{F}_{11}$ *by* $\{0,1,2,3,4,5,6,7,8,9,X\}$. *Let* H *be the matrix*

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & X \\ 1 & 4 & 9 & 5 & 3 & 3 & 5 & 9 & 4 & 1 \\ 1 & 3 & 5 & 9 & 4 & 7 & 2 & 8 & 3 & X \end{pmatrix}.$$

This is the parity check matrix for the BCH code $\mathcal{BCH}(11,4)$ *of length 10 with designed minimum weight 5 over the field* $\mathbb{F}_{11}$ *Since there are 10 columns and the rank is four, the nullity is six and therefore the code* $\mathcal{BCH}(11,4)$ *has dimension six and is therefore a (10,6)-linear code over* $\mathbb{F}_{11}$ *with minimum weight 5. It is a double error correcting code.*

A very accessible treatment of error correcting codes is ([18]).

Exercises

1. Let $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$. Prove that $wt(\boldsymbol{x}+\boldsymbol{y}) \leq wt(\boldsymbol{x}) + wt(\boldsymbol{y})$.

2. Prove part iii. of Theorem (13.10).

3. Prove Theorem (13.11).

A linear code $\mathcal{C}$ is called **self-dual** if it is contained in its dual code $\mathcal{C}^\perp$, equivalently, if every pair of codewords in $\mathcal{C}$ is orthogonal.

4. Assume that $\mathcal{C}$ is a self-dual (2n,k)-code over the field $\mathbb{F}_q$. Prove that $k \leq n$.

5. a) Show that in the binary Hamming code $\mathcal{H}(3,2)$ there are equally many codewords of weight w and $7-w$.

b) Without writing out all the codewords, prove that there are 7 codewords of weight 3, and 7 of weight 4 in the binary Hamming code $\mathcal{H}(3,2)$. (Hint: Make use of a) and the fact that the minimum weight of $\mathcal{H}(3,2)$ is 3.)

6. Let $\overline{\mathcal{H}}(3,2)$ be the ***extended binary Hamming code***, that is, the code obtained from $\mathcal{H}(3,2)$ by adding an overall parity check. Prove that this code contains the zero vector, the all-one vector, and 14 vectors of weight 4. (Hint: Make use of 2b)).

7. Let $\boldsymbol{x}$ be a word in $\mathbb{F}_2^n$. Prove that $\boldsymbol{x} \cdot \boldsymbol{x} = 0$ if and only if the weight of $\boldsymbol{x}$ is even.

For a vector $\boldsymbol{x} = (x_1\ x_2\ \dots\ x_n)$ in $\mathbb{F}_2^n$ let the ***support*** of $\boldsymbol{x}, spt(\boldsymbol{x})$, be the subset of $\{1, 2, \dots, n\}$ such that $x_i \neq 0$. For example, the support of (1001011) is $\{1, 4, 6, 7\}$.

8. Let $\boldsymbol{x}, \boldsymbol{y}$ be words in $\mathbb{F}_2^n$. Prove that $\boldsymbol{x} \cdot \boldsymbol{y} = 0$ if and only if there are an even number of elements in the intersection of $spt(\boldsymbol{x}) \cap spt(\boldsymbol{y})$.

9. Prove that the extended binary Hamming code $\overline{\mathcal{H}}(3,2)$ is a self-dual code. (Hint: Use Exercises 6, 7, and 8).

10. Suppose $\mathcal{C}$ is a (23, 12) binary linear code and the minimum weight is seven. Prove that the balls of radius 3 centered at the codewords are disjoint and cover all the vectors in $\mathbb{F}_2^{23}$. (This means that this is a **perfect** 3-error correcting code. Such a code exists and is unique. It is known as the ***binary Golay code***).

11. Prove Theorem (13.19).

13.3 Ranking Webpages for Search Engines

In this section we show how linear algebra is applied to develop query independent rankings of webpages that might be used by a search engine.

What You Need to Know

In order to understand the new material of this section you should have mastered the following concepts: eigenvalue and eigenvector of a square matrix, nonnegative matrix, positive vector, positive matrix, irreducible matrix, primitive matrix, probability vector, stochastic matrix, stationary vector of a stochastic matrix, and the Perron vector of a positive matrix.

Search engines are essential utilities for using the world wide web and have been since its origins. Their task is to find, among billions of webpages, those that best answer a query submitted by a user. The query may be a question (Which team was the last of the major league ball clubs to sign an African America player?) or a collection of words or phrases. The search engine will first determine, among all indexed webpages, which ones exceed some measure of relevance to the query. This will usually return thousands, perhaps even millions of candidates. This is not of practical use since the time to examine all of them is prohibitive. Therefore it is necessary for the search engine to rank order the relevant pages. PageRank, developed by Larry Page and Sergei Brin who founded the company Google, is such a method and the basis of the rankings used by the search engine they invented. We will describe how PageRank computes its ratings by computing eigenvectors for a large square matrix called the Google matrix. This matrix is constructed from a sparse matrix (one with mostly zero entries) which captures the link structure of the world wide web and is designed to have spectral radius one and such that the eigenvalue one has algebraic multiplicity one. We will also say something about how a search engine decides if a page is relevant to a query since this, too, involves linear algebra. Before we turn to these two objectives we first describe the elements of a search engine to see how determining the relevance of a web page to a query and ranking web pages fit into the entire process of a search.

The main elements of a search engine are a crawler module, a page repository, an indexing module, the indexes, the query module, and the ranking module, the last two are the ones relevant to this section.

The **crawler module** is responsible for collecting and characterizing the documents on the web. Its software creates “spiders,” which are virtual robots that search the web for new webpages and returns with copies to be placed in a **page repository**. The pages accumulated by the spiders are temporarily stored there until sent to the **indexing module** where its essential information (important descriptors and terms, as well as the links to and from the page) is extracted, compressed and then stored in several **indexes**. One such index is the **content index** where keywords, title, and anchor text are stored. Information about the links to and from the page are stored in the **structure index**. In addition there are other, special-purpose indexes.

The **query module** translates the search engine user's query from natural language into a format that can be understood by the search engine and compared with the content of indexed pages to determine which ones include the query terms. The pages that are returned are the **relevant pages**.

Finally, the **ranking module** rank orders the pages returned by the query module with the intent that the pages at the top of the ordering are those sought by the user. The ranking module is the most important component of the search engine since the query module will almost always return far too many relevant pages (from thousands to millions) to be of value to the user. Typically, the ranking consists of two components, a **content score** and a **popularity score**.

To understand the basic idea underlying how this is determined, imagine that a web surfer starts at an arbitrary web page and then proceeds to the next page via one of the outlinks from that page, where each outlink is equally probable of being selected. The ranking of a particular page is determined by the probability of ending at that page over the long run (made precise by the notion of limit). This will only work if the probabilities obtained are independent of the starting page, which is definitely not the case for the real web: Imagine four web pages, P_1, P_2, P_3, P_4, where P_1 is linked to P_2 and P_2 to P_1 and similarly, P_3 to P_4 and P_4 to P_3 and there are no other outlinks from $P_1, \dots, P_4$. If one starts at P_1 then the probability of ending at P_3 or P_4 is zero while the probability of ending at P_1 is $\frac{1}{2}$, as is the probability of ending at P_2. On the other hand if we start at P_3 then the probability of ending at P_1 or P_2 is zero and the probability of ending at P_3 is $\frac{1}{2}$, as is the probability of ending at P_4. One needs to make alterations to the actual link structure so that the probabilities are independent of the starting page. How this is done is explained below.

We begin by describing how a nonnegative integer vector is associated to each web page and to a query.

Definition 13.17 *By a* **text document** *we mean either a webp age or a query which contains words and phrases, some of which are common and therefore do not differentiate one document from another, for example, "the," "and," "or," "but." Others are* **key words** *which will be found in a fraction of the documents. All possible key words are ordered in some way, say lexicographically, and given a number consistent with this ordering from 1 to N, where N is the number of all possible key words. For a particular document D, we make a real N-vector, called the* **text vector** $\boldsymbol{t}(D)$*, by setting $\boldsymbol{t}_i(D) = 0$ if the i^{th} key word is not contained in the document and $\boldsymbol{t}_i(D) = 1$ if it is.*

Assume that there are n web pages, $P_1, \ldots, P_n$ and set $\boldsymbol{t}_j = \boldsymbol{t}(P_j)$. Now that we have associated a text vector with each web page, P_j, and each query, Q, we can compare them for common content. A good measure of commonality is the cosine of the angle between $\boldsymbol{t}_j$ and $\boldsymbol{t}(Q)$, the smaller the angle, hence the closer the cosine to one, the greater the common content. By choosing some value *tol*, the tolerance of the query, we can say that a web page $\boldsymbol{t}_j$ is relevant to the query Q if

$$\cos(\boldsymbol{t}_j, \boldsymbol{t}(Q)) = \frac{\boldsymbol{t}_j \cdot \boldsymbol{t}(Q)}{\parallel \boldsymbol{t}_j \parallel \quad \parallel \boldsymbol{t}(Q) \parallel} > tol.$$

When *tol* is decreased, more pages are defined as relevant, and when *tol* is increased, fewer are relevant. There are two important measures of search performance: precision and recall.

Definition 13.18 *The* **precision** *of a search is the quotient $P = \frac{D_r(Q)}{D_{tot}(Q)}$ where $D_r(Q)$ is the number of genuinely relevant documents that are retrieved and $D_{tot}(Q)$ is the total number of documents retrieved. The* **recall** *of the search is the quotient $R = \frac{D_r(Q)}{N_r(Q)}$ where N_r is the total number of relevant documents in the database.*

Remark 13.2 *When tol is large, one would expect precision to be high but recall lower, whereas when it tol is smaller, one might expect precision to be low and recall high. To actually determine this, for a particular database, requires human reading of documents and when this has been determined the precision and recall of the search engine can be tested against the pre-determined values.*

In addition to indicating that web page $\boldsymbol{t}_j$ is relevant to the query Q, the actual value of the cosine can be used to give $\boldsymbol{t}_j$ a content score which may be combined with a query independent popularity score to determine its overall score and ranking within all the relevant pages. We now turn to the question of how a popularity score can be assigned to a page.

Definition 13.19 *By a* **ranking vector** *for the web we will mean any non-negative real n-vector $\boldsymbol{r}$ such that $\parallel \boldsymbol{r} \parallel_1 = 1$ (here, n is the number of indexed webpages). Thus, $\boldsymbol{r}$ is a probability vector.*

Of course, one could sit in a closet and make up a ranking vector arbitrarily but this does not incorporate any information about how important or popular the web pages are relative to one another. A first pass at defining a ranking vector which takes into account importance and popularity begins with the assumption that a page with lots of links to it is probably more important/popular than a page with fewer links. This, however, is inadequate for at least two reasons: First, it is possible to exploit such a definition by creating lots of nonsense web pages (without meaningful content) which all link to a given page. Second, such a definition does not take into account whether the web pages linked to it are themselves important and popular. Before we get to how this is done, we introduce some additional definitions and terminology.

Definition 13.20 *For a web page P_j let O_j consist of all the web pages P_i such that there is a link from P_j to P_i. This is the set of* **outlinks** *from P_j. We also let I_j consist of all the webpages P_i such that there is a link from P_i to Pj. These are the* **inlinks** *to P_j. We set $n_j = |O_j|$, that is, the number of outlinks from P_j.*

In our next definition we show how to associate a vector with each webpage that captures information about links from the page.

Definition 13.21 *Assume P_j is a web page and O_j is empty, that is, there are no outlinks from P_j. Then set $\boldsymbol{s}_j = \mathbf{0}_n$. Otherwise, if O_j is not empty, let $\boldsymbol{s}_j = \begin{pmatrix} s_{1j} \\ \vdots \\ s_{nj} \end{pmatrix}$ where $s_{ij} = \frac{1}{n_j}$ if $P_i \in O_j$ and $s_{ij} = 0$ otherwise. This is the* **link vector** *of the web page P_j.*

With all these columns it is natural to consider making a matrix from them and we do.

Definition 13.22 *The* **link matrix** *of the web is the $n \times n$ matrix whose columns are $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n$.We denote this matrix by L.*

Remark 13.3 *The link matrix L is sparse, that is, most of its elements are zero.*

The link structure of the web can also be usefully represented by a directed graph, a concept we introduce now.

Definition 13.23 *A* **directed graph** *is a pair $\Gamma = (V, \Delta)$ where V is a set, whose elements are called* **vertices** *and Δ is a subset of the Cartesian product $V^2 = V \times V$ whose elements are called* **edges**. *One can think of a directed graph as a set of points together with arrows pointing from some vertices to other vertices.*

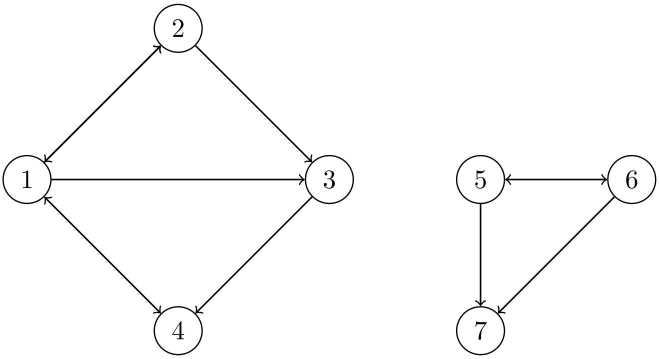

FIGURE 13.2
Directed graph on seven vertices.

Example 13.16 *An example of a directed graph on seven vertices with 11 edges is given in the Figure (13.2). Note between nodes 1 and 2, between 1 and 4, and between 5 and 6, there are arrows in both directions.*

Definition 13.24 *The* **link graph** *of the web is the graph whose vertex set is $\mathcal{S} = \{P_1, \ldots, P_n\}$ where (P_j, P_i) is an edge if there is a link* **from** P_j **to** P_i*. This is denoted by Λ.*

Now a natural way to define the ranking r_j of a webpage P_j is as a weighted sum of the all the inlinks to P_j. Thus, assume P_k has ranking r_k and is linked to P_j. We then distribute the ranking r_k equally among all the n_k outlinks from P_k. Thus, the link from P_k to P_j contributes $\frac{1}{n_k} r_k = s_{jk} r_k$. We therefore get the following recursive definition of r_j

$$r_j = \sum_{k \in I_j} \frac{1}{n_k} r_k = \sum_{k \in I_j} s_{jk} r_k. \tag{13.17}$$

If we set $\boldsymbol{r} = \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}$ then Equation (13.17) can be represented by the single matrix equation:

$$\boldsymbol{r} = L\boldsymbol{r}. \tag{13.18}$$

You should recognize from Equation (13.18) that $\boldsymbol{r}$, if it exists, is an eigenvector of L with eigenvalue one. It is natural to ask if $\boldsymbol{r}$ necessarily exists and, if it does, whether it is unique. If L did not have any zero columns it would be a column-stochastic matrix. We could then definitely conclude that it has a non-negative eigenvector with eigenvalue one by the weak form of the Perron–Frobenius theorem, Theorem (12.18), but not necessarily a unique one. We will therefore make some modifications to L that will guarantee the existence of a unique positive stationary vector $\boldsymbol{r}$ with $\parallel \boldsymbol{r} \parallel_1 = 1$. Before doing so we return to our web surfer whose journey through the web is nearly a Markov chain with transition matrix L.

As mentioned, the existence of zero columns means that L is not a stochastic matrix (which means that the surfer may get stranded at some web page depending on the initial page). In order to insure that this doesn't happen, we modify L by replacing each zero column with a column that assumes an equal probability of going to any of the n webpages. To be explicit, define $\delta_j = 0$ if $n_j \neq 0$ and $\delta_j = 1$ if $n_j = 0$ and set $\boldsymbol{d} = \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix}$. Also let $\boldsymbol{j} = \boldsymbol{j}_n$ be the all-one n-vector. We define the matrix $\widehat{L}$ as follows:

$$\widehat{L} = L + \frac{1}{n}\boldsymbol{j}\boldsymbol{d}^{tr}.$$

The matrix $\widehat{L}$ is a column-stochastic matrix, that is, every column $\boldsymbol{c}$ of $\widehat{L}$ is a probability vector: $\boldsymbol{c} \geq 0$ and $\parallel \boldsymbol{c} \parallel_1 = 1$. The matrix $\widehat{L}$ can be interpreted as follows: If P_j is a page with $n_j > 0$ outlinks, then the probability of going from P_j to P_i, with $P_i \in O_j$, is $\frac{1}{n_j}$. On the other hand, if the surfer should land at P_j with $n_j = 0$ then the surfer goes to a random page with probability $\frac{1}{n}$.

