LINEAR ALGEBRA II

Edited by
Dr. Sachin Kaushal

Printed by
EXCEL BOOKS PRIVATE LIMITED
A-45, Naraina, Phase-I,
New Delhi-110028
for
Lovely Professional University
Phagwara

SYLLABUS

Linear Algebra II

Objectives: This course is designed for theoretical study of vector spaces, bases and dimension, subspaces, linear transformations, dual spaces, Elementary Canonical forms, rational and Jordan forms, inner product spaces, spectral theory and bilinear forms. It should be noted that the successful student will be able to prove simple theorems in the subject.

Sr. No.	Description
6	The Jordan Form, Computation of Invariant Factors, Semi-Simple Operators
7	Inner product, Inner Product Space, Linear Functional and Adjoints, Unitary Operators, Normal Operators
8	Introduction, Forms on Inner Product Spaces, Positive Forms, More on Forms
9	Spectral Theory, Properties of Normal operators
10	Bilinear Forms, Symmetric Bilinear Forms, Skew-Symmetric Bilinear Forms, Groups Preserving Bilinear Forms

CONTENT

Unit 1:	The Jordan Form *Richa Nandra, Lovely Professional University*	1
Unit 2:	Computation of Invariant Factors *Richa Nandra, Lovely Professional University*	9
Unit 3:	Semi-simple Operators *Sachin Kaushal, Lovely Professional University*	20
Unit 4:	Inner Product and Inner Product Spaces *Sachin Kaushal, Lovely Professional University*	27
Unit 5:	Linear Functional and Adjoints of Inner Product Space *Sachin Kaushal, Lovely Professional University*	46
Unit 6:	Unitary Operators and Normal Operators *Sachin Kaushal, Lovely Professional University*	55
Unit 7:	Introduction and Forms on Inner Product Spaces *Richa Nandra, Lovely Professional University*	69
Unit 8:	Positive Forms and More on Forms *Richa Nandra, Lovely Professional University*	75
Unit 9:	Spectral Theory and Properties of Normal Operators *Sachin Kaushal, Lovely Professional University*	84
Unit 10:	Bilinear Forms and Symmetric Bilinear Forms *Sachin Kaushal, Lovely Professional University*	104
Unit 11:	Skew-symmetric Bilinear Forms *Sachin Kaushal, Lovely Professional University*	116
Unit 12:	Groups Preserving Bilinear Forms *Sachin Kaushal, Lovely Professional University*	120

Unit 1: The Jordan Form

CONTENTS

Objectives

Introduction

1.1 Overview

1.2 Jordan Form

1.3 Summary

1.4 Keywords

1.5 Review Questions

1.6 Further Readings

Objectives

After studying this unit, you will be able to:

- Understand the finite vector space V for a linear operator T can be written as a direct sum of the cyclic invariant subspaces $Z(\alpha_i, T)$.
- Know that the characteristic polynomial f of T decomposes as the product of the individual characteristic polynomial $p_i = x^{ki}$ for the r annihilators such that $k_1 \geq k_2 \geq \dots \geq k_r$. The minimal polynomial also has the form

$$p = (x - c_1)^{r_1} \dots (x - c_k)^{r_k}$$

- See that with the help of the companion matrix the linear operator represented by the matrix can be put into the Jordan form.

Introduction

In this unit the findings of the unit 20 are used to put any matrix A representing the linear operator into the Jordan form.

It is seen that by using the idea of the direct decomposition of the vector space into the sum of the cyclic subspaces the given matrix A can be shown to be similar to a Jordan matrix.

1.1 Overview

Suppose that N is a nilpotent linear operator on a finite-dimensional space. From Theorem 1 of the last unit we find that with N-annihilators $p_1, p_2, \dots, p_r$ for r non-zero vectors $\alpha_1, \alpha_2, \dots, \alpha_r$, V is decomposed as follows:

$$V = Z(\alpha_1, N) \oplus \cdots \oplus Z(\alpha_r, N)$$

Here p_{i+1} divides for $i = 1, \dots, r-1$. As N is nilpotent the minimal polynomial is x^K for $K \leq n$, thus each $p_i = x^{ki}$, such that

$$K_1 = K_1 \geq K_2 \geq \dots K_r$$

Notes

The companion matrix of x^{K_i} is the $K_i \times K_i$ matrix

$$A_i = \begin{bmatrix} 0 & 0 & \cdots & \cdots & 0 & 0 \\ 1 & 0 & \cdots & \cdots & 0 & 0 \\ 0 & 1 & \cdots & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{bmatrix} \qquad ...(1)$$

Thus Theorem 1 of unit 20 gives us an ordered basis for V in which the matrix of N is the direct sum of the elementary nilpotent matrices (1). Thus with a nilpotent $n \times n$ matrix we associate an integer r such that $k_1 + k_2 + ... + k_r = n$ and $k_i \geq k_{i+1}$ and which determines the rational form of matrix. The positive integer is precisely the nullity of N, as the null space has a basis the r vectors

$$N^{k_i - 1}\ \alpha_i \qquad ...(2)$$

For, let α be in the null space of N, we write α as

$$\alpha = f_1\alpha_1 + ... + f_r\alpha_r$$

where f_i is a polynomial, the degree of f_i is assumed to be less than k_i. Since $N\alpha = 0$ for each i we have

$$\begin{aligned} 0 &= N(f_i\alpha_i) \\ &= Nf_i(N)\alpha_i, \\ &= (xf_i)\ \alpha_i \end{aligned}$$

Thus $x\,f_i$ is divisible by x^k and since deg $(f_i) < k_i$, this means that

$$f_i = c_i x^{k_i - 1}$$

where c_i is some scalar. But then

$$\alpha = c_1(x^{k_1 - 1}\ \alpha_1) + ... + c_r(x^{k_r - 1}\ \alpha_r)$$

which shows that the vectors (2) form a basis for the null space of N.

1.2 Jordan Form

Now we combine our findings about nilpotent operators or matrices with the primary decomposition theorem of unit 18. Suppose that T is a linear operator on V and that the characteristic polynomials for T factors over F as follows:

$$f = (x - c_1)^{d_1} \cdots (x - c_k)^{d_k}$$

where $c_1,..., c_k$ are distinct elements of F and $d_i \geq 1$. Then the minimal polynomial for T will be

$$p = (x - c_1)^{r_1} \cdots (x - c_k)^{r_k}$$

where $1 \leq r_i \leq d_i$. If W_i is the null space of $(T - c_iI)^{r_i}$, then the primary decomposition theorem tells us that

$$V = W_1 \oplus \cdots \oplus W_k$$

and that the operator T_i induced on W_i by T has minimal polynomial $(x - c_i)^{r_i}$. Let N_i be the linear operator on W_i defined by $N_i = T - c_iI$. Then N_i is nilpotent and has minimal polynomial x^{r_i}. On W_i, T acts like N_i plus the scalar c_i times the identity operator. Suppose we choose a basis for the subspace W_i corresponding to the cyclic decomposition for the nilpotent operator N_i. Then the matrix of T_i in this ordered basis will be the direct sum of matrices

$$\begin{bmatrix} c & 0 & \cdots & 0 & 0 \\ 1 & c & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ & & & c & \\ 0 & 0 & \cdots & 1 & c \end{bmatrix} \qquad \ldots(3)$$

each with $c = c_i$. Furthermore, the sizes of these matrices will decrease as one reads from left to right. A matrix of the form (3) is called an elementary Jordan matrix with characteristic value c. Now if we put all the bases for the W_i together, we obtain an ordered basis for V. Let us describe the matrix A of T in this ordered basis.

The matrix A is the direct sum

$$A = \begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & A_k \end{bmatrix} \qquad \ldots(4)$$

of matrices $A_1, \ldots, A_k$. Each A_i is of the form

$$A_i = \begin{bmatrix} J_1^{(i)} & 0 & \cdots & 0 \\ 0 & J_2^{(i)} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & J_{n_i}^{(l)} \end{bmatrix}$$

where each $J_j^{(i)}$ is an elementary Jordan matrix with characteristic value c_i. Also, within each A_i, the sizes of the matrices $J_j^{(i)}$ decrease as j increases. An $n \times n$ matrix A which satisfies all the conditions described so far in this paragraph (for some distinct scalars $c_1, \ldots, c_k$) will be said to be in Jordan form.

We have just pointed out that if T is a linear operator for which the characteristic polynomial factors completely over the scalar field, then there is an ordered basis for V in which T is represented by a matrix which is in Jordan form. We should like to show now that this matrix is something uniquely associated with T, up to the order in which the characteristic values of T are written down.

The uniqueness we see as follows. Suppose there is some ordered basis for V in which T is represented by the Jordan matrix A described in the previous paragraph. If A_i is a $d_i \times d_i$ matrix, then d_i is clearly the multiplicity of c_i as a root of the characteristic polynomial for A, or for T. In other words, the characteristic polynomial for T is

$$f = (x - c_1)^{d_1} \ldots (x - c_k)^{d_k}$$

This shows that $c_j, \ldots, c_k$ and $d_1, \ldots, d_k$ are unique, up to the order in which we write them. The fact that A is the direct sum of the matrices A_i gives us a direct sum decomposition $V = W_1 \oplus \ldots \oplus W_k$ invariant under T. Now note that W_i must be the null space of $(T - c_iI)^n$, where $n = \dim V$; for, $A_i - c_iI$ is clearly nilpotent and $A_j - c_iI$ is non-singular for $j \neq i$. So we see that the subspaces W_i are unique. If T_i is the operator induced on W_i by T, then the matrix A_i is uniquely determined as the rational form for $(T_i \ldots c_iI)$.

Notes

Now we wish to make some further observations about the operator T and the Jordan matrix A which represents T in some ordered basis. We shall list a string of observations:

(1) Every entry of A not on or immediately below the main diagonal is 0. On the diagonal of A occur the k distinct characteristic values $c_1,..., c_k$ of T. Also, c_i is repeated d_i times, where d_i is the multiplicity of c_i as a root of the characteristic polynomial, i.e., d_i = dim W_i.

(2) For each i, the matrix A_i is the direct sum of n_i elementary Jordan matrices $J_j^{(i)}$ with characteristic values c_i. The number n_i is precisely the dimension of the space of characteristic vectors associated with the characteristic value c_i. For, n_i is the number of elementary nilpotent blocks in the rational form for $(T_i - c_iI)$, and is thus equal to the dimension of the null space of $(T - c_iI)$. In particular notice that T is diagonalizable if and only if $n_i = d_i$ for each i.

(3) For each i, the first block $J_1^{(t)}$ in the matrix A, is an $r_i \times r_i$ matrix, where r_i is the multiplicity of c_i as a root of the minimal polynomial for T. This follows from the fact that the minimal polynomial for the nilpotent operator $(T_i - c_iI)$ is x^{r_i}.

Of course we have as usual the straight matrix result. If B is an $n \times n$ matrix over the field F and if the characteristic polynomial for B factors completely over F, then B is similar over F to an $n \times n$ matrix A in Jordan form, and A is unique up to a rearrangement of the order of its characteristic values. We call A the Jordan form of B.

Also, note that if F is an algebraically closed field, then the above remarks apply to every linear operator on a finite-dimensional space over F, or to every $n \times n$ matrix over F. Thus, for example, every $n \times n$ matrix over the field of complex numbers is similar to an essentially unique matrix in Jordan form.

If the linear transformation T is nilpotent then $T^{n_1} = 0$ where n_1 is the index of nilpotency. If $T^{n_1 - 1} \neq 0$ we can find a vector v in the space V such that $T^{n_1 - 1} \neq 0$. Then we can form the vectors $v_1 = v$, $v_2 = T\,v$, $v_3 = T^2v$, … $v_{n_1} = T^{n_1 - 1}v$ vectors which are claimed to be linearly independent over the field F.

Let V_1 be the subspace of V spanned by $v_1 = v$, $v_2 = Tv$, … $v_{n_1} = T^{n_1-1}v$, V_1 is invariant under T, and in the basis above, the linear transformation induced by T on V_1 has a matrix A_{n_1} of the form (1).

Let the vector space V is of the form $V = V_1 \oplus W$ where W is invariant under T. Using the basis $v_1, v_2, \ldots v_{n_1}$ of V_1 and any basis of W as a basis of V, the matrix of T in this basis has the form

$$\begin{pmatrix} A_{n_1} & 0 \\ 0 & A_{n_2} \end{pmatrix}$$

where A_2 is the matrix of T_2, the linear transformation induced on W by T. Since $T^{n_1} = 0, T_2^{1/2} = 0$ for some $n_2 \leq n_1$.