It now follows that $\widehat{L}^{tr}\boldsymbol{j} = \boldsymbol{j}$ so that one is a eigenvalue of $\widehat{L}^{tr}$ and therefore of $\widehat{L}$. This proves the existence of a ranking vector, however it may not be unique. This might occur if the matrix $\widehat{L}$ is reducible which we previously defined in Section (12.3). Recall, an $n \times n$ matrix A is reducible if there is a permutation matrix P such that

$$PAP^{tr} = PAP^{-1} = \begin{pmatrix} B & C \\ O_{k,n-k} & D \end{pmatrix}$$

where B is a $k \times k$ matrix, D is $(n-k) \times (n-k)$, and C is a $k \times (n-k)$ matrix. A matrix which is not reducible is irreducible.

Example 13.17 *The following matrix is reducible*

$$\begin{pmatrix} 0 & \frac{1}{2} & 0 & 1 & 0 & 0 & 0 \\ \frac{1}{3} & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{3} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{3} & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 \end{pmatrix}.$$

Note that the vectors $\begin{pmatrix} \frac{3}{8} \\ \frac{1}{8} \\ \frac{3}{16} \\ \frac{5}{16} \\ 0 \\ 0 \\ 0 \end{pmatrix}$ *and* $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \frac{2}{5} \\ \frac{2}{5} \\ \frac{1}{5} \end{pmatrix}$ *are eigenvectors with eigenvalue one.*
*This matrix represents the linked graph shown in Figure (**??**). Note that a surfer who lands on one of the webpages P_1, P_2, P_3, P_4 will just cycle among them and likewise for P_5, P_6, P_7.*

It is almost certainly the case that $\widehat{L}$ is reducible and therefore to insure irreducibility, we will modify $\widehat{L}$ to obtain a positive stochastic matrix (which is necessarily irreducible). This is referred to as the **primitivity adjustment**. The resulting matrix, known as a *Google matrix* will have a unique ranking vector: By Theorem (12.22), the spectral radius of a stochastic matrix is one, and by Theorem (12.19), if A is nonnegative and irreducible then $\rho(A)$ is a simple eigenvalue (in fact has algebraic multiplicity one) and there exists a positive eigenvector for this eigenvalue.

Let $J = \boldsymbol{j}\boldsymbol{j}^{tr}$ be the all-one matrix and set $K = \frac{1}{n}J$ which is a rank-one doubly stochastic matrix all of whose entries are $\frac{1}{n}$. Choose α with $0 < \alpha < 1$ and set $G_\alpha = \alpha\widehat{L} + (1-\alpha)K$. Clearly, this is a positive matrix (consequently irreducible) since it is the sum of the nonnegative matrix $\alpha\widehat{L}$ and the positive matrix $(1-\alpha)K$. We show in the next result that G_α is column stochastic.

Theorem 13.20 *If α is a real number and $0 < \alpha < 1$ then G_α is a stochastic matrix.*

Proof *Since $G_\alpha > 0$, we need only show that $G_\alpha^{tr}\boldsymbol{j} = \boldsymbol{j}$. Since $\widehat{L}$ and K are column-stochastic, we have*

$$\widehat{L}^{tr}\boldsymbol{j} = \boldsymbol{j} = K^{tr}\boldsymbol{j}.$$

It then follows that

$$\begin{aligned} G_\alpha^{tr}\boldsymbol{j} &= [\alpha\widehat{L} + (1-\alpha)K]^{tr}\boldsymbol{j} \\ &= [\alpha\widehat{L}^{tr} + (1-\alpha)K^{tr}]\boldsymbol{j} \\ &= \alpha\widehat{L}^{tr}\boldsymbol{j} + (1-\alpha)K^{tr}\boldsymbol{j} \\ &= \alpha\boldsymbol{j} + (1-\alpha)\boldsymbol{j} = \boldsymbol{j}. \end{aligned}$$

In terms of the web surfer, the primitivity adjustment can be interpreted as follows: The surfer follows the links of the web with probability α but acts randomly with probability $1-\alpha$ (jumping to an arbitrary page with equal probability). This is referred to by Brin and Page as "teleporting."

Each G_α is a *Google matrix*, though a particular value of α is used in practice, apparently α is about 0.85. The ranking vector is the probability vector $\boldsymbol{r}$ for which $G\boldsymbol{r} = \boldsymbol{r}$. This vector is not calculated directly, that is, by finding the one dimensional null space of the matrix $G - I_n$ using Gaussian elimination. This computation is too large. Rather $\boldsymbol{r}$ is approximated by choosing a probability vector $\boldsymbol{r}_0$ and then computing $\boldsymbol{r}_k = G^k\boldsymbol{r}_0$. A priori there is no certainty that this would converge. However, since G_α is a positive matrix we are guaranteed convergence by Theorem (12.21) from which we can conclude that

$$\lim_{k\to\infty} \boldsymbol{r}_k = \boldsymbol{r}.$$

This method of computing $\boldsymbol{r}$ is known as the power method, which is just one of many methods available for finding an eigenvector for the dominant eigenvalue of a matrix. This method is slow, perhaps the slowest for finding an eigenvector for the dominant eigenvalue. However, there are good reasons why it was chosen by Brin and Page. Among these are: it is simple, the multiplications of G_α can be reduced to multiplications on the sparse matrix L, and it uses a minimum of storage as contrasted with other methods. Finally, with $\alpha = 0.85$, $\boldsymbol{r}_k$ converges to $\boldsymbol{r}$ with between 50 and 100 iterations.

A good source for further investigation of this topic is ([14]).

Exercises

1. Write down the matrix L associated with the directed graph shown in Figure (13.3).

2. Explain why L is not a stochastic matrix.

3. Write down the matrix $\widehat{L}$ in order to obtain a stochastic matrix.

4. Explain why $\widehat{L}$ is reducible.

5. Determine the 1-eigenspace of $\widehat{L}$.

6. Write down the Google matrix, G, obtained from $\widehat{L}$ with $\alpha = \frac{3}{4}$.

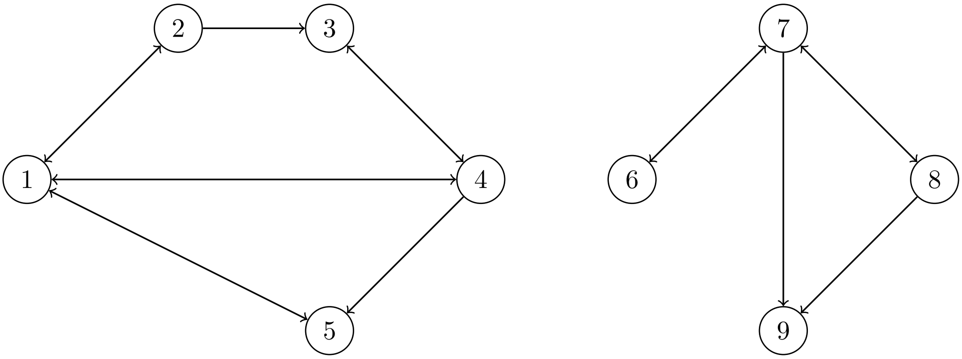

FIGURE 13.3
Directed graph on nine vertices.

Appendix A

Concepts from Topology and Analysis

In this appendix we give a brief introduction to concepts from analysis. Specifically we define the following: Metric space, topology and topological space, limit of a sequence in a topological space, Cauchy sequence in a metric space, compact subset of a topological space, continuous function between topological spaces, convex subset of $\mathbb{R}^n$. We also state two theorems which we use in Chapter 12: The Krein–Milman theorem and the Brouwer fixed point theorem. A proof of the former can be found in ([5]) and the latter in ([15]).

Definition A.1 *A* **metric space** *is a pair* (X, d) *consisting of a set* X *and a function* $d : X \times X \to \mathbb{R}_{\geq 0}$*, called a* **metric** *if the following are satisfied:*

(M1) For $x, y \in X, d(x, y) \geq 0$ *and* $d(x, y) = 0$ *if and only if* $x = y$*.*
(M2) $d(x, y) = d(y, x)$*.*
(M3) For $x, y, z \in X, d(x, z) \leq d(x, y) + d(y, z)$*. This is referred to as the* **triangle inequality***.*

Definition A.2 *Let* (X, d) *be a metric space,* $x \in X$ *and* r *a positive real number. The* **open ball of radius** r **centered at** x *is*

$$B_r(x) := \{y \in X | d(x, y) < r\}.$$

Metric spaces give rise to topological spaces, a concept we now define.

Definition A.3 *Let* X *be a set and* $\mathcal{T}$ *a collection of subsets of* X*. Then* $\mathcal{T}$ *is said to be a* **topology** *on* X*, and* $(X, \mathcal{T})$ *is a* **topological space***, if the following are satisfied:*

1. The empty set and X *are in* $\mathcal{T}$*.*
2. The union of an arbitrary subset of $\mathcal{T}$ *is contained in* $\mathcal{T}$*.*
3. The intersection of a finite subset of $\mathcal{T}$ *is contained in* $\mathcal{T}$*.*

The elements of $\mathcal{T}$ *are referred to as* **open subsets** *of* X*. A subset* C *of* X *is said to be* **closed** *if* $X \setminus C$ *is open.*

Definition A.4 *Let (X, d) be a metric space. We will say a subset U of X is* **open** *if for every $u \in U$ there exists a positive real number r such that $B_r(u) \subset U$. Note that, vacuously, the empty set is an open subset of X.*

In the following theorem we show that the set of such subsets of X is a topology on X.

Theorem A.1 *Let (X, d) be a metric space and set $\mathcal{T}$ equal to the collection of all open subsets of X. The $\mathcal{T}$ is a topology.*

Proof *Clearly $\emptyset, X \in \mathcal{T}$ as is the fact that the union of an arbitrary subset of $\mathcal{T}$ is contained in $\mathcal{T}$, so it only remains to show that the intersection of finitely many open subsets is open. Let $U_1, \dots, U_m$ be open sets. If $\cap_{i=1}^m U_i = \emptyset$ there is nothing to prove, so assume $u \in \cap_{i=1}^m U_i$. Since each U_i is open there exists a positive real number r_i such that $B_{r_i}(u) \subset U_i$. Set $r = min\{r_1, \dots, r_m\}$. Then $B_r(u) \subset B_{r_i}(u) \subset U_i$. Consequently, $B_r(u) \subset \cap_{i=1}^m U_i$.*

Definition A.5 *Let $(X, \mathcal{T})$ be a topological space and $\{x_k\}_{k=1}^\infty$ a sequence of elements from X and $x \in X$. We say that x is the* **limit of the sequence** *and write*

$$\lim_{k \to \infty} x_k = x$$

if whenever U is an open subset containing x, then there exists a natural number N (which may depend on U), such that $x_k \in U$ for all $k \geq N$.

When the topological space $(X, \mathcal{T})$ comes from a metric d on X the notion of limit can be formulated as follows: $\lim_{k \to \infty} x_k = x$ if for every positive real number r there is a natural number N such that $d(x_k, x) < r$ if $k \geq N$.

In would not be desirable if a sequence had two or more limits. This can happen in arbitrary topological spaces but not those that arise from a metric as we now show.

Theorem A.2 *Let (X, d) be a metric space and $\{x_k\}_{k=1}^\infty$. If $\lim_{k \to \infty} x_k$ exists then it is unique.*

Proof *Assume $\lim_{k \to \infty} x_k = x$ and $y \in X, y \neq x$. Let $s = d(x, y) > 0$ and set $r = \frac{s}{3}$. By assumption there is a natural number N such that if $k \geq N$ then $d(x, x_k) < r$. We then have by the triangle inequality*

$$3r = s = d(x, y) \leq d(x, x_k) + d(x_k, y) > r + d(x_k, y).$$

It follows that $d(x_k, y) > 2r$ and therefore $lim_{k \to \infty} x_k \neq y$. As y is arbitrary we can conclude that x is unique.

Definition A.6 *A sequence $\{x_k\}_{k=1}^{\infty}$ in a metric space (X, d) is a* **Cauchy sequence** *if for every positive real number r there is a natural number N (depending on r), such that if $k, l \geq N$ then $d(x_k, x_l) < r$.*

Definition A.7 *Assume $(X, \mathcal{T})$ is a topological space and C is a subset of X. An* **open cover** *of C is a subset $\mathcal{S}$ of $\mathcal{T}$ such that $C \subset \cup_{S \in \mathcal{S}} S$. A subset C of X is said to be* **compact** *if every open cover $\mathcal{S}$ of C contains a finite subcover.*

Definition A.8 *Assume (X_1, d_1) and (X_2, d_2) are metric spaces and $f : X_1 \to X_2$ is a function. We say that f is* **continuous** *at $x \in X_1$ if for each positive real number ϵ there exists a positive real number δ (depending on ϵ) such that if $d_1(x, y) < \delta$ then $d_2(f(x), f(y)) < \epsilon$. We say that f is* **continuous** *if it is continuous at x for every $x \in X_1$.*

The following is fairly easy to prove:

Theorem A.3 *Assume (X_1, d_1) and (X_2, d_2) are metric spaces and $f : X_1 \to X_2$ is a continuous function. If $C \subset X$ is compact then $f(C)$ is compact.*

We next introduce some concepts which we will need for our treatment of doubly stochastic matrices in Section (12.3).

Definition A.9 *Let C be a subset of $\mathbb{R}^n$. C is said to be* **convex** *if whenever $\boldsymbol{u}, \boldsymbol{v} \in C$ and $t \in \mathbb{R}$ satisfies $0 \leq t \leq 1$ then $t\boldsymbol{u} + (1-t)\boldsymbol{v} \in C$.*

To clarify the meaning of this definition: the set $\{t\boldsymbol{u} + (1-t)\boldsymbol{v} | 0 \leq t \leq 1\}$ is the line segment with endpoints $\boldsymbol{u}$ and $\boldsymbol{v}$. Thus, C is convex if whenever it contains points $\boldsymbol{u}$ and $\boldsymbol{v}$ then it contains the line segment with endpoints $\boldsymbol{u}$ and $\boldsymbol{v}$. We denote this by $[\boldsymbol{u}, \boldsymbol{v}]$. The ***interior*** of the line segment $[\boldsymbol{u}, \boldsymbol{v}]$, denoted by $(\boldsymbol{u}, \boldsymbol{v})$, is $\{t\boldsymbol{u} + (1-t)\boldsymbol{v} | 0 < t < 1\}$.

It is an easy consequence of the definition that the intersection of convex subsets is convex. This motivates the following definition.

Definition A.10 *Let X be a subset of $\mathbb{R}^n$. The* **convex hull** *of X is the intersection of all convex subsets of $\mathbb{R}^n$ which contain X. It is the unique minimal (with respect to inclusion) convex subset of $\mathbb{R}^n$ which contains X.*

Definition A.11 *Let C be a convex subset of $\mathbb{R}^n$. An* **extreme point** *of C is a point $\boldsymbol{x} \in C$ such that whenever $\boldsymbol{u}, \boldsymbol{v} \in C$ and $t \in \mathbb{R}, 0 < t < 1$ satisfy $\boldsymbol{x} = t\boldsymbol{u} + (1-t)\boldsymbol{v}$ then $\boldsymbol{u} = \boldsymbol{v}$. Thus, $\boldsymbol{x}$ is an extreme point if it is not on the interior of any line segment contained in C.*

We will cite the following result known as the Krein–Milman theorem:

Theorem A.4 *Let C be a compact convex subset of $\mathbb{R}^n$. Let $E(C)$ denote the extreme points of C. Then $E(C)$ is nonempty and F is the convex hull of $E(C)$.*

Finally, we will also need to cite the Brouwer fixed point theorem:

Theorem A.5 *Let C be a convex and compact subset of $\mathbb{R}^n$ (with respect to the metric defined by some norm on $\mathbb{R}^n$) and $f : C \rightarrow C$ be a continuous function. Then f has a fixed point, that is, there exists $\boldsymbol{x} \in C$ such that $f(\boldsymbol{x}) = \boldsymbol{x}$.*

Appendix B

Concepts from Group Theory

In this appendix we give a brief introduction to concepts from group theory. Specifically, we define the following: group, subgroup of a group, center of a group, normal subgroup of a group, simple group, commutator subgroup of a group, derived series of a group, solvable group, quotient group, homomorphism, kernel of a homomorphism, group action, transitive group action, primitive group action, doubly transitive group action, kernel of a group action, and a faithful group action. We also prove Iwasawa's theorem which is used extensively in Chapter 11.