Let T is a linear operator on C^2. The characteristic polynomial for T is either $(x - C_1)(x - C_2)$ where C_1 and C_2 are distinct or is $(x - C)^2$. In the former case T is diagonalizable and is represented in some ordered basis by the matrix

$$\begin{bmatrix} C_1 & 0 \\ 0 & C_2 \end{bmatrix}.$$

In the later case, the minimal polynomial for T may be $(x - C)$, in which case $T = C\,I$, or may be $(x - C)^2$, in which case T is represented in some order basis by the matrix

$$\begin{bmatrix} C & 0 \\ 1 & C \end{bmatrix}$$

Thus every 2 × 2 matrix over the field of complex numbers is similar to a matrix of one of the two types displayed above, possibly with $C_1 = C_2$.

Example 1: Let T be represented in ordered basis by the matrix

$$A = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \in F_3$$

The ordered basis is $\varepsilon_1 = (1, 0, 0)$, $\varepsilon_2 = (0, 1, 0)$, $\varepsilon_3 = (0, 0, 1)$

Let $\nu_1 = \varepsilon_1$, $\nu_2 = A\varepsilon_1 = \varepsilon_2 + \varepsilon_3$, $\nu_3 = \varepsilon_3$. In this basis

(ν_1, ν_2, ν_3) the matrix A becomes

$$A' = PAP^{-1}$$

where $$P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix},$$

A straight forward method gives

$$P^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix},$$

then $$A' = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

which is in Jordan form. Thus A is similar to A'.

Example 2: Let A be a complex 3 × 3 matrix

$$A = \begin{bmatrix} 2 & 0 & 0 \\ a & 2 & 0 \\ b & c & -1 \end{bmatrix}$$

The characteristic polynomial for A is obviously $(x - 2)^2 (x + 1)$. Either this is the minimal polynomial, in which case A is similar to

$$\begin{bmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

or the minimal polynomial is $(x - 2)(x + 1)$, in which case A is similar to

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

Now

$$(A-2I)(A+I)=\begin{bmatrix}0 & 0 & 0\\ 3a & 0 & 0\\ ac & 0 & 0\end{bmatrix}$$

and thus A is similar to a diagonal matrix if and only if $a = 0$.

Example 3: Let

$$A=\begin{bmatrix}2 & 0 & 0 & 0\\ 1 & 2 & 0 & 0\\ 0 & 0 & 2 & 0\\ 0 & 0 & a & 2\end{bmatrix}$$

The characteristic polynomial for A is $(x - 2)^4$. Since A is the direct sum of two 2×2 matrices, it is clear that the minimal polynomial for A is $(x - 2)^2$. Now if $a = 0$ or if $a = 1$, then the matrix A is in Jordan form. Notice that the two matrices we obtain for $a = 0$ and $a = 1$ have the same characteristic polynomial and the same minimal polynomial, but are not similar. They are not similar because for the first matrix the solution space of $(A - 2I)$ has dimension 3, while for the second matrix it has dimension 2.

Example 4: Linear differential equations with constant coefficients provide a nice illustration of the Jordan form. Let $a_0,\ldots, a_{n-1}$ be complex numbers and let V be the space of all n times differentiable functions f on an interval of the real line which satisfy the differential equation

$$\frac{d^n f}{dx^n}+a_{n-1}\frac{d^{n-1} f}{dx^{n-1}}+\cdots+a_1\frac{df}{dx}+a_0 f=0$$

Let D be the differentiation operator. Then V is invariant under D, because V is the null space of $p(D)$, where

$$p = x^n + \cdots + a_1 x + a_0$$

What is the Jordan form for the differentiation operator on V?

Let $c_1,\ldots, c_k$ be the distinct complex roots of p:

$$p = (x - c_1)^{r_1} f \cdots (x - c_k)^{r_k}$$

Let V_i be the null space of $(D - c_i I)^{r_i}$, that is, the set of solutions to the differential equation

$$(D - c_i I)^{r_i} f = 0$$

Then the primary decomposition theorem tells us that

$$V = V_1 \oplus \ldots \oplus V_k$$

Let N_i be the restriction of $D - c_i I$ to V_i. The Jordan form for the operator D (on V) is then determined by the rational forms for the nilpotent operators $N_1,\ldots, N_k$ on the spaces $V_1,\ldots, V_k$.

So, what we must know (for various values of c) is the rational form for the operator $N = (D - cI)$ on the space V_c, which consists of the solutions of the equation

$$(D - cI)^r f = 0$$

How many elementary nilpotent blocks will there be in the rational form for N? The number will be the nullity of N, i.e., the dimension of the characteristic space associated with the characteristic value c. That dimension is 1, because any function which satisfies the differential equation

$$Df = cf$$

is a scalar multiple of the exponential function $h(x) = e^{cx}$. Therefore, the operator N (on the space V_c) has a cyclic vector. A good choice for a cyclic vector is $g = x^{r-1}h$:

$$g(x) = x^{r-1}e^{cx}$$

This gives

$$\begin{aligned} Ng &= (r-1)x^{r-2}h \\ \vdots & \qquad \vdots \\ N^{r-1}g &= (r-1)!h \end{aligned}$$

The preceding paragraph shows us that the Jordan form for D (on the space V) is the direct sum of k elementary Jordan matrices, one for each root c_i.

Self Assessment

1. If A is an $n \times n$ matrix over the field F with characteristic polynomials

   $$f = (x - c_1)^{d_1} (x - c_2)^{d_2} \dots (x - c_k)^{d_k}$$

   What is the trace of A?

2. Show that the matrix

   $$A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix}$$

   is nilpotent. Show also that the Jordan form of A consists of a single 3×3 matrix.

1.3 Summary

- The findings of the theorem 1 of the last unit helps us to see that the finite vector space V for a linear nilpotent operator is decomposed as the direct sum of its cyclic invariant subspaces $Z(\alpha_i; N)$ with N annihilators $p_1, p_2, \dots, p_r$.
- Since N is nilpotent, the minimal polynomial is x^k where $k \le n$, and thus each p_i is also of the form $p_i = x^{k_i}$.
- Theorem 1 of the last unit also helps us to write N as the direct sum of the elementary nilpotent matrices known as companion matrices.

1.4 Keywords

Companion Matrix: is such an $n \times n$ matrix whose elements are zeros every where except immediately below the diagonal line has 1*s*.