Definition B.1 *A* **group** *consists of a nonempty set* G *together with a binary operation (function)* $\mu : G \times G \to G$*, denoted by* $\mu(x, y) = x \cdot y$ *or simply as* xy*, and an element* $e \in G$ *such that the following hold:*

1) The binary operation μ *is associative, that is, for all* $x, y, z \in G, (xy)z = x(yz)$*.*

2) For every $x \in G, ex = xe = x$*.*

3) For every $x \in G$ *there is an element* $y \in G$ *such that* $xy = yx = e$*.*

A group G *is said to be* **Abelian** *if it also satisfies*

4) For all elements $x, y \in G$*,* $xy = yx$*.*

Remark B.1 *The element* e *of a group* G *is unique, that is to say if* $f \in G$ *and* $xf = fx = x$ *for every* $x \in G$ *then* $f = e$*. This element is called the* **identity** *of* G*. Also, if* $x \in G$ *the element* $y \in G$ *such that* $xy = yx = e$ *is unique. We will denote it by* x^{-1} *and refer to it as the* **inverse** *of* x*.*

Definition B.2 *Let* X *be a set. Denote by* $S(X)$ *the set of all bijective functions* $\sigma : X \to X$*. For* $\sigma, \tau \in S(X)$ *let* $\sigma\tau$ *be the composition* $\sigma \circ \tau$*. Then* $S(X)$ *is a group. The identity element is the identity map* $I_X : X \to X$ *which is defined by* $I_X(x) = x$ *for all* $x \in X$*. The group* $S(X)$ *is referred to as the* **symmetric group** *on* X*. We refer to elements of* $S(X)$ *as permutations on* X*. When* $X = \{1, 2, \ldots, n\}$ *we denote* $S(X)$ *by* S_n*.*

Definition B.3 *Let (G, μ, e) be a group. A* **subgroup** *of G is a nonempty subset H of G such that*

1) if $x, y \in H$ then $xy \in H$, and

2) if $x \in H$ then $x^{-1} \in H$.

Remark B.2 *If H is a subgroup of a group G, then $e \in H$ where e is the identity of G. Also, setting $\mu_H = \mu$ restricted to $H \times H$, it is then the case that H is a group.*

The following is easy to prove:

Theorem B.1 *Let G be a group and assume $\{H_a | a \in A\}$ is a family of subgroups of G. Then $\cap_{a \in A} H_a$ is a subgroup of G.*

Definition B.4 *Let G be a group and X a subset of G. The* **subgroup of** *G* **generated by** *X, denoted by $\langle X \rangle$, is the intersection of all subgroups of G which contain X.*

Definition B.5 *Let G be a group, H a subgroup of G, and $g \in G$. The subset $gH := \{gh | h \in H\}$ is a* **left coset** *of H in G.*

Remark B.3 *The set of left cosets of H in G are the equivalence classes of the relation $\equiv_H$ given by $x \equiv_H y$ if and only if $x^{-1}y \in H$. We denote the set of left cosets of H in G by G/H and refer to it as the* **quotient set** *of G modulo H.*

Definition B.6 *Let X and Y be subsets of a group G. The product XY consists of all elements xy such that $x \in X$ and $y \in Y$.*

Definition B.7 *Let G be a group. Elements x and y in G are said to* **commute** *if $xy = yx$. Suppose H a subgroup. The* **centralizer** *of H in G, denoted by $C_G(H)$, is the subset of G consisting of all those elements which commute with every element of H, that is, $C_G(H) = \{g \in G | gh = hg \forall h \in G\}$.*

Remark B.4 *Let G be a group, H a subgroup of G. Then $C_G(H)$ is a subgroup of G.*

Definition B.8 *Let G be a group. The* **center** *of G, denoted by $Z(G)$ is given by*

$$Z(G) := \{z \in G | zx = xz \ \ \forall x \in G\} = C_G(G).$$

Definition B.9 *Let G be a group, H a subgroup of G, and $g \in G$. The* **g-conjugate** *of H is $g^{-1}Hg = \{g^{-1}hg | h \in H\}$. Note that $g^{-1}Hg$ is a subgroup of G. Any such subgroup obtained this way is said to be a conjugate of H.*

Definition B.10 *Let G be a group and H a subgroup of G. The* **normalizer** *of H in G , denoted by $N_G(H)$ is given by*

$$N_G(H) := \{g \in G | g^{-1}Hg = H\}.$$

Remark B.5 *Let G be a group and H a subgroup of G. Then $N_G(H)$ is a subgroup of G which contains H.*

Definition B.11 *Let G be a group. A subgroup N of G is* **normal** *if $N_G(N) = G$. Equivalently, for every $g \in G, g^{-1}Ng = N$, that is, the only conjugate of N is N. When N is normal in G we write $N \lhd G$.*

The following are fairly straightforward to prove and are covered in a first course in abstract algebra.

Theorem B.2 *Assume N is a normal subgroup of a group G and H is a subgroup of G. Then NH is a subgroup of G.*

Theorem B.3 *Assume N is a normal subgroup of a group G and H is a subgroup of G. Then $N \cap H$ is a normal subgroup of H.*

Theorem B.4 *Let G be a group and N a normal subgroup. For xN, yN left cosets of H define $(xN) \cdot (yN) = (xy)N$. This is well defined (independent of the representatives x and y) and G/N with this multiplication is a group.*

Definition B.12 *Let G be a group and N a normal subgroup. The quotient set G/N together with the multiplication given by $(xN) \cdot (yN) = (xy)N$ is the* **quotient group** *of G modulo N.*

Definition B.13 *A group G is* **simple** *if G has more than one element and the only normal subgroups of G are $\{e\}$ and G.*

Definition B.14 *Let G be a group and $g, h \in G$. The element $[g, h] := g^{-1}h^{-1}gh$ is the* **commutator** *of g and h. The* **commutator subgroup** *of G is the subgroup of G generated by the set of all commutators. The commutator subgroup of G is denoted by either G' or $D(G)$. A group G is* **perfect** *if $G = D(G)$.*

The following is proved in a first course in abstract algebra:

Theorem B.5 *Let G be a group. The commutator subgroup, $D(G)$, of G is a normal subgroup. The quotient group $G/D(G)$ is an Abelian group. If H is a subgroup of G and $D(G) \subset H$ then H is normal in G. Finally, if H is a normal subgroup of G then the quotient group G/H is Abelian if and only if $D(G) \subset H$.*

Definition B.15 *Let G be a group. Set $G^{(0)} = G$ and assume that $G^{(k)}$ has been defined for $k \in \mathbb{Z}_{\geq 0}$. Then $G^{(k+1)} = D(G^{(k)})$, the commutator subgroup of $G^{(k)}$. This is the* **derived series** *of G. The group G is said to be* **solvable** *if for some natural number $n, G^{(n)} = \{e\}$.*

Remark B.6 *For every $n \in \mathbb{N}, G^{(n)}$ is normal in G. Moreover, each of the quotient groups $G^{(n)}/G^{(n+1)}$ is Abelian.*

Definition B.16 *Assume G and H are groups. A function $f : G \to H$ is a* **homomorphism** *if $f(xy) = f(x)f(y)$ for every $x, y \in G$.*

Definition B.17 *Let G and H be groups and $f : G \to H$ a homomorphism. Then f is said to be an* **isomorphism of groups** *if f is bijective. When there exists an isomorphism from a group G to a group H, we say that G and H are* **isomorphic***.*

Just as there are isomorphism theorems for vector spaces, there are for groups as well. The following is used in the proof of Iwasawa's theorem.

Theorem B.6 *Assume N is a normal subgroup of the group G, H is a subgroup of G, and $G = NH$. Then G/N is isomorphic to $H/(N \cap H)$.*

Definition B.18 *Let $f : G \to H$ be a homomorphism of groups. The* **kernel** *of f is $Ker(f) := \{x \in G | f(x) = e_H\}$.*

The following is straightforward to prove:

Theorem B.7 *Let $f : G \to H$ be a homomorphism of groups. Then $Ker(f)$ is an normal subgroup of G.*

Definition B.19 *Let G be a group and X a set. By a left-action of G on X we mean a map $\nu : G \times X \to X$ which we will denote by $\nu(g, x) = g \cdot x$ which satisfies the following:*

1) If e is the identity of G then $e \cdot x = x$ for all $x \in X$.

2) For $g, h \in G$ and $x \in X, g \cdot (h \cdot x) = (gh) \cdot x$.

Remark B.7 *Assume $\nu : G \times X \to X$ defines a left action of G on X. For $g \in G$ let $\nu_g : X \to X$ be the function given by $\nu_g(x) = \nu(g, x) = g \cdot x$. The map $\nu_g : X \to X$ is bijective and so a permutation of X. Also it follows from the second property that $\nu_{gh} = \nu_g \circ \nu_h$ so that $\nu : G \to S(X)$ is a homomorphism of groups. Conversely, given a homomorphism $f : G \to S(X)$, define $\nu : G \times X \to X$ by $\nu(g, x) = f(g)(x)$. This defines a left action of G on X.*

Definition B.20 *Assume the group G acts on the set X and $x \in X$. The* **stabilizer** *of x in G, denoted by G_x, consists of all those $g \in G$ such that $g \cdot x = x$.*

Definition B.21 *Assume $\nu : G \times X \to X$ defines a left action of G on X. The* **kernel of the group action** *consists of the set of $g \in G$ such that $g \cdot x = x$ for all $x \in X$. Equivalently, the kernel of the action is the kernel of the homomorphism $g \to \nu_g$ from G to $S(X)$. The action is said to be* **faithful** *if the kernel is trivial, that is, it is equal to $\{e\}$.*

Definition B.22 *Assume $\nu : G \times X \to X$ defines a left action of G on X. Define a relation $\sim$ on X as follows: $x \sim y$ if there exists $g \in G$ such that $g \cdot x = y$. This is an equivalence relation. The equivalence class containing x is $G \cdot x = \{g \cdot x | g \in G\}$ and is referred to as the* **orbit** *of G acting on X or simply the* G**-orbit containing** *x.*

Remark B.8 *Since the orbits of G acting on X are equivalence classes of an equivalence relation on X they are a partition of X. Thus, every $x \in X$ belongs to one and only one orbit.*

Definition B.23 *Assume the group G acts on the set X. The action is* **transitive** *if there is a single orbit. Equivalently, for any $x, y \in G$ there exists a $g \in G$ such that $g \cdot x = y$.*

Definition B.24 *Assume the group G acts on the set X. A* **block of imprimitivity** *is a proper subset B of X that satisfies*

1) $1 < |B|$ *and*
2) if $g \in G$, then either $g \cdot B = B$ or $(g \cdot B) \cap B = \emptyset$.

An action of G on X is said to be **primitive** *if no block of imprimitivity exists and* **imprimitive** *otherwise.*

Definition B.25 *An action of a group G on a set X is said to be* **doubly transitive** *if for any pairs (x_1, x_2) and (y_1, y_2) from X with $x_1 \neq x_2$ and $y_1 \neq y_2$ there exists $g \in G$ such that $g \cdot x_1 = y_1, g \cdot x_2 = y_2$.*

The following is an important result:

Theorem B.8 *Assume an action of the group G on the set X is doubly transitive. Then the action is primitive.*

We will need the following result on primitive group actions for the proof of Iwasawa's theorem.

Theorem B.9 *Assume G acts primitively and faithfully on the set X. If $N \neq \{e\}$ is a normal subgroup then N is transitive on X.*

Proof *Since $N \neq \{e\}$ and the action is faithful there exists $x \in X$ and $g \in N$ such that $g \cdot x \neq x$. Set $B = N \cdot x := \{h \cdot x | h \in N\}$, that is, the N-orbit which contains x. We have just shown that $|B| > 1$. We will prove for any $\sigma \in G$ that either $\sigma \cdot B = B$ or $(\sigma \cdot B) \cap B = \emptyset$.*

Let $y \in B$ and $\sigma \in G$ and set $z = \sigma \cdot y$. Since $y \in B$, there is an $h \in N$ such that $y = h \cdot x$. Then $z = \sigma \cdot (h \cdot x) = (\sigma h) \cdot x$. Note that $\sigma h = \sigma h \sigma^{-1} \sigma$. If we set $h' = \sigma h \sigma^{-1}$ then h' is in N since N is normal in G. Thus, $z = (h' \sigma) \cdot x = h' \cdot (\sigma \cdot x) = h' \cdot y$. Thus, z is in $N \cdot y$. However, $y \in B = N \cdot x$ so that $N \cdot y = N \cdot x = B$. We can therefore conclude that $z \in N \cdot x = B$ as required.

We can now prove Iwasawa's theorem.

Theorem B.10 *Assume the group G acts faithfully and primitively on the set X, and that G is perfect. Let $x \in X$ and assume G_x contains a solvable normal subgroup A_x such that G is generated by the conjugates of $A_x, G = \langle gA_xg^{-1} | g \in G\rangle = \langle A_{g \cdot x} | g \in G\rangle$. Then G is a simple group.*

Proof *Let $N \neq \{e\}$ be a normal subgroup of G. We need to prove that $N = G$. Since the action is faithful and $N \lhd G$ and $N \neq \{e\}$, it follows that N is transitive on X. This implies for any $x \in X$ that $G = NG_x$. We next show that $G = NA_x$. Since G is generated by gA_xg^{-1} as g ranges over G, it suffices to prove that $gA_xg^{-1} \subset NA_x$. Let $a \in A_x$ be arbitrary. Since $G = NG_x$, there are elements $n \in N, h \in G_x$ such that $g = nh$. Then $gag^{-1} = (nh)a(nh)^{-1} = n[hah^{-1}]n^{-1}$. Since $A_x \lhd G_x$ and $h \in G_x, b = hah^{-1} \in A_x$. Now $nbn^{-1} = nbn^{-1}b^{-1}b$. The element $nbn^{-1}b^{-1} \in N(bnb^{-1}) = N$ since N is normal in G. Thus, $gag^{-1} = nbn^{-1} \in NA_x$ as required. Suppose to the contrary that $N \neq G$. Then G/N is a nontrivial group. However, $G/N = NA_x/N$ is isomorphic to $A_x/(N \cap A_x)$, a quotient of a solvable group, which is solvable. However, this contradicts the assumption that G is a perfect group.*

This page intentionally left blank

Appendix C

Answers to Selected Exercises

Section (1.1)

7. $x = 4$

8. $x = 2 + i$.

Section (1.2)

1. $\begin{pmatrix} 2i \\ -2+2i \\ 4-2i \end{pmatrix}$

2. $\begin{pmatrix} 2 \\ 6 \\ -4 \end{pmatrix}$

3. $\begin{pmatrix} -6i \\ 2i \\ 8i \end{pmatrix}$

4. $\begin{pmatrix} 1+3i \\ 2 \\ -1+i \end{pmatrix}$

5. $\begin{pmatrix} -3+2i \\ -2-i \\ 1 \end{pmatrix}$

6. $\begin{pmatrix} 1+2i \\ 3+i \\ 5 \end{pmatrix}$

7. $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$

8. $\begin{pmatrix} 4 \\ 1 \\ 1 \end{pmatrix}$

9. $\begin{pmatrix} 1 \\ 4 \\ 2 \end{pmatrix}$

10. $\begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix}$

11. $\boldsymbol{v} = \begin{pmatrix} 3-i \\ 3+i \end{pmatrix}$

12. $\boldsymbol{v} = \begin{pmatrix} 4 \\ 2 \end{pmatrix}$

Section (1.6)

10. a) 48 bases
10. b) 480 bases
10. c) $(p^2-1)(p^2-p)$ bases

Section (1.8)

1. b) $[1]_{\mathcal{F}} = \begin{pmatrix} -2 \\ 2 \\ 1 \end{pmatrix},$

$$[x]_{\mathcal{F}} = \begin{pmatrix} 3 \\ -2 \\ -1 \end{pmatrix},$$

$$[x^2]_{\mathcal{F}} = \begin{pmatrix} 2 \\ -1 \\ -1 \end{pmatrix}.$$

Section (2.2)

1. $nullity(T) = 3 = rank(T)$.

2. $Ker(T) = Span((x-a)(x-$

$b), x(x-a)(x-b))$. $rank(T) = 2 = nullity(T)$.

3. $Range(T) = Span(\begin{pmatrix}1\\1\\1\\1\end{pmatrix}, \begin{pmatrix}2\\3\\1\\2\end{pmatrix}, \begin{pmatrix}2\\1\\1\\2\end{pmatrix})$.

$Ker(T) = Span(-2+x-x^2)$. $rank(T) = 3, nullity(T) = 1$.

Section (2.4)

3. $\begin{pmatrix}0&1\\0&0\end{pmatrix}$ is an example of such a matrix. The operator $T(\begin{pmatrix}x\\y\end{pmatrix}) = \begin{pmatrix}y\\0\end{pmatrix}$ is an example of such an operator.