Nilpotent Matrix: A matrix A such that $A^k = 0$, is called nilpotent matrix of index k. Provided $a^{k-1} \neq 0$.

1.5 Review Questions

Notes

1. The differentiation operator on the space of the polynomials of degree less than or equal to 3 is represented by the matrix

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

   What is the Jordan form of the matrix?

2. If A is a complex 5×5 matrix with the characteristic polynomial

$$f = (x - 2)^3 (x + 7)^2$$

   and the minimal polynomial $p = (x - 2)^2 (x + 7)$, what is the Jordan form for A?

Answer: Self Assessment

1. Trace of $A = c_1d_1 + c_2d_2 + ... + c_kd_k$

1.6 Further Readings

Books

Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I.N. Herstein, *Topics in Algebra*

Unit 2: Computation of Invariant Factors

CONTENTS

Objectives

Introduction

2.1 Overview

2.2 Computation of Invariant Factors

2.3 Summary

2.4 Keywords

2.5 Review Question

2 .6 Further Readings

Objectives

After studying this unit, you will be able to:

- Understand how to obtain the characteristic polynomial for a matrix of large size with the help of the elementary row and column operations.
- See that this unit gives a detailed method which can be used by computation of invariant factors as the matrix involved depends upon the polynomials in the field $F^n(x)$.
- See that with method of elementary row and column operations a matrix can be put into the Jordan form.
- Understand that if P is an $m \times m$ matrix with entries in the polynomial algebra $F(x)$ then P is invertible means that P is row equivalent to the $m \times m$ identity matrix and P is a product of elementary matrices.

Introduction

In this unit a method for computing the invariant factors $p_1, \ldots p_r$ is given where p_1, $p_2, \ldots p_r$ define the rational form for the $n \times n$ matrix A.

The elementary row operations and column operations are to be used to reduce $(xI - A)$ into an row equivalent matrix.

It is also shown that if N is row equivalent to M then $N = PM$, where P an $m \times m$ matrix is a product of elementary matrices.

2.1 Overview

We wish to find a method for computing the invariant factors $p_1, \; p_2, \ldots p_r$ which define the rational form for an $n \times n$ matrix A with entries in the field F. To begin with a very simple case in which A is the companion matrix (2) of unit 9 of a monic polynomial

$$p = x^n + C_{n-1} x^{n-1} + \ldots + C_1 x + C_0.$$

In unit (19) we saw that p is both the minimal and the characteristic polynomial for the companion matrix A. Now, we want to give a direct calculation which shows that p is the characteristic polynomial for A.

In this case

$$xI - A = \begin{bmatrix} x & 0 & 0 & \cdots & 0 & C_0 \\ -1 & x & 0 & \cdots & 0 & C_1 \\ 0 & -1 & x & \cdots & 0 & C_2 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \cdots & C_{n-2} \\ 0 & 0 & 0 & \cdots & -1 & x + C_{n-1} \end{bmatrix}$$

In the row-operation, let us add x times row n to row $(n - 1)$. This will remove the x in the $(n - 1, n - 1)$ place and still the determinant of $[xI - A]$ does not change. To continue, add x times the new row $(n - 1)$ to row $(n - 2)$. Continuing successively unit all of the x's on the main diagonal have been removed by that process, the result is the matrix

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & x^n + \ldots + C_1 x + C_0 \\ -1 & 0 & 0 & \cdots & 0 & x^{n-1} + \ldots + C_2 x + C_1 \\ 0 & -1 & 0 & \cdots & 0 & x^{n-2} + \ldots + C_3 x + C_2 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots\;\vdots\;\vdots\;\vdots\;\vdots\;\vdots \\ 0 & 0 & 0 & \cdots & 0 & x^2 + C_{n-1}x + C_{n-2} \\ 0 & 0 & 0 & \cdots & 01 & x + C_{n-1} \end{bmatrix}$$

which has the same determinant as $xI - A$. The upper right-hand entry of this matrix is the polynomial p. Now we use column operations to clean up the last columns. We do so by adding to last column appropriate multiples of the other columns:

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & p \\ -1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & -1 & 0 \end{bmatrix}$$

Multiply each of the first $(n - 1)$ columns by -1 and then perform $(n - 1)$ interchanges of adjacent columns to bring the present nth column to the first position. The total effect of the $2n - 2$ sign changes is to have the determinant unaltered. We obtain the matrix

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix} \qquad \ldots(1)$$

It is then clear that $p = \det(xI - A)$.

2.2 Computation of Invariant Factors

We are going to show that for any $n \times n$ matrix A, there is a succession of row and column operations which will transform $xI - A$ into a matrix, in which the invariant factors of A appear down the main diagonal.

Notes

We will be concerned with $F\overset{m \times n}{(x)}$, the collection of $m \times n$ matrices with entries which are polynomials over the field F. If M is such a matrix, an elementary row operation on M is one of the following:

1. multiplications of one row of M by a non-zero scalar in F;
2. replacement of the rth row of M by row r plus f times row s, where f is any polynomial over F and $r = s$;
3. interchange of two rows of M.

The inverse operation of an elementary row operation is an elementary row operation of the same type. Notice that we could not make such an assertion if we allowed non-scalar polynomials in (1). An $m \times m$ elementary matrix, that is, an elementary matrix in $F[x]^{m \times m}$, is one which can be obtained from the $m \times m$ identity matrix by means of a single elementary row operation. Clearly each elementary row operation on M can be effected by multiplying M on the left by a suitable $m \times m$ elementary matrix; in fact, if e is the operation, then

$$e(M) = e(I)M.$$

Let M, N be matrices in $F[x]^{m \times n}$. We say that N is row-equivalent to M if N can be obtained from M by a finite succession of elementary row operations:

$$M = M_0 \to M_1 \to \ldots \to M_k = N.$$

Evidently N is row-equivalent to M if and only if M is row-equivalent to N, so that we may use the terminology 'M and N are row-equivalent.' If N is row-equivalent to M, then

$$N = PM$$

where the $m \times m$ matrix P is a product of elementary matrices:

$$P = E_1 \ldots E_k.$$

In particular, P is an invertible matrix with inverse

$$P^{-1} = E_k^{-1} \ldots E_1^{-1}.$$

Of course, the inverse of E, comes from the inverse elementary row operation.

All of this is just as it is in the case of matrices with entries in F. Thus, the next problem which suggests itself is to introduce a row-reduced echelon form for polynomial matrices. Here, we meet a new obstacle. How do we row-reduce a matrix? The first step is to single out the leading non-zero entry of row 1 and to divide every entry of row 1 by that entry. We cannot (necessarily) do that when the matrix has polynomial entries. As we shall see in the next theorem, we can circumvent this difficulty in certain cases; however, there is not any entirely suitable row-reduced form for the general matrix in $F[x]^{m \times n}$. If we introduce column operations as well and study the type of equivalence which results from allowing the use of both types of operations, we can obtain a very useful standard form for each matrix. The basic tool is the following.

Lemma: Let M be a matrix in $F[x]^{m \times n}$ which has some non-zero entry in its first column, and let p be the greatest common divisor of the entries in column 1 of M. Then M is row-equivalent to a matrix N which has

$$\begin{bmatrix} p \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

as its first column.

Proof: We shall prove something more than we have stated. We shall show that there is an algorithm for finding N, i.e., a prescription which a machine could use to calculate N in a finite number of steps. First, we need some notation.

Let M be any $m \times n$ matrix with entries in $F[x]$ which has a non-zero first column

$$M_1 = \begin{bmatrix} f_1 \\ \vdots \\ f_m \end{bmatrix}$$

Define

$$l(M_1) = \min_{f_i \neq 0} \deg f_i$$
$$p(M_1) = \text{g.c.d.}\ (f_1, \dots f_m) \qquad \dots(2)$$

Let j be some index such that $\deg f_j, = l(M_1)$. To be specific, let j be the smallest index i for which $\deg f_i, = l(M_1)$. Attempt to divide each f, by f_j:

$$f_i = f_j g_i, + r_i, \qquad r_i = 0 \ \text{ or } \ \deg r_i < \deg f_j \qquad \dots(3)$$

For each i different from j, replace row i of M by row i minus g_i times row j. Multiply row j by the reciprocal of the leading coefficient of f_j and then interchange rows j and 1. The result of all these operations is a matrix M' which has for its first column

$$M_1' = \begin{bmatrix} \hat{f}_j \\ r_2 \\ \vdots \\ r_{j-1} \\ r_1 \\ r_{j+1} \\ \vdots \\ r_m \end{bmatrix} \qquad \dots(4)$$

where $\hat{f}_j$ is the monic polynomial obtained by normalizing f_j to have leading coefficient 1. We have given a well-defined procedure for associating with each M a matrix M' with these properties.

(a) M' is row-equivalent to M.

(b) $p(M_1') = p(M_1)$.

(c) Either $l(M_1') < l(M_1)$ or

$$M_1' = \begin{bmatrix} p(M_1) \\ 0 \\ \vdots \\ 0 \end{bmatrix} \qquad \dots(4A)$$

It is easy to verify (b) and (c) from (3) and (4). Property (c) is just another way of stating that either there is some i such that $r, \neq 0$ and $\deg r_i, < \deg f_j,$ or else $r_i, = 0$ for all i and $\hat{f}_j$ is (therefore) the greatest common divisor of $f_1, \dots, f_m$.

The proof of the lemma is now quite simple. We start with the matrix M and apply the above procedure to obtain M'. Property (c) tells us that either M' will serve as the matrix N in the lemma or $l(M_1') < l(M_1)$. In the latter case, we apply the procedure to M' to obtain the matrix

$M^{(2)} = (M')'$. If $M^{(2)}$ is not a suitable N, we form $M^{(3)} = M^{(2)})'$, and so on. The point is that the strict inequalities

$$l(M_i) > l(M'_1) > l(M_1^{(2)} > \ldots$$

cannot continue for very long. After not more than $l(M_1)$ iterations of our procedure, we must arrive at a matrix $M^{(k)}$ which has the properties we seek.

Theorem 1: Let P be an $m \times m$ matrix with entries in the polynomial algebra $F[x]$. The following are equivalent.

(i) P is invertible.

(ii) The determinant of P is a non-zero scalar polynomial.

(iii) P is row-equivalent to the $m \times m$ identity matrix.

(iv) P is a product of elementary matrices.

Proof: Certainly (i) implies (ii) because the determinant function is multiplicative and the only polynomials invertible in $F[x]$ are the non-zero scalar ones. Our argument here provides a proof that (i) follows from (ii). We shall complete the merry-go-round

$$\begin{array}{ccc} \text{(i)} & \rightarrow & \text{(ii)} \\ \uparrow & & \downarrow \\ \text{(iv)} & \leftarrow & \text{(iii).} \end{array}$$

The only implication which is not obvious is that (iii) follows from (ii).

Assume (ii) and consider the first column of P. It contains certain polynomials $p_1, \ldots, p_m$, and

$$\text{g.c.d.}\ (p_1, \ldots, p_m) = 1$$

because any common divisor of $p_1, \ldots, p_m$. must divide (the scalar) det P. Apply the previous lemma to P to obtain a matrix

$$Q = \begin{bmatrix} 1 & a_2 & \cdots & a_m \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{bmatrix} \qquad \ldots(5)$$

which is row-equivalent to P. An elementary row operation changes the determinant of a matrix by (at most) a non-zero scalar factor. Thus det Q is a non-zero scalar polynomial. Evidently the $(m - 1) \times (m - 1)$ matrix B in (5) has the same determinant as does Q. Therefore, we may apply the last lemma to B. If we continue this way for m steps, we obtain an upper-triangular matrix

$$R = \begin{bmatrix} 1 & a_2 & \cdots & a_m \\ 0 & 1 & \cdots & b_m \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

which is row-equivalent to R. Obviously R is row-equivalent to the $m \times m$ identity matrix.

Corollary: Let M and N be $m \times n$ matrices with entries in the polynomial algebra $F]x]$. Then N is row-equivalent to M if and only if

$$N = PM$$

where P is an invertible $m \times m$ matrix with entries in $F[x]$.

Notes

We now define elementary column operations and column-equivalence in a manner analogous to row operations and row-equivalence. We do not need a new concept of elementary matrix because the class of matrices which can be obtained by performing one elementary column operation on the identity matrix is the same as the class obtained by using a single elementary row operation.

Definition: The matrix N is equivalent to the matrix M if we can pass from M to N by means of a sequence of operations

$$M = M_0 \to M_1 \to \ldots \to M_k = N$$

each of which is an elementary row operation or an elementary column operation.