4. Lots of example, $(A,B) = \left(\begin{pmatrix}1&-1\\1&-1\end{pmatrix}, \begin{pmatrix}1&0\\1&0\end{pmatrix}\right)$ is one.

5. $\mathcal{M}_T(\mathcal{S},\mathcal{S}) = \begin{pmatrix}2&2&1\\1&1&0\\1&0&0\end{pmatrix}$

9. $\begin{pmatrix}4&-2&-1\\-5&3&2\\0&0&0\\2&-1&-1\end{pmatrix}$ is an example.

10. $\begin{pmatrix}2&-1&-2&0\\-1&0&1&0\\0&-1&1&0\end{pmatrix}$ is an example.

Section (2.6)

1. $\begin{pmatrix}4&5&2\\2&3&1\\-1&-1&-1\end{pmatrix}$

5. 168.

6. $2^5 3^3 13$.

Section (3.1)

1. x^2+1.

Section (3.2)

13. $\mathcal{M}_{I_{\mathbb{F}_{(n-1)}[x]}}(\mathcal{S},\mathcal{B}) =$

$$\begin{pmatrix}1&\alpha_1&\alpha_1^2&\dots&\alpha_1^{n-1}\\1&\alpha_2&\alpha_2^2&\dots&\alpha_2^{n-1}\\\vdots&\vdots&\vdots&\dots&\vdots\\1&\alpha_n&\alpha_n^2&\dots&\alpha_n^{n-1}\end{pmatrix}.$$

Section (4.1)

1. $T(\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix} = \begin{pmatrix}x_1\\x_2\\x_1+x_2\end{pmatrix}$.

3. x^3-2x^2-x+2.

4. x^3-2x^2-x+2.

8. There are four T-invariant subspaces: $\{\mathbf{0}\}, \mathbb{R}^3, Span(\begin{pmatrix}1\\1\\1\end{pmatrix})$, $Span(\begin{pmatrix}1\\0\\-1\end{pmatrix}, \begin{pmatrix}0\\1\\-1\end{pmatrix})$

9. The T-invariant subspaces are $\{\mathbf{0}\}, Span(\begin{pmatrix}1\\0\\0\end{pmatrix}), Span(\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix})$, and $\mathbb{R}^3$.

Section (4.2)

1. a) $\mu_{T,\boldsymbol{z}}(x) = x^3-2x^2+x-2$. Since $deg(\mu_{T,\boldsymbol{z}}(x) = 3$ it follows that $\langle T,\boldsymbol{z}\rangle = \mathbb{R}^3$.
b) $\mu_{T,\boldsymbol{u}}(x) = x-2$.

2. $\mu_{T,\boldsymbol{z}}(x) = x^4+5x^2+4 = (x^2+1)(x^2+4)$. Since $deg(\mu_{T,\boldsymbol{z}})(x) = 4$ it follows that $\langle T,\boldsymbol{z}\rangle = \mathbb{R}^4$.

4. Lots of operators work. One example is $T(\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}) = \begin{pmatrix}x_1\\2x_2\\3x_3\\4x_4\end{pmatrix}$.

6. Let T have matrix $\begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}$ with respect to the standard basis.

7. Let T have matrix $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ with respect to the standard basis.

9. Let T have matrix $\begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$ with respect to the standard basis.

10. Let T have matrix $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$ with respect to the standard basis.

11. Let T have matrix $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}$ with respect to the standard basis.

Section (4.3)

1. a) $\mu_{T,\boldsymbol{e}_1}(x) = x^2 + 2x + 2$,
$\mu_{T,\boldsymbol{e}_2}(x) = x^3 - 2x - 4$,
$\mu_{T,\boldsymbol{e}_3}(x) = x^3 - 2x - 4$.
b) $\mu_T(x) = x^3 - 2x - 4$.
c) $\boldsymbol{e}_2, \boldsymbol{e}_3$ are maximal vectors.

2. $\mu_T(x) = x^2+2x+2 = x^2-3x-3 = (x-1)(x-2)$. Each of $\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3$ is a maximal vector.

3. $\mu_T(x) = x^4 - x^3 - x^2 - x - 2 =$

$$(x-2)(x^3 + x^2 + x + 1) =$$

$$(x-2)(x+1)(x^2+1).$$

$\boldsymbol{e}_1$ is a maximal vector.

Section (4.4)

1. This operator has minimal polynomial $(x+1)^2$ and so is not cyclic. Therefore it is decomposable.

2. This operator has minimal polynomial $(x+1)^3$ and is indecomposable.

3. This operator has minimal polynomial $(x-2)^3$ and is indecomposable.

Section (4.5)

1. $(d_1, \ldots, d_5) = (12, 22, 28, 34, 38)$.

2. The invariant factors, $d_i(x)$ ordered so $d_i(x) \mid d_{i+1}(x)$ are
$d_1(x) = (x^2 - x + 1)^2(x^2+1)$,
$d_2(x) = (x^2 - x + 1)^2(x^2+1)^2(x+2)$,
$d_3(x) = (x^2 - x + 1)^3(x^2+1)^2(x+2)^2$,
$d_4(x) = (x^2 - x + 1)^4(x^2+1)^3 * x+2)^2$.
$dim(V) = 44$.

3. The elementary divisors are x^2+1 and x^2+1. These are also the invariant factors.

4. There is a single elementary divisor (invariant factor), which is $(x^2+1)^2$.

5. The elementary divisors are $x^2+1, x+1$ and $x-1$. There is a single invariant factor, x^4-1.

6. The elementary divisors are $x, x, x-1, x-1$. The invariant factors are $x^2 - x, x^2 - x$.

Section (4.6)

2. $\begin{pmatrix} 0 & -4 \\ 1 & 4 \end{pmatrix}$

3. $\begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -2 \\ 0 & 1 & -2 \end{pmatrix}$

4. $\begin{pmatrix} 3 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 1 & -2 \end{pmatrix}$

5. $\begin{pmatrix} 2 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & 2 \end{pmatrix}$

6. $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$

$$\begin{pmatrix}1&0&0&0\\1&1&0&0\\0&0&1&0\\0&0&1&1\end{pmatrix},\begin{pmatrix}1&0&0&0\\1&1&0&0\\0&1&1&0\\0&0&1&1\end{pmatrix}$$

8. $0_{44}, \begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&1&0\end{pmatrix},\begin{pmatrix}0&0&0&0\\1&0&0&0\\0&0&0&0\\0&0&1&0\end{pmatrix}$

$$\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&1&0&0\\0&0&1&0\end{pmatrix},\begin{pmatrix}0&0&0&0\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{pmatrix}$$

12. $\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&1&0\\0&0&1&1\end{pmatrix}$

Section (4.7)

3. The minimal polynomial if $\mu_T(x) = (x-1)(x^3-1)$. The characteristic polynomial is $(x-1)(x^3-1)^2$.

The invariant factors are
$(x-1)(x^3-1)$ and x^3-1.

The elementary divisors are
$x-1, (x-1)^2, x^2+x+1, x^2+x+1$.

4. $\begin{pmatrix}1&0&0&0&0&0&0\\0&1&0&0&0&0&0\\0&1&1&0&0&0&0\\0&0&0&0&-1&0&0\\0&0&0&1&-1&0&0\\0&0&0&0&0&0&-1\\0&0&0&0&0&1&-1\end{pmatrix}$

5. Set $\omega = -\frac{1}{2}+i\frac{\sqrt{3}}{2}$ and $\omega^2 = \frac{1}{\omega} = -\frac{1}{2}-i\frac{\sqrt{3}}{2}$. Then the Jordan canonical form of T over the complex numbers is

$$\begin{pmatrix}1&0&0&0&0&0&0\\0&1&0&0&0&0&0\\0&1&1&0&0&0&0\\0&0&0&\omega&0&0&0\\0&0&0&0&\omega&0&0\\0&0&0&0&0&\omega^2&0\\0&0&0&0&0&0&\omega^2\end{pmatrix}.$$

7. There are eight possibilities. They are

$J_2(0)\oplus J_3(-2i)\oplus J_1(0)\oplus J_1(0)\oplus J_1(0)$

$J_2(0)\oplus J_3(-2i)\oplus J_1(0)\oplus J_2(0))$

$J_2(0)\oplus J_3(-2i)\oplus J_1(0)\oplus$
$J_1(0)\oplus J_1(-2i)$

$J_2(0)\oplus J_3(-2i)\oplus J_2(0)\oplus J_1(-2i)$

$J_2(0)\oplus J_3(-2i)\oplus J_1(0)\oplus J_2(-2i)$

$J_2(0)\oplus J_3(-2i)\oplus J_1(-2i)\oplus$
$J_1(-2i)\oplus J_1(-2i)$

$J_2(0)\oplus J_3(-2i)\oplus J_1(-2i)\oplus J_2(-2i)$

$J_2(0)\oplus J_3(-2i)\oplus J_3(-2i)$

9. $\begin{pmatrix}-2&0&0&0\\1&-2&0&0\\0&0&2&0\\0&0&1&2\end{pmatrix}$

Section (5.2)

4. $(x^2+x+1)^{\perp} =$
$Span(\frac{110}{47}x^2-1, \frac{65}{47}x-1)$.

5. $d(A,B) = 5\sqrt{2}$.

8. $d(x^2,x) = \frac{\sqrt{30}}{30}$.

13. The angle is $\frac{\pi}{4}$.

Section (5.3)

11. Applying Gram–Schmidt we get the following orthogonal basis:

$$\begin{pmatrix}1&-1\\0&0\end{pmatrix},$$

$$\begin{pmatrix}\frac{1}{2}&\frac{1}{2}\\-1&0\end{pmatrix},$$

$$\begin{pmatrix} \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & -1 \end{pmatrix}.$$

The first matrix has norm $\sqrt{3}$, the second has norm $\sqrt{\frac{3}{2}}$, and the last has norm $\sqrt{\frac{4}{3}}$. Dividing the respective vectors by these numbers gives an orthonormal basis.

Section (5.4)

1. $Proj_W(\boldsymbol{u}) = \begin{pmatrix} 2 \\ 3 \\ 2 \\ 3 \end{pmatrix}$,

$Proj_{W^\perp}(\boldsymbol{u}) = \begin{pmatrix} -1 \\ -1 \\ 1 \\ 1 \end{pmatrix}$.

2. $Proj_W(J_2) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$,

$Proj_{W^\perp}(J_2) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

3. $Proj_W(x^3) = \frac{3}{2}x^3 - \frac{3}{5}x + \frac{1}{20}$.

4. $\frac{5}{3}$.

5. $\frac{2\sqrt{15}}{5}$.

6. $\frac{\sqrt{266}}{7}$.

7. $\frac{1}{35}(-244x^2 + 1248x - 194)$.

Section (5.5)

1. Set

$$g_1 = -5f_1 + 3f_2 + f_4$$

$$g_2 = -f_1 + f_2 - f_3$$

$$g_3 = -2f_1 + f_2 + f_4$$

$$g_4 = 5f_1 - 3f_2 + f_3 - f_4$$

Then (g_1, g_2, g_3, g_4) is the basis of $(\mathbb{R}^4)'$ which is dual to $\mathcal{B}$.

Section (5.6)

1. $\begin{pmatrix} 2 \\ 3 \\ -1 \end{pmatrix}$

2. $-420x^2 + 396x - 60$.

3. $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Section (5.7)

1.a) $\| \begin{pmatrix} -4 \\ 2 \\ -1 \\ -2 \end{pmatrix} \|_1 = 9$,

$\| \begin{pmatrix} -4 \\ 2 \\ -1 \\ -2 \end{pmatrix} \|_2 = 5$,

$\| \begin{pmatrix} -4 \\ 2 \\ -1 \\ -2 \end{pmatrix} \|_\infty = 4$.

b) $\| \begin{pmatrix} 3 \\ -6 \\ 0 \\ 2 \end{pmatrix} \|_1 = 11$,

$\| \begin{pmatrix} 3 \\ -6 \\ 0 \\ 2 \end{pmatrix} \|_2 = 7$,

$\| \begin{pmatrix} 3 \\ -6 \\ 0 \\ 2 \end{pmatrix} \|_\infty = 6$.

If $\boldsymbol{x} = \begin{pmatrix} -4 \\ 2 \\ -1 \\ -2 \end{pmatrix}$ and

$\boldsymbol{y} = \begin{pmatrix} 3 \\ -6 \\ 0 \\ 2 \end{pmatrix}$ then

$d_1(\boldsymbol{x}, \boldsymbol{y}) = 16, d_2(\boldsymbol{x}, \boldsymbol{y}) = \sqrt{114}$,

and $d_\infty(\boldsymbol{x}, \boldsymbol{y}) = 8$.

Section (6.2)

3. $\overline{\begin{pmatrix} 4 & -i \\ i & 4 \end{pmatrix}}^{tr} = \begin{pmatrix} 4 & i \\ -i & 4 \end{pmatrix}^{tr} = \begin{pmatrix} 4 & -i \\ i & 4 \end{pmatrix}$. Thus, $T^* = T$.

With respect to the orthonormal basis $\left(\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix}, \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-i}{\sqrt{2}} \end{pmatrix} \right)$ the matrix of T is $\begin{pmatrix} 5 & 0 \\ 0 & 3 \end{pmatrix}$.

4. $(\frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{6}} \begin{pmatrix} 1 \\ 1 \\ -2 \end{pmatrix})$.

Section (6.3)

1. Let $\mathcal{S}_4$ be the standard basis of $\mathbb{R}^4$. Let T be the operator on $\mathbb{R}^4$ such that

$$\mathcal{M}_T(\mathcal{S}_4, \mathcal{S}_4) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & -2 & 0 \end{pmatrix}.$$

2. Let T be the operator on $\mathbb{R}^4$ such that

$$\mathcal{M}_T(\mathcal{S}_4, \mathcal{S}_4) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}.$$

11. $dim(C(T)) = 8$.

Section (6.5)

14. Let S and T be defined on $\mathbb{R}^2$ be defined as multiplication by the following matrices, respectively:

$$\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 3 & -1 \\ -1 & 3 \end{pmatrix}.$$

16. Since T is not invertible, S is not unique. One solution is

$$\begin{pmatrix} \frac{1}{3} & \frac{-\sqrt{3}-1}{3} & \frac{-\sqrt{3}+1}{3} \\ \frac{\sqrt{3}-1}{3} & \frac{1}{3} & \frac{-\sqrt{3}-1}{3} \\ \frac{\sqrt{3}+1}{3} & \frac{\sqrt{3}+1}{3} & \frac{1}{3} \end{pmatrix}.$$

Section (7.2)

18. The minimum is $n-1$. There can't be fewer than $n-1$, for otherwise there will be at least two rows of all 1's and then the determinant is zero. On the other hand, the matrix

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & 0 & \dots & 1 \\ \vdots & \vdots & \dots & \vdots \\ 1 & 1 & \dots & 0 \end{pmatrix}$$

has non-zero determinant as can be seen by subtracting the first row from all the other rows. The resulting matrix is

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & -1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & -1 \end{pmatrix}.$$

This matrix has determinant $(-1)^{n-1}$.

Section (8.1)

6. Let $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Set $V = \mathbb{F}^2$ and define $f : V \times V \to$

$\mathbb{F}$ by $f(\boldsymbol{v}, \boldsymbol{w}) = \boldsymbol{v}^{tr} A \boldsymbol{w}$. Then $Rad_L(f) = \left\{ \begin{pmatrix} 0 \\ a \end{pmatrix} | a \in \mathbb{F} \right\}$ and $Rad_R(f) = \left\{ \begin{pmatrix} b \\ 0 \end{pmatrix} | b \in \mathbb{F} \right\}$.

7. Let $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. Set $V = \mathbb{F}^3$ and define $f : V \times V \to \mathbb{F}$ by $f(\boldsymbol{v}, \boldsymbol{w}) = \boldsymbol{v}^{tr} A \boldsymbol{w}$. Then $Rad_R(f) = Rad_L(f) = Span(\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix})$. However,

$$f(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}) = 0$$

$$f(\begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}) = 1.$$

8. Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Set $V = \mathbb{F}^2$ and define $f : V \times V \to \mathbb{F}$ by $f(\boldsymbol{v}, \boldsymbol{w}) = \boldsymbol{v}^{tr} A \boldsymbol{w}$. Then

$$f(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix}) = 0$$

$$f(\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}) = 1.$$

Section (8.2)

9. The number of such pairs is $q^{2n-1}(q^{2n} - 1)$.

Section (8.5)

1. $(\pi, \sigma) = (1, 0)$.

2. $(\pi, \sigma) = (2, 1)$.