Theorem 2: Let M and N be $m \times n$ matrices with entries in the polynomial algebra $F[x]$. Then N is equivalent to M if and only if

$$N = PMQ$$

where P is an invertible matrix in $F[x]^{m \times m}$ and Q is an invertible matrix in $F[x]^{n \times n}$.

Theorem 3: Let A be an $n \times n$ matrix with entries in the field F, and let $p_1, \ldots, p_r$ be the invariant factors for A. The matrix $xI - A$ is equivalent to the $n \times n$ diagonal matrix with diagonal entries $p_1, \ldots, p_r, 1, 1, \ldots, 1$.

Proof: There exists an invertible $n \times n$ matrix P, with entries in F, such that PAP^{-1} is in rational form, that is, has the block form

$$PAP^{-1} = \begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_r \end{bmatrix}$$

where A_i is the companion matrix of the polynomial p_i. According to Theorem 2, the matrix

$$P(xI - A)P^{-1} = xI - PAP^{-1} \qquad \ldots(6)$$

is equivalent to $xI - A$. Now

$$xI - PAP^{-1} = \begin{bmatrix} xI - A_1 & 0 & \cdots & 0 \\ 0 & xI - A_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & xI - A_r \end{bmatrix} \qquad \ldots(7)$$

where the various I's we have used are identity matrices of appropriate sizes. At the beginning of this section, we showed that $xl - A$, is equivalent to the matrix

$$\begin{bmatrix} p_i & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}.$$

From (6) and (7) it is then clear that $xl - A$ is equivalent to a diagonal matrix which has the polynomials p_i, and $(n - r)$ 1's on its main diagonal. By a succession of row and column interchanges, we can arrange those diagonal entries in any order we choose. For example: $p_1, \ldots, p_r, 1, \ldots, 1$.

Theorem 3 does not give us an effective way of calculating the elementary divisors $p_1, \ldots, p_r$ because our proof depends upon the cyclic decomposition theorem. We shall now give an explicit algorithm for reducing a polynomial matrix to diagonal form. Theorem 3 suggests that we may also arrange that successive elements on the main diagonal divide one another.

Definition: Let N be a matrix in $F[x]^{m \times n}$. We say that N is in (Smith) normal form if

(a) every entry off the main diagonal of N is 0;

(b) on the main diagonal of N there appear (in order) polynomials $f_1, \ldots, f_l$ such that f_k divides f_{k+j}, $1 \le k \le l - 1$.

In the definition, the number l is $l = \min(m, n)$. The main diagonal entries are $f_k = N_{kk}$, $k = 1, \ldots, l$.

Theorem 4: Let M be an $m \times n$ matrix with entries in the polynomial algebra $F[x]$. Then M is equivalent to a matrix N which is in normal form.

Proof: If $M = 0$, there is nothing to prove. If $M \neq 0$, we shall give an algorithm for finding a matrix M' which is equivalent to M and which has the form

$$M' = \begin{bmatrix} f_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & R & \\ 0 & & & \end{bmatrix} \qquad \ldots(8)$$

where R is an $(m - 1) \times (n - 1)$ matrix and f_1 divides every entry of R. We shall then be finished, because we can apply the same procedure to R and obtain f_2, etc.

Let $l(M)$ be the minimum of the degrees of the non-zero entries of M. Find the first column which contains an entry with degree $l(M)$ and interchange that column with column 1. Call the resulting matrix $M^{(0)}$. We describe a procedure for finding a matrix of the form

$$\begin{bmatrix} g & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & S & \\ 0 & & & \end{bmatrix} \qquad \ldots(9)$$

which is equivalent to $M^{(0)}$. We begin by applying to the matrix $M^{(0)}$ the procedure of the lemma before Theorem 1, a procedure which we shall call PL6. There results a matrix

$$M^{(1)} = \begin{bmatrix} p & a & \cdots & b \\ 0 & c & \cdots & d \\ \vdots & \vdots & & \vdots \\ 0 & e & \cdots & f \end{bmatrix} \qquad \ldots(10)$$

If the entries $a, \ldots, b$ are all 0, fine. If not, we use the analogue of PL6 for the first row, a procedure which we might call PL6'. The result is a matrix

$$M^{(2)} = \begin{bmatrix} q & 0 & \cdots & 0 \\ a' & c' & \cdots & e' \\ \vdots & \vdots & & \vdots \\ b' & d' & \cdots & f' \end{bmatrix} \qquad \ldots(11)$$

where q is the greatest common divisor of $p, a, \ldots, b$. In producing $M^{(2)}$, we may or may not have disturbed the nice form of column 1. If we did, we can apply PL6 once again. Here is the point. In not more than $l(M)$ steps:

$$M^{(0)} \xrightarrow{\text{PL6}} M^{(1)} \xrightarrow{\text{PL6}'} M^{(2)} \ldots \xrightarrow{\text{PL6}} M^{(t)}$$

we must arrive at a matrix $M^{(t)}$ which has the form (9): because at each successive step we have $l(M^{(k+1)} < l(M^{(k)}$. We name the process which we have just defined P7-36.

$$M^{(0)} \xrightarrow{\text{PL-36}} M^{(t)}$$

In (9), the polynomial g may or may not divide every entry of S. If it does not, find the first column which has an entry not divisible by g and add that column to column 1. The new first column contains both g and an entry $gh + r$ where $r \neq 0$ and $\deg r < \deg g$. Apply process P7-36 and the result will be another matrix of the form (9), where the degree of the corresponding g has decreased.

It should now be obvious that in a finite number of steps we will obtain (8), i.e., we will reach a matrix of the form (9) where the degree of g cannot be further reduced.

We want to show that the normal form associated with a matrix M is unique. Two things we have seen provide clues as to how the polynomials $f_1 ..., f_1$ in Theorem 4 are uniquely determined by M. First, elementary row and column operations do not change the determinant of a square matrix by more than a non-zero scalar factor. Second, elementary row and column operations do not change the greatest common divisor of the entries of a matrix.

Definition: Let M be an $m \times n$ matrix with entries in $F[x]$. If $1 \leq k \leq \min(m, n)$, we define $\delta_k(M)$ to be the greatest common divisor of the determinants of all $k \times k$ submatrices of M.