3. $(\begin{pmatrix} -\frac{1}{2} \\ \frac{1}{2} \\ 0 \end{pmatrix} \begin{pmatrix} -1 \\ -1 \\ 2 \end{pmatrix}, \begin{pmatrix} \frac{1}{3} \\ \frac{1}{3} \\ \frac{1}{3} \end{pmatrix})$.

4. $(\begin{pmatrix} \frac{1}{3} \\ \frac{2}{3} \\ \frac{2}{3} \end{pmatrix}, \begin{pmatrix} -\frac{2}{3} \\ -\frac{1}{3} \\ \frac{2}{3} \end{pmatrix}, \begin{pmatrix} \frac{2}{3} \\ -\frac{2}{3} \\ \frac{1}{3} \end{pmatrix})$

5. The number of congruence classes is equal to the number of triples $(\pi, \nu, \zeta) \in \mathbb{N}^3$ such that $\pi + \nu + \zeta = n$. This is $\binom{n+1}{2}$.

Section (10.2)

7. For any cyclic diagonalizable operator $S : V \to V$, the operator $S \otimes S : V \otimes V \to V \otimes V$ will not be cyclic. For example, let $S : \mathbb{R}^2 \to \mathbb{R}^2$ be given by multiplication by $A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$. Then

$$A \otimes A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}.$$

So, the eigenvalue 2 occurs with algebraic multiplicity 2 and the operator is not cyclic.

Section (10.3)

5. The eigenvalues are 8, 27, 125 (with multiplicity 1) 12, 20, 18, 50, 45, 75 (with multiplicity 3) and 30 (with multiplicity 6).

6. Let $S(\boldsymbol{v}_1) = 2\boldsymbol{v}_1, S(\boldsymbol{v}_2) = 3\boldsymbol{v}_2$. Then $\boldsymbol{v}_1 \otimes \boldsymbol{v}_2, \boldsymbol{v}_2 \otimes \boldsymbol{v}_1$ are both eigenvectors of $\mathcal{T}_2(S)$ with eigenvalue 6. Thus, $\mathcal{T}_2(S)$ is not cyclic.

Section (10.4)

4. The eigenvalues are 1, 2, 8, 16 with multiplicity 1 and 4 with multiplicity 2. This operator is not cyclic.

5. $a_3^2 - a_2$.

Section (10.5)

9. Let $S : \mathbb{R}^4 \to \mathbb{R}^4$ be the operator with matrix $\begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 3 & 4 \\ 0 & 0 & -3 & 4 \end{pmatrix}$.

Then the eigenvalues of S are $\pm i, 3 \pm 4i$. On the other hand, the eigenvalues of $\wedge^2(S)$ are $1, 25, -4+3i, 4+3i, -4-3i, 4-3i$.

14. $x^6 + 14x^4 + 96x^3 - 128x - 32$.

15. $x^3 + 6x^2 - 9$.

16. $x^6 - 3x^4 - 27x^3 - 9x^2 + 27$.

Section (11.1)

1.

$$|GL(V)| = q^{\binom{n}{2}} \prod_{i=1}^{n} (q^i - 1)$$

$$|SL(V)| = q^{\binom{n}{2}} \prod_{i=2}^{n} (q^i - 1).$$

Section (12.1)

3.

$$\| A \|_F = \sqrt{193}$$

$$\| A \|_{1,1} = 14$$

$$\| A \|_{\infty,\infty} = 19$$

$$\| A \|_{2,2} = 14.$$

4.

$$\| A \|_F = \sqrt{33}$$

$$\| A \|_{1,1} = \| A \|_{\infty,\infty} = 5$$

$$\| A \|_{2,2} = 5.$$

Section (13.1)

4. $\begin{pmatrix} \frac{31}{4} \\ \frac{15}{4} \end{pmatrix}$

5. $\begin{pmatrix} -7 \\ \frac{9}{2} \end{pmatrix}$

6. $\begin{pmatrix} 20 \\ -16 \end{pmatrix}$

7. $\begin{pmatrix} \frac{3}{2} \\ -\frac{5}{4} \\ \frac{5}{4} \end{pmatrix}$

8. The general least square solution consists of all vectors $\boldsymbol{z} + \boldsymbol{y}$ where $\boldsymbol{z} = \begin{pmatrix} -\frac{1}{10} \\ -\frac{11}{2} \\ \frac{7}{2} \end{pmatrix}$ and $\boldsymbol{y} \in Span(\begin{pmatrix} 2 \\ -1 \\ -1 \end{pmatrix}$.

9. The general least square solution consists of all vectors $\boldsymbol{z}+\boldsymbol{y}$ where $\boldsymbol{z} = \begin{pmatrix} \frac{3}{5} \\ 1 \\ \frac{2}{5} \\ \frac{1}{5} \end{pmatrix}$ and $\boldsymbol{y} \in Span(\begin{pmatrix} 1 \\ 1 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 0 \\ 2 \end{pmatrix})$.

10. $\begin{pmatrix} -\frac{13}{3} \\ \frac{5}{3} \end{pmatrix}$.

11. $\begin{pmatrix} 3 \\ 1 \\ -2 \end{pmatrix}$.

12. $y = 2.06 + 3.01x$.

14. $y = 2.92 - 1.88x + 1.20x^2$.

16. $y = .35e^{1.55t}$.

Section (13.3)

1. The matrix is $\begin{pmatrix} A & \mathbf{0}_{5\times 4} \\ \mathbf{0}_{4\times 5} & B \end{pmatrix}$

where $A = \begin{pmatrix} 0 & \frac{1}{2} & 0 & \frac{1}{2} & 1 \\ \frac{1}{3} & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 & 0 \\ \frac{1}{3} & 0 & 1 & 0 & 0 \\ \frac{1}{3} & 0 & 0 & \frac{1}{2} & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & \frac{1}{3} & 0 & 0 \\ 1 & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{3} & 0 & 0 \\ 0 & \frac{1}{3} & \frac{1}{2} & 0 \end{pmatrix}$.

2. The last column is a zero column and therefore its entries do not add up to 1.

3. $\widehat{L} = \begin{pmatrix} A & \mathbf{0}_{5\times 3} & \frac{1}{9}\boldsymbol{j}_5 \\ \mathbf{0}_{4\times 5} & B' & \frac{1}{9}\boldsymbol{j}_4 \end{pmatrix}$. where $\boldsymbol{j}_5$ is the all one 5-vector, $\boldsymbol{j}_4$ is the all one 4-vector and $B' = \begin{pmatrix} 0 & \frac{1}{3} & 0 \\ 1 & 0 & \frac{1}{2} \\ 0 & \frac{1}{3} & 0 \\ 0 & \frac{1}{3} & \frac{1}{2} \end{pmatrix}$.

4. Since $Span(\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3, \boldsymbol{e}_4, \boldsymbol{e}_5)$ is invariant the matrix is reducible.

5. $Span(\begin{pmatrix} \frac{12}{31} \\ \frac{4}{31} \\ \frac{2}{31} \\ \frac{6}{31} \\ \frac{7}{31} \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix})$.

6.

$$\begin{pmatrix}
\frac{1}{36} & \frac{29}{72} & \frac{1}{36} & \frac{10}{36} & \frac{28}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{9} \\
\frac{10}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{9} \\
\frac{1}{36} & \frac{29}{72} & \frac{1}{36} & \frac{29}{72} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{9} \\
\frac{10}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{9} \\
\frac{10}{36} & \frac{1}{36} & \frac{1}{36} & \frac{29}{72} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{9} \\
\frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{10}{36} & \frac{1}{36} & \frac{1}{9} \\
\frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{7}{9} & \frac{1}{36} & \frac{29}{72} & \frac{1}{9} \\
\frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{10}{36} & \frac{1}{36} & \frac{1}{9} \\
\frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{1}{36} & \frac{10}{36} & \frac{29}{72} & \frac{1}{9}
\end{pmatrix}$$

This page intentionally left blank

Appendix D

Hints to Selected Problems

Section (1.3)

1. Use the fact that $\mathbf{0} = \mathbf{0} + \mathbf{0}$ and the distributive property.

2. Multiply by c^{-1} and use $c^{-1}(c\boldsymbol{u}) = (c^{-1}c)\boldsymbol{u}$.

Section (1.4)

6. Choose $\boldsymbol{u} \in U \setminus W$ and $\boldsymbol{w} \in W \setminus U$ and prove that $\boldsymbol{u} + \boldsymbol{w} \notin U \cup W$.

Section (1.5)

11. Assume you have a non-trivial dependence relation $\sum_{i=1}^{k} a_i\boldsymbol{u}_i + \sum_{j=1}^{l} b_i\boldsymbol{v}_i$. Then show that $\sum_{i=1}^{k} a_i\boldsymbol{u}_i \in U \cap W$ to get a contradiction. Conversely, assume $\boldsymbol{x} \in U \cap W, \boldsymbol{x} \neq \mathbf{0}$. Express is a linear combination of $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$ and $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_l)$. Set them equal and get a non-trivial dependence relation.

Section (1.6)

3. To prove independent start with a dependence relation $c_1\boldsymbol{u}_1 + c_2\boldsymbol{u}_2 + d_1\boldsymbol{v}_1 + d_2\boldsymbol{v}_2 + d_3\boldsymbol{v}_3 = \mathbf{0}$ and show if it is not trivial then $U \cap W \neq \{\mathbf{0}\}$. contrary to assumption. Alternatively, use Exercise 11 of Section (1.5).

6. Set $dim(U) = m, dim(W) = n$ and $dim(U \cap W) = l$. Start with a basis $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_l)$ of $U \cap W$ and extend to bases $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_l, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_{m-l})$ of U and $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_l, \boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n-l})$ for W and show that $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_l, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_{m-l}, \boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n-l})$ is a basis of $U + W$.

7. Use Exercise 6.

8. Use Exercise 6.

13. Suppose there exists a subspace U of V such that $X \cap U = Y \cap U = \{\mathbf{0}\}$ such that $X \oplus U = Y \oplus U = X + Y$. Take a complement, W, to $X + Y$ in V and set $Z = U + W$. To prove U exists let $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_j)$ be a basis of $X \cap Y$. Let $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_l)$ be a sequence from X such that $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_j, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_l)$ is a basis of X and a sequence $(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_l)$ from Y such that $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_j, \boldsymbol{y}_1, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_l)$ is a basis of Y. Set $\boldsymbol{u}_i = \boldsymbol{x}_i + \boldsymbol{y}_i$ and $U = Span(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_l)$.

Section (1.7)

4. Let $\mathcal{B}$ be a basis of V and let X be a subset of $\mathcal{B}$ with n elements. Set $U = Span(\mathcal{B} \setminus X)$.

Section (1.8)

3b. Set $F(x) = g(x) - g(0)f_1(x) - g(1)f_2(x) - g(2)f_3(x) - g(3)f_4(x)$ an element of $\mathbb{R}_3[x]$. Prove that F is zero at 0,1,2,3 and then conclude that $F(x)$ must be the zero polynomial.

5. Use Theorem (1.29).

6. Use Exercise 5 and Theorem (1.23).

Section (2.1)

10. Let $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ be a basis for V. Apply the exchange theorem to $(T(\boldsymbol{v}_1), \dots, T(\boldsymbol{v}_n))$.

12. Choose $\boldsymbol{v}_j \in V$ such that $T(\boldsymbol{v}_j) = \boldsymbol{w}_j$. Show that an arbitrary vector in W is an image of a vector in $Span(\boldsymbol{v}_1, \dots, \boldsymbol{v}_m)$.

13. If $\boldsymbol{w} = T(\boldsymbol{v})$ write $\boldsymbol{v}$ as a linear combination of $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ and then show that $\boldsymbol{w} = T(\boldsymbol{v})$ is a linear combination of $(T(\boldsymbol{v}_1), \dots, T(\boldsymbol{v}_n))$.

15. Let $\mathcal{X}$ consist of all pairs $(Span(\mathcal{A}), \phi)$ where $\mathcal{A} \subset \mathcal{B}, \phi$ is a linear transformation from $Span(\mathcal{A})$ to W, and ϕ restricted to $\mathcal{A}$ is equal to f restricted to $\mathcal{A}$. Order $\mathcal{X}$ as follows: $(\mathcal{A}, \phi) \leq (\mathcal{A}', \phi')$ if and only if $\mathcal{A} \subset \mathcal{A}'$ and ϕ' restricted to $Span(\mathcal{A})$ is equal to ϕ. Prove that every chain has an upper bound. By Zorn's lemma, there are maximal elements. Prove that a maximal element is a linear transformation from V to W which extends f.

16. Start with a dependence relation $c_1\boldsymbol{v}_1 + \cdots + c_k\boldsymbol{v}_k = \mathbf{0}_V$ and apply T. Use the properties of a linear transformation to get a dependence relation on $(\boldsymbol{w}_1, \dots, \boldsymbol{w}_k)$ and use this to show that $c_1 = \cdots = c_k = 0$.

Section (2.2)

10. Let $\mathcal{B}_V = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ be a basis of V and set $\boldsymbol{w}_j = T(\boldsymbol{v}_j)$. Prove that $(\boldsymbol{w}_1, \dots, \boldsymbol{w}_n)$ is a basis for W. Let S be the unique linear transformation from W to V such that $S(\boldsymbol{w}_j) = \boldsymbol{v}_j$. Prove that $S = T^{-1}$.

11. Let $\mathcal{B}_V = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ be a basis for V and $\mathcal{B}_W = (\boldsymbol{w}_1, \dots, \boldsymbol{w}_m)$ be a basis of W. Apply the Exchange Theorem to $(T(\boldsymbol{v}_1), \dots, T(\boldsymbol{v}_n))$.

12. Use the Exchange Theorem.

13. Let $\mathcal{B}_W = (\boldsymbol{w}_1, \dots, \boldsymbol{w}_m)$ be a basis for W. Choose $\boldsymbol{v}_j \in V$ such that $T(\boldsymbol{v}_j) = \boldsymbol{w}_j$ and let $S : W \to V$ be the linear transformation such that $S(\boldsymbol{w}_j) = \boldsymbol{v}_j$.

14. Let $\mathcal{B}_V = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ be a basis of V. Prove that $(T(\boldsymbol{v}_1), \dots, T(\boldsymbol{v}_n))$ can be extended to a basis $(\boldsymbol{w}_1, \dots, \boldsymbol{w}_m)$ of W. Let $S : W \to V$ be the linear transformation such that $S(\boldsymbol{w}_j) = \boldsymbol{v}_j$ if $j \leq n$ and $S(\boldsymbol{w}_j) = \mathbf{0}_V$ if $j > n$.

16. First prove that $Ker(T^n) = Ker(T^{n+1})$ and then use the Rank-Nullity Theorem to conclude that $R(T^n) = R(T^{n+1})$. Consider separately the cases: i) There is an $l < n$ such that $Ker(T^l) = Ker(T^{l+1})$ and ii) $Ker(T^l) \subsetneq Ker(T^{l+1})$ for $l = 1, \dots, n-1$. Use a dimension argument to prove that T^n is the zero operator.

17. Use Exercise 16 to prove that $Ker(T^n) \cap R(T^n) = \mathbf{0}$ and then use the Rank-Nullity Theorem.

18. Use the Rank-Nullity Theorem.

19.a) If $TS = \mathbf{0}_{V \to V}$ then $Range(S) \subset ker(T)$. b) Let $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_{n-k}$ be a basis of $ker(T)$ and extend to a basis $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ of V. Let S be the linear transformation such that $S(\boldsymbol{v}_j) = \boldsymbol{v}_j$ if $1 \leq j \leq n-k$ and $S(\boldsymbol{v}_j) = \mathbf{0}$ if $n-k < j$.

Section (2.3)

6. Define $T : U \oplus V \to (U/X) \oplus (V/Y)$ by $T(\boldsymbol{u}, \boldsymbol{v}) = (\boldsymbol{u} + X, \boldsymbol{v} + Y)$. Determine the kernel of T and apply the First Isomorphism Theorem.

8. Apply the Third Isomorphism Theorem to conclude that $dim(U/(U \cap$

$W)) \leq n$. Use the Second Isomorphism Theorem to conclude that $dim(V/(U \cap W))/(U/U \cap W)) = m$. Use this to obtain the result.

Section (2.4)

1. Use Exercises (2.1.13) and (1.8.5).

2. Use Theorem (2.11) and Theorem (1.30).

6. Let $\mathcal{S}^n$ be the standard basis of $\mathbb{F}^n$ and $\mathcal{S}^m$ be the standard basis of $\mathbb{F}^n$. Let $A = \mathcal{M}_T(\mathcal{S}^n, \mathcal{S}^m)$.