Recall that a $k \times k$ submatrix of M is one obtained by deleting some $m - k$ rows and some $n - k$ columns of M. In other words, we select certain k-tuples

$$I = (i_1, ..., i_k), \qquad 1 \leq i_1 < ... < i_k \leq m$$

$$J = (j_1, ..., j_k), \qquad 1 \leq j_1, < ... < j_k \leq n$$

and look at the matrix formed using those rows and columns of M. We are interested in the determinants

$$D_{I, J}(M) = \det \begin{bmatrix} M_{i_1 j_1} & \cdots & M_{i_1 j_k} \\ \vdots & & \vdots \\ M_{i_k j_1} & \cdots & M_{i_k j_k} \end{bmatrix} \qquad ...(12)$$

The polynomial $\delta_k(M)$ is the greatest common divisor of the polynomials $D_{I, J}(M)$, as I and J range over the possible k-tuples.

Theorem 5: If M and N are equivalent $m \times n$ matrices with entries in $F[x]$, then

$$\delta_k(M) = \delta_k(N), \quad 1 \leq k \leq \min(m, n) \qquad ...(13)$$

Proof: It will suffice to show that a single elementary row operation e does not change δ_k. Since the inverse of e is also an elementary row operation, it will suffice to show this: If a polynomial f divides every $D_{I, J}(M)$, then f divides $D_{I, J}(e(M))$ for all k-tuples I and J.

Since we are considering a row operation, let $\alpha_1, ..., \alpha_m$ be the rows of M and let us employ the notation

$$D_J(\alpha_{i_1} ..., \alpha_{i_k}) = D_{I, J}(M).$$

Given I and J, what is the relation between $D_{I, J}(M)$ and $D_{I, J}(e(M))$? Consider the three types of operations e:

(a) multiplication of row r by a non-zero scalar c;

(b) replacement of row r by row r plus g times row s, $r \neq s$;

(c) interchange of rows r and s, $r \neq$ s.

Notes

Forget about type (c) operations for the moment, and concentrate on types (a) and (b), which change only row r. If r is not one of the indices $i_1, \ldots, i_k$, then

$$D_{I', J}(e(M)) = D_{I', J}(M).$$

If r is among the indices $i_1, \ldots, i_k$, then in the two cases we have

(a) $\quad D_{I', J}(e(M)) = D_J(\alpha_{i1}, \ldots, c\alpha_r, \ldots, \alpha_{ik})$

$$= cD_J(\alpha_{i1}, \ldots, \alpha_r, \ldots, \alpha_{ik})$$

$$= cD_{I, J}(M);$$

(b) $\quad D_{I, J}(e(M)) = D_J(\alpha_{i1}, \ldots, \alpha_r + g\alpha_s, \ldots, \alpha_{ik})$

$$= D_{I, J}(M) + gD_J(\alpha_{i1}, \ldots, \alpha_s, \ldots, \alpha_{ik})$$

For type (a) operations, it is clear that any f which divides $D_{I,J}(M)$ also divides $D_{I',J}(e(M))$. For the case of a type (c) operation, notice that

$$D_J(\alpha_{i1}, \ldots, \alpha_s, \ldots, \alpha_{ik}) = 0, \qquad \text{if } s = i, \text{ for some } j$$

$$D_J(\alpha_{i1}, \ldots, \alpha_s \ldots, \alpha_{ik}) = \pm D'_{I\,.\,J}(M), \qquad \text{if } s \neq i, \text{ for all } j.$$

The I' in the last equation is the k-tuple $(i_1, \ldots, s, \ldots, i_k)$ arranged in increasing order. It should now be apparent that, if f divides every $D_{I,J}(M)$, then f divides every $D_{I,J}(e(M))$.

Operations of type (c) can be taken care of by roughly the same argument or by using the fact that such an operation can be effected by a sequence of operations of types (a) and (b).

Corollary: Each matrix M in $F[x]^{m \times n}$ is equivalent to precisely one matrix N which is in normal form. The polynomials $f_1, \ldots, f_k$ which occur on the main diagonal of N are

$$f_k = \frac{\delta_k(M)}{\delta_{k-1}(M)}, \quad 1 \leq k \leq \min(m, n)$$

where, for convenience, we define $\delta_0(M) = 1$.

Proof: If N is in normal form with diagonal entries $f_1, \ldots, f_k$; it is quite easy to see that

$$\delta_k(N) = f_1 f_2 \ldots f_k.$$

Of course, we call the matrix N in the last corollary the normal form of M. The polynomials $f_1, \ldots, f_k$ are often called the invariant factors of M.

Suppose that A is an $n \times n$ matrix with entries in F, and let $p_1, \ldots, p_r$ be the invariant factors for A. We now see that the normal form of the matrix $xI - A$ has diagonal entries $1, 1, \ldots, 1, p_r, \ldots, p_1$. The last corollary tells us what $p_1, \ldots, p_r$ are, in terms of submatrices of $xI - A$. The number $n - r$ is the largest k such that $\delta_k(xI - A) = 1$. The minimal polynomial p_1 is the characteristic polynomial for A divided by the greatest common divisor of the determinants of all $(n - 1) \times (n - 1)$ submatrices of $xI - A$, etc.

Self Assessment

1. True or false? Every matrix in $F^{n \times n}$ is row-equivalent to an upper-triangular matrix.
2. T be a linear operator on a finite dimensional vector space and let A be the matrix of T in some ordered basis. Show that T has a cyclic vector if and only if the determinants of the $(n - 1)$ $(n - 1)$ sub-matrices of $(xI - A)$ are relatively prime.

2.3 Summary

Notes

- In this unit a method for computing the invariant factors $p_1 \ldots p_r$ which define the rational form of the matrix, is given. It is shown that by elementary row and column operations it can be achieved.
- It is shown that if N is row-equivalent to a matrix M then $N = PM$ where p is a product of elementary matrices.
- By this method one can show that

$$P(xI - A)\,P^{-1} = xI - PAP^{-1} = \begin{bmatrix} xI - A_1 & 0 & \cdots & 0 \\ 0 & xI - A_2 & \cdots & 0 \\ \vdots & & & \\ 0 & \cdots & \cdots & xI - A_r \end{bmatrix}$$

where A_i is companion matrix.

2.4 Keywords

An Elementary Matrix in $F^{n \times n}(x)$ is one which can be obtained from $n \times n$ identity matrix by means of a single elementary operation.