7. Use Exercises (1.8.5), (2.2.13) and Theorem (2.23).

8. Use Exercises (1.8.6), (2.2.14) and Theorem (2.23).

Section (2.5)

1. Find 2×2 matrices A and B such that $AB \neq BA$. For example, $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. Choose and basis $\mathcal{B}$ of V. Let S and T be the operators on V such that $\mathcal{M}_S(\mathcal{B}, \mathcal{B}) = A$ and $\mathcal{M}_T(\mathcal{B}, \mathcal{B}) = B$. Use Theorem (2.23).

2. Find non-zero 2×2 matrices A and B such that $AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Choose a basis $\mathcal{B}$ of V. Let S and T be the operators on V such that $\mathcal{M}_S(\mathcal{B}, \mathcal{B}) = A$ and $\mathcal{M}_T(\mathcal{B}, \mathcal{B}) = B$. Use Theorem (2.23).

7. Let E_{ij} be the matrix with all zeros except a 1 in position (i, j). Let P_{ij} the matrix obtained from the identity matrix by exchanging the i and j rows (equivalently, columns). Prove that $P_{ki}E_{ij}P_{jl} = E_{kl}$. Use this to prove that if an ideal J contains E_{ij} then $J = M_{nn}(\mathbb{F})$. Then show if J contains a matrix A whose (i, j)-entry, a_{ij} is nonzero, then $E_{ij} \in J$.

8. Assume $T \in \mathcal{L}(V, V)$ is not a unit. Then $Ker(T) \neq \{\mathbf{0}\}$. Let $\boldsymbol{v}$ be a nonzero vector in $Ker(T)$. Set $\boldsymbol{v}_1 = \boldsymbol{v}$ and extend to a basis $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$. Let S be the operator such that $S(\boldsymbol{v}_j) = \boldsymbol{v}$ for all j. Prove TS is the zero operator.

Section (2.6)

12. Use Theorem (2.23).

13. If Q is a matrix such that $Q\mathcal{M}_{T_1}(\mathcal{B}, \mathcal{B})Q^{-1} = \mathcal{M}_{T_2}(\mathcal{B}, \mathcal{B})$ let S be the operator on V such that $\mathcal{M}_S(\mathcal{B}, \mathcal{B}) = Q$. Use Theorem (2.23) to prove that $T_2 = ST_1S^{-1}$.

14. Use Exercise 13.

Section (3.1)

4. Use the division algorithm.

5. If $a(x), b(x)$ are polynomials such that $a(x)f(x) + b(x)g(x) = d(x)$, prove that $a(x)f'(x) + b(x)g'(x) = 1$.

9. Use Exercises 6 and 7.

10. Use the second principle of mathematical induction. Use the division algorithm in $\mathbb{F}[x]$ to write $f(x) = g(x)h^*(x) + r(x)$ where $r(x) = 0$ or $deg(r) < deg(g)$. Use a degree argument to prove that the leading terms of $h(x)$ and $h^*(x)$ are the same and apply induction to prove that $r(x)$ is the zero polynomial so that $h(x) = h^*(x)$.

Section (3.2)

1. Use Lemma (3.8) to obtain a pairing of complex, non-real roots.

5. Use Lemma (3.8) to conclude that $3-4i$ is also a root of $f(x)$ and of $g(x)$ and that $x^2-6x+25$ divides both $f(x)$ and $g(x)$.

Section (4.1)

5. Apply S to $T(\boldsymbol{v})$ and use commutativity.

6. Let T' be the restriction of T to U so that by hypothesis, T' is an operator on U. Use the invertibility of T to show that T' is injective and then show that this implies T' is bijective.

14. If $\boldsymbol{v}$ is a eigenvector with eigenvalue λ, show that $\mu_{T,\boldsymbol{v}}(x) = x - \lambda$. Then use the fact that for all vectors $\boldsymbol{v}, \mu_{T,\boldsymbol{v}}(x) \mid \mu_T(x)$.

15. Use Theorem (2.22).

16. Use Theorem (2.22).

21. Note for any polynomial $f(x)$ that $Sf(TS) = f(ST)T$. Use this to prove that $\mu_{ST}(x)$ divides $x\mu_{TS}(x)$ and $\mu_{TS}(x)$ divides $x\mu_{ST}(x)$.

Section (4.2)

3. Let $\boldsymbol{v}$ be any non-zero vector. Prove that $\langle T, \boldsymbol{v}\rangle = V$.

5. Consider the different possibilities for the minimum polynomial of T (there are 4 cases to consider).

8. Consider the possibilities for the minimum polynomial of T (there are 9 cases to consider).

12. Assume $V = \langle T, \boldsymbol{v}\rangle$. Set $\boldsymbol{v}_1 = \boldsymbol{v}$ and $\boldsymbol{v}_j = T^{j-1}(\boldsymbol{v})$ for $2 \leq j \leq n$. If $S(\boldsymbol{v}) = c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n$, set $g(x) = \sum_{j=0}^{n-1} c_{j+1}x^j$. Show that $S = g(T)$.

Section (4.3)

4. Prove that $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_j)$ is linearly independent by induction on j.

5. Use the fact that $x^2 + 1, x + 1$ and $x - 2$ are pairwise relatively prime polynomials to show that $\mu_{T,\boldsymbol{v}_1+\boldsymbol{v}_2}(x) = (x^2+1)(x-1)$ and then that $\mu_{T,\boldsymbol{v}_1+\boldsymbol{v}_2+\boldsymbol{v}_3}(x) = (x^2 + 1)(x - 1)(x-2)$. Then explain why T is cyclic and $\mu_T(x) = (x^2 + 1)(x - 1)(x - 2)$.

6. First mimic Exercise 5 to show that $\mu_{T,\boldsymbol{v}_1+\boldsymbol{v}_3+\boldsymbol{v}_4}(x) = \mu_T(x) = x^4 - 1$. Then show that if $\boldsymbol{u} = c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + c_3\boldsymbol{v}_3 + c_4\boldsymbol{v}_4$ then $\mu_{T,\boldsymbol{u}}(x) = x^4 - 1$ if and only if $c_3 \neq 0, c_4 \neq 0$ and at least one of $c_1, c_2 \neq 0$.

8. Note that $x^5 - x = x(x - 1)(x - 2)(x - 3)(x - 4)$ in $\mathbb{F}_5[x]$. Use this to prove that there are vectors $\boldsymbol{x}_i, 0 \leq i \leq 4$ such that $T(\boldsymbol{x}_i) = i\boldsymbol{x}_i$ and that $(\boldsymbol{x}_0, \ldots, \boldsymbol{x}_4)$ is a basis for $\mathbb{F}_5^5$. Then show that a vector $c_0\boldsymbol{x}_0 + \cdots + c_4\boldsymbol{x}_4$ is maximal if and only if all $c_i \neq 0$.

Section (4.4)

4. Use Exercise 21 of Section (4.1). If $S = g(T)$, use the irreducibility of $p(x)$ to show the existence of polynomials $a(x), b(x)$ such that $a(x)g(x) + b(x)p(x) = 1$ and then prove that $a(T)$ is an inverse to S.

5. Let $\mu_{T,\boldsymbol{v}_i}(x) = p(x)^{e_i}$. Choose i so that e_i is maximal and prove $e_i = m$. Use the fact that the LCM of $\{\mu_{T,\boldsymbol{v}_i}(x)\}$ is $\mu_T(x) = p(x)^m$.

6. Use Exercise 5.

7. Use the characterization of indecomposable operators to show that $\mu_T(x)$ is $p(x)^e$ for some real irreducible polynomial $p(x)$. Use the fact that the dimension of the space is odd to conclude that $p(x)$ is a linear polynomial.

8. Show that $\mu_T(x)$ is either of the form $(x - \lambda)^{2n}$ or $p(x)^m$ where $p(x)$ is a real irreducible quadratic and use Theorem (4.5).

9. Separate into cases as the minimum polynomial of T is either of the form $(x - \lambda)^4$ or $p(x)^2$ where $p(x)$ is a

quadratic polynomial irreducible over $\mathbb{F}_p$.

10. Assuming T is indecomposable, use Theorem (4.5). For the converse prove the contrapositive: If T is decomposable then there exists more than one maximal proper T-invariant subspace.

Section (4.5)

9. Set $V_i = \{\boldsymbol{v} \in V | p_i(x)^{dim(V)}(\boldsymbol{v}) = \boldsymbol{0}\}$ so that $V = V_1 \oplus \cdots \oplus V_t$. Since the existence of infinitely many T-invariant subspaces in $V(p_i)$ implies infinitely many T-invariant subspaces it is only necessary to prove if for each i there are only finitely many T-invariant subspaces in $V(p_i)$ then there are only finitely many T-invariant subspaces. Prove if U is a T invariant subspace and $U_i = U \cap V_i$ then $U = U_1 \oplus \cdots \oplus U_t$.

10. Continue with the notation of Exercise 9. The main thing one needs to show is that if some V_i is not cyclic then V_i has infinitely many T-invariant subspaces. Show if V_i is not cyclic then there are vectors $\boldsymbol{u}$ and $\boldsymbol{w}$ such that $\mu_{T,\boldsymbol{u}}(x) = \mu_{T,\boldsymbol{w}}(x) = p_i(x)$ and $\langle T, \boldsymbol{u}\rangle \cap \langle T, \boldsymbol{w}\rangle = \{\boldsymbol{0}\}$. Prove that $\langle T, \boldsymbol{u} + a\boldsymbol{w}\rangle, a \in \mathbb{F}$ are all distinct T-invariant subspaces.

Section (4.7)

10. Choose a basis $\mathcal{B}$ so that $M = \mathcal{M}_T(\mathcal{B}, \mathcal{B})$ is in Jordan canonical form. Let A be the diagonal of M and $B = M - A$ so that B is strictly lower triangular and hence nilpotent. Now use this to get the operators D and N.

11. Show if $p(x)$ is an irreducible factor of $\mu_T(x)$ then $p(x)$ is a real quadratic. Use this to prove that any elementary divisor of T restricted to a T-invariant subspace U has even degree and consequently U has even dimension.

Section (5.1)

8. If $\boldsymbol{v} = c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n = \boldsymbol{0}$ then $\boldsymbol{v} \cdot \boldsymbol{v}_j = 0$. Use additivity and homogeneity in the first argument to then show that $\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$ in the null space of the matrix A.

Section (5.2)

11. Set $\boldsymbol{x} = \sum_{i=1}^n \frac{x_j}{j}$ and $\boldsymbol{y} = \sum_{i=1}^n jy_j$. Use Cauchy-Schwartz.

16. Let α be the scalar such that $\boldsymbol{u} = \boldsymbol{y} - \alpha\boldsymbol{x} \perp \boldsymbol{x}$ so that $\boldsymbol{y} = \alpha\boldsymbol{x} + \boldsymbol{u}$. Compute $\langle \boldsymbol{y}, \boldsymbol{x}\rangle\langle \boldsymbol{x}, \boldsymbol{y}\rangle$ and $\langle \boldsymbol{y}, \boldsymbol{y}\rangle$.

Section (5.3)

4. Start with a basis $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k)$ and extend to a basis $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n)$ for V. Use Gram-Schmidt to get an orthonormal basis $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ such that $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)$ is an orthonormal basis of W. Prove that $W^{\perp} = Span(\boldsymbol{w}_{k+1}, \ldots, \boldsymbol{w}_n)$.

5. Use Exercise 4 and the fact that $W \cap W^{\perp} = \boldsymbol{0}$.

6. First prove that $W \subset (W^{\perp})^{\perp}$ and then use Exercise 4 to conclude that $dim(W) = dim((W^{\perp})^{\perp})$.

10. Extend $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)$ to an orthonormal basis $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ of V and write $\boldsymbol{u} = \sum_{i=1}^n c_i\boldsymbol{v}_i$.

12. Express $\boldsymbol{x}$ and $\boldsymbol{y}$ as linear combinations of $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$.

Section (5.4)

8. Set $W_i = Span(\boldsymbol{w}_i)$ and $P_i = Proj_{(W_i, W_i^{\perp})}$. Then $P = P_1 + \cdots + P_k$. Prove for $i \neq j$ that $P_iP_j =$

$\mathbf{0}_{V\to V}$ and $[\boldsymbol{w}_i]_{\mathcal{S}}^{tr}[\boldsymbol{w}_j]_{\mathcal{S}} = 0$. Show that $\mathcal{M}_{P_i}(\mathcal{S},\mathcal{S}) = [\boldsymbol{w}_i]_{\mathcal{S}}[\boldsymbol{w}_i]_{\mathcal{S}}^{tr}/$

12. Express $\boldsymbol{u}$ as $\boldsymbol{w}+\boldsymbol{x}$ where $\boldsymbol{w}\in W, \boldsymbol{x}\in W^{\perp}$. Use the Pythagorean theorem.

13. Express $\boldsymbol{u}$ as $\boldsymbol{w}+\boldsymbol{x}$ where $\boldsymbol{w}\in W, \boldsymbol{x}\in W^{\perp}$. Use the Pythagorean theorem.

Section (5.5)

5. Assume $rank(T) = k$ and $(\boldsymbol{w}_1,\dots,\boldsymbol{w}_k)$ is a basis for $R(T)$. Extend to a basis $\mathcal{B}_W = (\boldsymbol{w}_1,\dots,\boldsymbol{w}_m)$ for W. Let $(g_1,\dots,g_m)$ be the basis of W' dual to $\mathcal{B}_W$. Show $R(T') = Span(T'(g_1),\dots,T'(g_k))$. Then prove that $(T'(g_1),\dots T'(g_k))$ is linearly independent.

6. Use Exercise 5.

7. Prove that T is injective by proving for all $\boldsymbol{v}\neq\mathbf{0}$ that $T(\boldsymbol{v}) \neq \begin{pmatrix}0\\0\\\vdots\\0\end{pmatrix}$.

8. Use Exercise 4.

9. Try an indirect proof by first establishing the existence of a natural isomorphism between V and $(V')'$.

10. Start with a basis $(\boldsymbol{u}_1,\dots,\boldsymbol{u}_k)$ for U and extend to a basis $\mathcal{B} = (\boldsymbol{u}_1,\dots,\boldsymbol{u}_n)$. Let $(g_1,\dots,g_n)$ be the basis of V' dual to $\mathcal{B}$. Prove that $U' = Span(g_{k+1},\dots,g_n)$.

11. Get inclusions and use dimension arguments.

15. Show if $\mathcal{B} = (\boldsymbol{v}_1,\dots,\boldsymbol{v}_n)$ is a basis for V and $\mathcal{B}' = (g_1,\dots,g_n)$ is the basis of V' then $\mathcal{M}_{T'}(\mathcal{B}',\mathcal{B}') = \mathcal{M}_T(\mathcal{B},\mathcal{B})^{tr}$.

16. Get inclusions and use dimension arguments.

Section (5.6)

5. Prove that $\langle (T^*)^*(\boldsymbol{v}),\boldsymbol{w}\rangle_W = \langle T(\boldsymbol{v}),\boldsymbol{w}\rangle_W$ for all W and use this to conclude from positive definiteness that $T = (T^*)^*$.

6. Use the fact that $(S+T)^* = S^*+T^*$ and $(\lambda T)^* = \overline{\lambda}T^*$ to show that $(T-\lambda I_V)^* = T^*-\overline{\lambda}I_V$ is not surjective, hence not injective, whence has non-trivial kernel.

8. First prove T^*T is injective and then use the fact that V is finite dimensional to prove that T^*T is invertible.

9. Prove that $T^*: W\to V$ is injective and use Exercise 8.

10. Use the definition of T^* to show if $\boldsymbol{u}\in U, \boldsymbol{w}\in U^{\perp}$ then $\langle \boldsymbol{u}, T^*(\boldsymbol{w})\rangle = 0$.

11. Use the definition of T^* and positive definiteness.

13. Let $\mathcal{B}_V$ be an orthonormal basis of V and $\mathcal{B}_W$ an orthonormal basis of W. Set $A = \mathcal{M}_T(\mathcal{B}_V,\mathcal{B}_V)$ and $A^* = \mathcal{M}_{T^*}(\mathcal{B}_W,\mathcal{B}_W)$. Show $rank(T) = rank(A) = rank(A^*) = rank(T^*)$.

14. Assume S exists. Use $1 = \langle \boldsymbol{v}_1,\boldsymbol{v}_1\rangle = \langle \boldsymbol{v}_1, S^*(\boldsymbol{y})\rangle$ and the fundamental equation. Assume $\langle \boldsymbol{x},\boldsymbol{y}\rangle = 1$. To show the existence of S let $(\boldsymbol{x}_2,\dots,\boldsymbol{x}_n)$ be a basis for $\boldsymbol{y}^{\perp}$ and set $\boldsymbol{x}_1 = \boldsymbol{x}$. Prove $\boldsymbol{x}_1\notin\boldsymbol{y}^{\perp}$ and that $(\boldsymbol{x}_1,\dots,\boldsymbol{x}_n)$ is a basis for V. Let $S\in\mathcal{L}(V,V)$ such that $S(\boldsymbol{v}_i) = \boldsymbol{x}_i$. Prove that this satisfies the conclusions.

Section (5.7)

7. Let $\{\boldsymbol{x}_k\}_{k=1}^{\infty}$ be a Cauchy sequence in $(\mathbb{R}^n, \|\|_1)$ where $\boldsymbol{x}_k = \begin{pmatrix}x_{1k}\\\vdots\\x_{nk}\end{pmatrix}$. Prove

for each $i, 1 \leq i \leq n$, that $\{x_{ik}\}_{k=1}^n$ is a Cauchy sequence since $|x_i - x_j| \leq \| \boldsymbol{x}_i - \boldsymbol{x}_j \|$. So, each has a limit, x_i. Set $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ and prove that $lim_{k\to\infty}\boldsymbol{x}_k = \boldsymbol{x}$ in the l_1-topology.

8. This is proved similar to Exercise 7.

Section (6.1)

8. Start with the definition of $\| T(\boldsymbol{v}) \|$, use the definition of T^* and the assumption that $TT^* = T^*T$.

9. Use Exercise 8.

10. Use Exercise 9 and Theorem (5.21).

11. Start by proving $Ker(T) = Ker(T^*)$. Conclude from Theorem (5.21) that $Range(T) = Range(T^*)$. Let S be the restriction of T to $Range(T)$. Prove that $S = S^*$ and from this that $T = T^*$.

12. Do a proof by contradiction: set $U = Ker(T) = Ker(T^*)$ and assume $U \neq V$. Since T is a nilpotent operator, $Ker(T) \cap W \neq \{\boldsymbol{0}\}$ for any T-invariant subspace. But then $U \cap U^\perp \neq \{\boldsymbol{0}\}$, a contradiction.

Section (6.2)

1. If $\alpha_1, \ldots, \alpha_s$ are the distinct eigenvalues, then the minimum polynomial is $(x-\alpha_1)\ldots(x-\alpha_s)$. Set $F_i(x) = \frac{\mu_T(x)}{x-\alpha_i}$ and note that $x - \alpha_i$ and $F_i(x)$ are relatively prime. Set $V_i = \{\boldsymbol{v} \in V | T(\boldsymbol{v}) = \alpha_i \boldsymbol{v}\}$. Show that there exists a polynomial $g_i(x)$ such that $g_i(T)$ restricted to $V_i^\perp$ is the zero map and $g_i(T)$ restricted to V_i is $\overline{\alpha_i} I_{V_i}$.

7. The only implication you need to prove is T normal with real eigenvalues implies T is self-adjoint. Show that there is an orthonormal basis $\mathcal{B}$ such that $\mathcal{M}_T(\mathcal{B}, \mathcal{B}) = \mathcal{M}_{T^*}(\mathcal{B}, \mathcal{B})$.

8. Do induction on $dim(V)$. Since both S and T are self-adjoint they are diagonalizable. Use the fact that they commute to show that there exists a common eigenvector, $\boldsymbol{v}$, which you can assume has norm 1. Prove that they both leave $\boldsymbol{v}^\perp$ invariant and use the inductive hypothesis.

9. Note for any operator that $Ker(T) \subset Ker(T^2)$ and $Range(T^2) \subset Range(T)$ and by the rank-nullity theorem $Ker(T^2) = ker(T)$ if and only if $Range(T^2) = Range(T)$. Use the spectral theorem to obtain an orthonormal basis $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ for T where $(\boldsymbol{v}_{k+1}, \ldots, \boldsymbol{v}_n)$ is a basis for $Ker(T)$. Prove $Range(T) = Range(T^2) = Span(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)$.

10. Use the fact that there exists a basis $\mathcal{B}$ such that $\mathcal{M}_T(\mathcal{B}, \mathcal{B})$ is diagonal. Then define an inner product in such a way that $\mathcal{B}$ becomes an orthonormal.

11. Use the Spectral Theorem applied to T restricted to U and $U^\perp$ to obtain orthonomal bases of U and $U^\perp$, respectively, consisting of eigenvectors.

13. Note that $U = Range(T)$. If T is self-adjoint then use Theorem (5.21) to conclude that $W = U^\perp$. On the other hand, if $W = U^\perp$ prove there exists an orthonormal basis of V consisting of eigenvectors of T and that the eigenvalues are real (they are 0 or 1).

Section (6.3)

3. You can write down the matrix of T explicitly and define the polynomial.

4. Use Exercise 3.

5. Express the minimum polynomial of T as a product of linear and irreducible quadratics and decompose the space consistent with these.

6. Use Exercise 5.

7. Use the fact that T is cyclic.

8. Prove that T is cyclic.

9. Use Exercise 8.

10. Use the fact T is a cyclic operator.

Section (6.4)

1. Use the definition to show $Ker(T) = \{\mathbf{0}\}$.

3. Show directly that the norm of any vector is preserved.

5. Let S be the operator such that $S(\boldsymbol{u}_i) = \boldsymbol{v}_i$. Use Theorem (6.7) to prove this is a unitary operator and then apply Theorem (6.8).

11. Use the Spectral Theorem.

13. Prove that T restricted to U is bijective. Then prove for arbitrary $\boldsymbol{u} \in U, \boldsymbol{w} \in U^{\perp}$ that $\langle T(\boldsymbol{w}), \boldsymbol{u}\rangle = 0$.

14. Use induction and the fact that a unitary operator is normal and therefore completely reducible.

15. Let $(\boldsymbol{u}_{i1}, \ldots, \boldsymbol{u}_{ik})$ be an orthonormal basis of $U_i^{\perp}$ for $i = 1, 2$ and let $R' : U_1^{\perp} \to U_2^{\perp}$ be the transformation such that $R'(\boldsymbol{u}_{1j}) = \boldsymbol{u}_{2j}$. Then R' is an isometry. "Paste" R and R' together to define an isometry $S : V \to V$.

16. Show that there is an eigenvector $\boldsymbol{v}$ with eigenvalue in $\{-1, 1\}$.

19. Show that S is normal with respect to the inner product defined by the dot product but T is not.

Section (6.5)

2. Use the Spectral Theorem of normal operators on a complex inner product space.

3. Use Lemma (6.5).

4. Use Exercise 3.

5. Use the fact that the sum of self-adjoint operators is self-adjoint.

8. Use the Spectral Theorem.

11. Define [,] by $[\boldsymbol{v}, \boldsymbol{w}] = \langle T(\boldsymbol{v}), \boldsymbol{w}\rangle$ which is an inner product by Exercise 9. Set $S = RT$. Use Exercise 10 to show that S is self-adjoint. Then show that TR is similar to RT.

18. Use the fact that $Ker(T) = Ker(T^*T)$ and $Ker(T^*) = Ker(TT^*)$ to conclude that $rank(T^*T) = rank(TT^*)$. Let S be the restriction of T to $Range(T^*T)$. Show that S is an isomorphism of $Range(T^*T)$ to $Range(TT^*)$. Then prove if $\boldsymbol{v} \in Range(T^*T)$ is an eigenvector of T^*T with eigenvalue α then $S(\boldsymbol{v})$ is an eigenvector of TT^* with eigenvalue α.

Section (7.1)

8. Show that A has 0 as its unique eigenvalue using Exercise 7.

10. Prove the corresponding result for matrices. Further, show if E_{kl} is the matrix with all 0's except a 1 in the (k, l)- position prove and A has entries a_{ij} then $Trace(AE_{ji}) = a_{ij}$.

11. Choose a basis $\mathcal{B}$ of V such that $\mathcal{M}_T(\mathcal{B}, \mathcal{B})$ is lower triangular.

12. Choose a basis $\mathcal{B}$ for V such that $\mathcal{M}_T(\mathcal{B}, \mathcal{B})$ is lower triangular.

13. Choose an orthonormal basis for V use the relationship between $\mathcal{M}_T(\mathcal{B}, \mathcal{B})$ and $\mathcal{M}_{T^*}(\mathcal{B}, \mathcal{B})$.

14. Choose an orthonormal basis

for V use the relationship between $\mathcal{M}_T(\mathcal{B},\mathcal{B})$ and $\mathcal{M}_{T^*}(\mathcal{B},\mathcal{B})$.

16. T^*T is self-adjoint and semi-positive.

17. If T is the zero operator, then there is nothing to prove. Since the characteristic is zero, T is not a scalar operator. This implies that there is a vector $\boldsymbol{v}$ such that $(\boldsymbol{v}, T(\boldsymbol{v}))$ is linearly independent. Extend to a basis and use induction.

18. Let C be a diagonal matrix with distinct diagonal entries. Define an operator $ad(C) : M_{nn}(\mathbb{F}) \to M_{nn}(\mathbb{F})$ by $ad(C)(B) = BC - CB$. Prove that $dim(Ker(ad(C))) = n$ so that $dim(Range(ad(C))) = n^2 - n$ which is the dimension of the space of $n \times n$ matrices with zeros on the diagonal.

19. Use 17 and 18.

Section (7.2)

3. Choose an orthonormal basis $\mathcal{B}$ for V use the relationship between $\mathcal{M}_T(\mathcal{B},\mathcal{B})$ and $\mathcal{M}_{T^*}(\mathcal{B},\mathcal{B})$.

5. Use Exercise 4.

9. Use $1 = det(AA^{-1}) = det(A)det(A^{-1})$.

10. Use Exercise 8.

11. Use the Spectral Theorem.

12. T^*T is self-adjoint and so has real , non-negative eigenvalues.

13. T is normal. Use the result on normal operators on real inner product spaces along with the characterization of orthogonal operators.

14. T is normal. Use the Spectral Theorem and the Characterization Theorem.

17. Add or subtract the first row from each subsequent row obtain a matrix B such that all entries $b_{i1} = 0$ for $2 \leq i \leq n$. Show that every entry b_{ij} is divisible by 2 for $2 \leq i \leq n$.

Section (7.3)

5. Let $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m)$ be a sequence of vectors from V. By the Exchange Theorem it is linearly dependent. Use Lemma (7.11).

Section (8.1)

5. For $\boldsymbol{w} \in W$, denote by F the map from V to $\mathbb{F}$ given by $F(\boldsymbol{w})(\boldsymbol{v}) = f(\boldsymbol{v}, \boldsymbol{w})$. This is a transformation from W to V'. Use the Rank-Nullity Theorem.

13. Let $\mathcal{B}_V = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)$ be a basis of V and $\mathcal{B}_W = (\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n)$ be a basis of W and set $a_{ij} = f(\boldsymbol{v}_i, \boldsymbol{w}_j)$ and let A be the matrix with (i,j)-entry equal to a_{ij}. Note that $rank(A) = n - nullity(A) = rank(A^{tr}) = m - nullity(A^{tr})$.

14. Use Exercise 13.

16. Show that the map $F : W \to V'$ given by $F(\boldsymbol{w})(\boldsymbol{v}) = f(\boldsymbol{v}, \boldsymbol{w})$ is an isomorphism. Let $g_1, \ldots, g_n$ be a the basis of V' which is dual to $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ and then let $\boldsymbol{w}_i \in W$ be the preimage under F of g_i.

Section (8.2)

3. Prove $U \subset (U^\perp)^\perp$ and use a dimension argument to get equality.

5. Use $U \subset U^\perp$ and Lemma (8.12).

6. Choose a basis for U and extend this to a hyperbolic basis.

Section (8.3)

6. Let U and W be totally singular subspaces of dimensions k and l with $k \leq l$. Use Witt's Theorem to obtain an isometry S such that $S(U) \subset W$.

7. Do a proof by induction on n, the dimension of the space V.

8. Use Exercise 7.

18. Use the fact that for every $c \in \mathbb{F}_q$ there exists a and $b \in \mathbb{F}_q$ such that $a^2 + b^2 = c$.

19. Use Exercise 18.

Section (8.4)

4. First, use the fact that if U is a non-singular three dimensional subspace then it contains singular vectors to prove. Then prove if $dim(V) = 4$ then the index is one or two. Then do an induction on m.

8. Prove that $E_2 \perp E_2$ has index two.

Section (8.5)

8. For $\boldsymbol{y} \in V$ show there exists a unique vector $T(\boldsymbol{y}) \in V$ such that $f(\boldsymbol{x}, \boldsymbol{y}) = \langle \boldsymbol{x}, T(\boldsymbol{y}) \rangle$. Prove that T is linear and a symmetric operator.

Section (9.1)

6. Let g_i be the σ-semilinear map such that $g_i(\boldsymbol{v}_j) = 1$ if $j = i$ and $g_i(\boldsymbol{v}_j) = 0$, otherwise. Use Lemma (9.5) to obtain $\boldsymbol{v}_i'$.

7. Prove if $\sigma^2 = I_{\mathbb{F}}$ then f is reflexive. When $\sigma^2 \neq I_{\mathbb{F}}$ and $dim(V) > 1$, prove that f is not reflexive.

Section (9.2)

7. Let $\boldsymbol{x}$ be an anisotropic vector. Prove if $\boldsymbol{y} \perp \boldsymbol{x}$ then $\boldsymbol{y}$ is also anisotropic. Use the fact that N is surjective to conclude that there are $\boldsymbol{x}' \in Span(\boldsymbol{x})$ and $\boldsymbol{y}' \in Span(\boldsymbol{y})$ such that $f(\boldsymbol{x}', \boldsymbol{x}^p rime) = 1 = -f(\boldsymbol{y}', \boldsymbol{y}')$.

8. Do induction on $n = dim(V)$ and use Exercise 7.

9. Let I be the set of isotropic vectors and set $U = Span(I)$. Suffices to prove that $U = V$. Let $\boldsymbol{x} \in I$ and $\boldsymbol{y}$ an arbitrary non-isotropic vector. Assume $\boldsymbol{y} \not\perp \boldsymbol{x}$ so that $Span(\boldsymbol{x}, \boldsymbol{y})$ is non-degenerate. Prove there is an isotropic vector $\boldsymbol{y}' \in Span(\boldsymbol{x}, \boldsymbol{y}) \setminus Span(\boldsymbol{x})$ and then $\boldsymbol{y} \in Span(\boldsymbol{x}, \boldsymbol{y}) = Span(\boldsymbol{x}, \boldsymbol{y}') \subset U$.

Assume $\boldsymbol{y} \perp \boldsymbol{x}$. Choose $\boldsymbol{z} \in I$ such that $f(\boldsymbol{x}, \boldsymbol{z}) = 1$. Then $Span(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ is non-degenerate. Prove that there is a $\boldsymbol{y}' \in I \cap [Span(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \setminus Span(\boldsymbol{x}, \boldsymbol{z})]$. Then $Span(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = Span(\boldsymbol{x}, \boldsymbol{y}', \boldsymbol{z}) \subset Span(I)$.

Section (10.1)

5. Let $(\boldsymbol{z}_1, \ldots, \boldsymbol{z}_s)$ be a basis for $W' = Span(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n)$. Express each $\boldsymbol{w}_j$ as a linear combination of $(\boldsymbol{z}_1, \ldots, \boldsymbol{z}_s)$. Use the independence of $\{\boldsymbol{x}_j \otimes \boldsymbol{z}_i | 1 \leq j \leq n, \leq i \leq s\}$.

6. Show Z is a solution to the universal mapping property that defines the tensor product of V and W.

9. To avoid confusion denote the tensor product of X and Y by $X \otimes' Y$. Define a map $\theta : X \times Y \to V \otimes W$ by $\theta(x, y) = x \times y$. Use the universal property of $X \otimes' Y$ to get a linear map $\theta' : X \otimes' Y \to V \otimes W$ and show that it is injective and the range is Z.

Section (10.2)

1. Use the universal mapping property.

3 Do induction on $m \geq 2$.

4. Turn this into a problem of the rank of operators $R : \mathbb{F}^l \to \mathbb{F}^k$ and $S : \mathbb{F}^n \to \mathbb{F}^m$ and then into the dimension of the range of $R \otimes S$ from $\mathbb{F}^l \otimes \mathbb{F}^n$ to $\mathbb{F}^k \otimes \mathbb{F}^m$.

5. Prove the contrapositive: If S and

T are not nilpotent then $S \otimes T$ is not nilpotent.

6. Use a diagonalizing basis of V for S and a diagonalizing basis of W for T to obtain a diagonalizing basis of $V \otimes W$ for $S \otimes T$.

12. Choose a basis $\mathcal{B}_i$ for $V_i, i = 1, 2$ and set $A_i = \mathcal{M}_{S_i}(\mathcal{B}_i, \mathcal{B}_i)$ so that $\mathcal{M}_{S_1 \otimes S_2}(\mathcal{B}_1 \otimes \mathcal{B}_2, \mathcal{B}_1 \otimes \mathcal{B}_2) = A_1 \otimes A_2$. Use the definition of $A_1 \otimes A_2$ to prove that $Trace(A_1 \otimes A_2) = Trace(A_1)Trace(A_2)$.

14. Use Exercise 13.

Section (10.3)

2. Use Lemma (10.2) to argue that each $S \otimes \cdots \otimes S : \mathcal{T}_k(V) \to \mathcal{T}_k(W)$ is surjective, whence $\mathcal{T}(S) : \mathcal{T}(V) \to \mathcal{T}(W)$ is surjective.

3. Use Lemma (10.2) to argue that each $S \otimes \cdots \otimes S : \mathcal{T}_k(V) \to \mathcal{T}_k(W)$ is injective, whence $\mathcal{T}(S) : \mathcal{T}(V) \to \mathcal{T}(W)$ is injective.

4. Use part v) of Lemma (10.2).

10. Assume $S^l = 0_{V \to V}$. Prove that $\mathcal{T}_k(S)^{kl-l+1} = 0_{\mathcal{T}_k(V) \to \mathcal{T}_k(V)}$.

11. Make a conjecture based on the case that the minimum polynomial of S splits into linear factors in $\mathbb{F}[x]$ and then in the general case prove this conjecture by induction on $dim(V)$.

12. Make a conjecture based on the case that the minimum polynomial of S splits into linear factors in $\mathbb{F}[x]$ and then in the general case prove this conjecture by induction on $dim(V)$.

Section (10.4)

2. Use the identification of $Sym(V)$ with $\mathbb{F}[x_1, \ldots, x_n]$ when $dim(V) = n$.

3. Assume $\mathbb{K}$ is an extension field of $\mathbb{F}$ such that $\chi_T(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4)$. Express $a_0, \ldots, a_3$ in terms of $\alpha_1, \ldots, \alpha_4$. Then express the eigenvalues of $Sym_2(T)$ in terms of $\alpha_1, \ldots, \alpha_4$, whence in terms of $a_0, \ldots, a_3$.

Section (10.5)

8. Make a conjecture based on the case that the minimum polynomial of S splits into linear factors in $\mathbb{F}[x]$. Then prove this holds for every elementary matrix and use this to prove it in the general case.

14. Let $f(x) = x^4 - 8x^3 + 12 - 2$. You may assume with respect to some basis $\mathcal{B} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_4)$ that the matrix of S is the companion matrix $C(f)$. You can use this to find the matrix of $\wedge^2(S)$ with respect to the basis $(\boldsymbol{v}_1 \wedge \boldsymbol{v}_2, \ldots, \boldsymbol{v}_3 \wedge \boldsymbol{v}_4)$ and then determine the characteristic polynomial of this matrix.

15. Let $f(x) = x^3 - 6x + 3$. Let S be the operator on a three-dimensional vector space such that the matrix of S with respect to a basis $\mathcal{B} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3)$ is $C(f)$. Use this to find the matrix of $\wedge^2(V)$ with respect to the basis $(\boldsymbol{v}_1 \wedge \boldsymbol{v}_2, \boldsymbol{v}_1 \wedge \boldsymbol{v}_3, \boldsymbol{v}_2 \wedge \boldsymbol{v}_3)$ and the determine the characteristic polynomial of this matrix.

16. Let $f(x) = x^4 - 3x^3 + 3$. Let S be the operator on a three-dimensional vector space such that the matrix of S with respect to a basis $\mathcal{B} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3, \boldsymbol{v}_4)$ is $C(f)$. Use this to find the matrix of $\wedge^2(V)$ with respect to the basis $(\boldsymbol{v}_1 \wedge \boldsymbol{v}_2, \ldots, \boldsymbol{v}_3 \wedge \boldsymbol{v}_4)$ and the determine the characteristic polynomial of this matrix.

Section (10.6)

1. Show that there is a vector $\boldsymbol{v}$ such that $\phi(\boldsymbol{v}) = -1$. Show that the ideal

$\mathcal{I}_\phi$ is generated by $\boldsymbol{v} \otimes \boldsymbol{v} + 1$ and that $\mathcal{T}(V)/\mathcal{I}_\phi$ is isomorphic to $\mathbb{C}$.

6. Let $(\boldsymbol{x}, \boldsymbol{y})$ be a hyperbolic basis of V. Show that $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{xy}, \boldsymbol{yx})$ is a basis of $C(V)$. Denote the vector $a\boldsymbol{xy} + b\boldsymbol{y} + c\boldsymbol{x} + d\boldsymbol{yx}$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and show that the vector space isomorphism from $C(V)$ to $M_{22}(\mathbb{F})$ is a homomorphism of algebras.

Section (11.1)

4. May assume $H_1 \neq H_2$. Let $P = Span(\boldsymbol{x}_1)$. Extend to basis $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{n-2})$ for $H_1 \cap H_2$. Let $\boldsymbol{x}_{n-1}$ be a vector in $H_1 \setminus H_2$ and $\boldsymbol{x}_n$ a vector in $H_2 \setminus H_1$. Then $H_1 = Span(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{n-1})$ and $H_2 = Span(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{n-2}, \boldsymbol{x}_n)$ and $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ is a basis for V. Note that S restricted to H_1 is the identity and there is a scalar a such that $S(\boldsymbol{x}_n) = \boldsymbol{x}_n + a\boldsymbol{x}_1$. Likewise T restricted to H_2 is the identity and there is a scalar b such that $T(\boldsymbol{x}_{n-1}) = \boldsymbol{x}_{n-1} + b\boldsymbol{x}_1$. Can compute ST and TS on the bases and show they are the same.

5. Set $\boldsymbol{x}'_{n-1} = b\boldsymbol{x}_{n-1} - a\boldsymbol{x}_n$ and $H = Span(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{n-2}, \boldsymbol{x}'_{n-1})$. Prove that $ST \in \chi(P, H)$.

6. This is like Exercise 4.

7. This is like Exercise 5

Section (11.2)

10. Let $X = Span(\boldsymbol{x})$. Let U be a complement to X in $X^\perp$. Then U is non-degenerate. Choose a hyperbolic basis $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{n-1}, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{n-1})$ where $f(\boldsymbol{u}_i, \boldsymbol{u}_j) = f(\boldsymbol{v}_i, \boldsymbol{v}_j) = f(\boldsymbol{u}_i, \boldsymbol{v}_j) = 0$ for $i \neq j$ and $f(\boldsymbol{u}_i, \boldsymbol{v}_i) = 1$. Set $M_0 = Span(\boldsymbol{x}, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_{n-1})$ and for $1 \leq j \leq n-1$ set $M_j = Span(\boldsymbol{x}, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_j, \boldsymbol{u}_{j+1}, \ldots, \boldsymbol{u}_{n-1})$.

Section (11.3)

1. Show that $\tau_{\boldsymbol{u},\boldsymbol{y}}$ and $\rho_{\boldsymbol{z}}\rho_{\boldsymbol{y}}$ have the same images on $\boldsymbol{u}^\perp$.

4. Let G be the group generated by $T_{\boldsymbol{u}} \cup T_{\boldsymbol{v}}$ and prove that G is transitive on singular one dimensional subspaces. Then show if $\boldsymbol{w}$ is a singular vector then $T_{\boldsymbol{w}}$ is contained in G.

10. Set $\boldsymbol{u}' = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \boldsymbol{v}' = \begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix}$. Show that $(\boldsymbol{u}_1, \boldsymbol{v}')$ is a hyperbolic pair of (M, q). Show that the orthogonal complement to $Span(\boldsymbol{u}', \boldsymbol{v}')$ is $\{\begin{pmatrix} 0 & \alpha \\ \overline{\alpha} & 0 \end{pmatrix}$. Set $\boldsymbol{x}' = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\boldsymbol{y}' = \begin{pmatrix} 0 & \omega \\ -\omega & 0 \end{pmatrix}$. Show that $q(\boldsymbol{x}') = 1$, $q(\boldsymbol{y}') = d$, $\boldsymbol{x}' \perp_q \boldsymbol{y}'$. Conclude that (M, q) and (V, ϕ) are isometric.

11. Argue that it suffices to prove that $A \cdot m \in M$ for $A = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}$ where $\alpha \in \mathbb{K}$.

Section (11.4)

1. For $T \in \Omega(W)$ let $\widehat{T} : V \to V$ defined by $T(\boldsymbol{w} + \boldsymbol{u}) = T(\boldsymbol{w}) + \boldsymbol{u}$ where $\boldsymbol{w} \in W$ and $\boldsymbol{u} \in W^\perp$. First prove if $T \in \chi(X, X^\perp \cap W)$, where X is an isotropic one subspace of W (so T is a unitary transvection with center X and axis $X^\perp$ then $\widehat{T} \in \chi(X, X^\perp)$. Then use this to prove the result for arbitrary T.

Section (12.2)

1. Prove that the four Penrose–Moore equations are satisfied by P.

2. Prove that the four Penrose–Moore equations are satisfied by $diag\{\frac{1}{d_1}, \ldots, \frac{1}{d_r}, 0, \ldots, 0\}$.

6. Use the Penrose–Moore equations.

7. Use the Penrose–Moore equations.

11. Use Exercises 7, 8, and the Penrose–Moore equations.

12. Use Exercises 8 and 11.

15. Use Exercises 6, 11, and the Penrose-Moore equations.

Section (12.3)

1. Show if the (i, j)-entry of A^l is non-zero and the (j, k)-entry of A^m is non-zero then the (i, k)-entry of A^{l+m} is non-zero.

5. Expand $(I_n + A)^{n-1}$ using the binomial theorem and use this to conclude for all $i \neq j$ there is an $l < n$ such that $a^l_{ij} \neq 0$. Then show there is an m such that $a^m_{ii} \neq 0$.

8. Prove if $\boldsymbol{v}$ is a positive eigenvector and $A\boldsymbol{v} = \lambda\boldsymbol{v}$ then $\lambda \in \mathbb{R}^+$.

11. Note that this is equivalent to the following: If $z_1 \in \mathbb{R}^+, z_2, \ldots, z_n \in \mathbb{C}$ and $|z_1+\cdots+z_n| = z_1+|z_2|+\cdots+|z_n|$ then $z_i \in \mathbb{R}^+$ for all i. Do an induction on $n \geq 2$.

16. Use Corollary (12.4).

17. Use Corollary (12.5).

Section (12.4)

1. Apply Theorem (12.26) to A^{tr}. Then note that $C'_i(A) = 1 - a_{ii}$.

2. Use Theorem (12.32).

3. Use Theorem (12.26) to conclude that each disc, $\Gamma_i(A)$, contains one eigenvalue, whence the eigenvalues of A are distinct.

4. Use Theorem (12.32) to conclude that each disc, $\Gamma_i(A)$, contains exactly one eigenvalue. Prove that under the hypothesis no disc can contain a pair of conjugate complex numbers.

6. This is proved like Exercise 4.

7. Set $I = \{i_1 < \cdots < i_k\}$ and let $A_{I,I}$ be the $k \times k$ matrix whose (j, m)-entry is a_{i_j, i_m}. Prove that $A_{I,I}$ is strictly diagonally dominant.

8. Use $\sum_{i=1}^n R'_i(A) = \sum_{j=1}^n C'_j(A)$.

9. First show that you can reduce to the case that all $a_{ii} > 0$ and show that $det(A) > 0$. Then do a proof by induction on n.

Section (13.2)

5.a) Let $\boldsymbol{z}$ be the all one vector. The map $\boldsymbol{x} \to \boldsymbol{x} + \boldsymbol{z}$ is a bijection from the collection of words of length t to the words of length $7 - t$.

b) Since the minimal weight is 3 it follows that there are no words of length 5 or 6 (otherwise by a) there would be words of weight 2 or 1). It then follows that, apart from the zero word and the word of weight 7 there are 14 words of weight 3 or 4. Since there are equally many of each, there are 7 words of weight 3 and 7 words of weight 4.

6. The parity check takes a word of weight 3 to a word of weight 4. A word of length weight 4 remains 4.

This page intentionally left blank

Bibliography

[1] B.N. Cooperstein. *Elementary Linear Algebra.* Worldwide Center of Mathematics, Cambridge, MA, 2012.

[2] B.N. Cooperstein. *An Introduction to Groups, Rings, and Fields.* Worldwide Center of Mathematics, Cambridge, MA, 2012.

[3] D.S. Dummit and R.M. Foote. *Abstract Algebra.* John Wiley and Sons, Inc., Hoboken, NJ, 2004.

[4] H. Dym. *Linear Algebra in Action.* American Mathematical Society, Providence, Rhode Island, 2013.

[5] Y. Eidelman, V. Milman, and A. Tsolomitis. *Functional Analysis: An Introduction.* American Mathematical Society, Providence, Rhode Island, 2004.

[6] M. Eisenberg. *The Mathematical Method: A Transition to Advanced Mathematics.* Prentice Hall, Upper Saddle River, NJ, 1996.

[7] T. Gamelin. *Complex Analysis.* Springer-Verlag, New York, NY, 2003.

[8] L.C. Grove. *Classical Groups and Geometric Algebra.* American Mathematical Society, Providence, Rhode Island, 2002.

[9] P.R. Halmos. *Naive Set Theory.* Springer-Verlag, New York, NY, 1974.

[10] P.C. Hansen, V. Pereyra, and G. Scherer. *Least Squares Data Fitting With Applications.* John Hopkins University Press, Baltimore, MD, 2013.

[11] R.A. Horn and C.R. Johnson. *Topics in Matrix Analysis.* Cambridge University Press, New York, NY, 1991.

[12] R.A. Horn and C.R. Johnson. *Matrix Analysis, Second Edition.* Cambridge University Press, New York, NY, 2013.

[13] N. Jacobson. *Lectures in Abstract Algebra: II. Linear Algebra.* Springer-Verlag, New York, NY, 1953.

[14] A.N. Langville and C.D. Meyer. *Google's PageRank and Beyond: The Science of Search Engine Rankings.* Princeton University Press, Princeton, NJ, 2011.

[15] J.R. Munkres. *Topology, Second Edition.* Prentice Hall, Upper Saddle River, NJ, 2000.

[16] R. Piziak and P.L. Odell. *From Generalized Inverses to Jordan Form.* Chapman & Hall/CRC, Boca Raton, FL, 2007.

[17] D. Poole. *Linear Algebra: A Modern Introduction, Second Edition.* Thompson, Brooks/Cole, Belmont, CA, 2006.

[18] O. Pretzel. *Erroc-Correcting Codes and Finite Fields.* Oxford University Press, Oxford, UK, 1992.

[19] D. Serre. *Matrices: Theory and Practice.* Springer-Verlag, New York, NY, 2000.

[20] T. Sundstrom. *Mathematical Reasoning: Writing and Proof.* Prentice Hall, Upper Saddle River, NJ, 2003.

[21] R. S. Varga. *Geršgorin and His Circles.* Springer-Verlag, New York, NY, 2004.

Mathematics

TEXTBOOKS in MATHEMATICS

Advanced Linear Algebra, Second Edition takes a gentle approach that starts with familiar concepts and then gradually builds to deeper results. Each section begins with an outline of previously introduced concepts and results necessary for mastering the new material. By reviewing what students need to know before moving forward, the text builds a solid foundation upon which to progress.

The new edition of this successful text focuses on vector spaces and the maps between them that preserve their structure (linear transformations). Designed for advanced undergraduate and beginning graduate students, the book discusses the structure theory of an operator, various topics on inner product spaces, and the trace and determinant functions of a linear operator. It addresses bilinear forms with a full treatment of symplectic spaces and orthogonal spaces, as well as explains the construction of tensor, symmetric, and exterior algebras.

Featuring updates and revisions throughout, **Advanced Linear Algebra, Second Edition**:

- Contains new chapters covering sesquilinear forms, linear groups and groups of isometries, matrices, and three important applications of linear algebra
- Adds sections on normed vector spaces, orthogonal spaces over perfect fields of characteristic two, and Clifford algebras
- Includes several new exercises and examples, with a solutions manual available upon qualifying course adoption

The book shows students the beauty of linear algebra while preparing them for further study in mathematics.

CRC Press
Taylor & Francis Group
an **informa** business
www.crcpress.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
711 Third Avenue
New York, NY 10017
2 Park Square, Milton Park
Abingdon, Oxon OX14 4RN, UK

K23692
ISBN: 978-1-4822-4884-5
90000
9 781482 248845
www.crcpress.com