An Elementary Row Operation: An elementary row operation on a matrix M whose determinant has to be found, will not change the determinant of M if this row operation is one of the following: (i) multiplication of one row of M by a non-zero scalar in F; (ii) replacement of the rth row of M by the row r plus f times row s, where f is any polynomial over F and $r \neq s$; (iii) interchange of two rows of M.

Row equivalent: Let M, N be matrices in $F^{m \times m}(x)$. We say that N is row equivalent to M if N can be obtained from M by a finite succession of elementary row operations.

2.5 Review Question

1. Let T be the linear operator on R^8 which is represented in the standard basis by the matrix

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & -1 & -1 & -1 & -1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

   (a) Find the characteristic polynomial and the invariant factors.

   (b) Find the Jordan form of A.

   (c) Find a direct sum decomposition of R^8 into T-cyclic subspaces as in theorem 1 of unit 20.

Answer: Self Assessment

1. True

2.6 Further Readings

Books Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I.N. Herstein, *Topics in Algebra*

Unit 3: Semi-simple Operators

Notes

CONTENTS

Objectives

Introduction

3 .1 Overview

3 .2 Semi-simple Operators

3 .3 Summary

3 .4 Keywords

3 .5 Review Questions

3 .6 Further Readings

Objectives

After studying this unit, you will be able to:

- Understand the meaning of semi-simple linear operator T by means of a few lemma stated in this unit.
- See that if T is a linear operator on V and the minimal polynomial for T is irreducible over the scalar field then T is semi-simple.
- Know that T, a linear operator on a finite-dimensional space is semi-simple if and only if T is diagonalizable.
- Understand that if T is a linear operator on V, a finite dimensional vector space over F a subfield of the field of complex numbers, then there is a semi-simple operator S and a nilpotent operator N on V such that $T = S + N$ and $SN = NS$.

Introduction

In this unit the outcome of the last few units is reviewed and a few lemmas based on these ideas are proved.

The criteria for an operator to be semi-simple are given. It is shown that a linear operator on finite dimensional space having minimal polynomial to be irreducible is semi-simple.

It is also shown that for a linear operator T on a finite dimensional vector space V over the field F which is subfield of the field of complex numbers, the operator is the sum of a semi-simple operator S on V and a nilpotent operator N on V such that $T = S + N$ and $SN = NS$.

3.1 Overview

In the last couple of units we have been dealing with a single linear operator T on a finite dimensional vector space V. The aim has been to decompose T into a direct sum of linear operators of an elementary nature.

We first of all studied the characteristic values and characteristic vectors and also constructed diagonalizable operators. It was observed then that the characteristic vectors of T need not space the space.

Then the cyclic decomposition theorem help us in expressing any linear operator as a direct sum of operators with a cyclic vector. If U is a linear operator with a cyclic vector, there is a basis $(\alpha_1, \alpha_2, ..., \alpha_n)$ with

$$U\alpha_i = \alpha_{i+1} \quad i = 1, ... n-1,$$

$$U\alpha_n = -c_0\alpha_1 - c_1\alpha_1, ... -c_{n-1}\alpha_n.$$

This means that action of U on this basis is to shift each α_i to the next vector α_{j+1}, except that $U\alpha_n$ is some prescribed linear combination of the vectors in the basis. The general operator T is the direct sum of a finite number of such operators U and got reasonably elementary description of the action of T. Then cyclic decomposition theorem to nilpotent operators is applied and with the help of the primary decomposition theorem Jordan form is obtained.

The importance of the rational form or the Jordan form is obtained from the fact that these forms can be computed in specific cases. Of course, if one is given a specific linear operator T and if its cyclic or Jordan form can be computed, one can obtain vast amounts of information about T. However there are some difficulties in this method. At first the computation may be lengthy. The other difficulty is there may not be any method for doing computations. In the case of rational form the difficulty may be due to lengthy calculation. It is also worthwhile to mention a theorem which states that if T is a linear operator on a finite-dimensional vector space over an algebraically closed field then T is uniquely expressible as the sum of a diagonalizable operator and a nilpotent operate which commute.

In this unit we shall prose analogous theorem without assuming that the scalar field is algebraically closed. We begin by defining the operators which will play the role of the diagonalizable operators.

3.2 Semi-simple Operators

We say that T a linear operator on a finite dimensional space V over the field F, is semi-simple if every T-invariant subspace has a complementary T-invariant subspace.

We are going to characterize semi-simple operators by means of their minimal polynomials, and this characterization will show us, that, when F is algebraically closed, an operator is semi-simple if and only it is diagonalizable.

Lemma: Let T be a linear operator on the finite dimensional vector space V and let

$$V = W_1 \oplus ... + W_k$$

be the primary decomposition for T. In other words, if p is the minimal polynomial for T and $p = p_1^{r_1} ... p_k^{r_k}$ is the prime factorization of p, then W_j is the null space of $p_j(T)^{r_j}$. Let W be any subspace of V which is invariant under T. Then

$$W = (W \cap W_1) \oplus ... \oplus (W \cap W_k)$$

Proof: If $E_1, E_2, ... E_k$ the projections associated with the decomposition $V = W_1 \oplus ... \oplus W_k$, then each E_j is a polynomial in T. That is, there are polynomials $h_1, ..., h_k$ such that $E_j = h_j(T)$.

Now let W be a subspace which is invariant under T. If α is any vector in W, then $\alpha = \alpha_1 + ... + \alpha_k$, where α_j is in W_j. Now $\alpha_j = E_j\alpha = h_j(T)\alpha$, and since W is invariant under T, each α_j is also in W. Thus each vector α in W is of the form $\alpha = \alpha_1 + ... + \alpha_k$, where α_j is in the intersection $W \cap W_j$. This expression is unique, since $V = W_1 \oplus ... \oplus W_k$. Therefore

$$W = (W \cap W_1) \oplus ... \oplus (W \cap W_k)$$

Lemma: Let T be a linear operator on V, and suppose that the minimal polynomial for T is irreducible over the scalar field F. Then T is semi-simple.

Proof: Let W be a subspace of V which is invariant under T. We must prove that W has a complementary T-invariant subspace. According to corollary of Theorem 1 of unit 20 it will suffice to prove that if f is a polynomial and β is a vector in V such that $f(T)\beta$ is in W, then there is a vector α in W with $f(T)\beta = f(T)\alpha$. So suppose β is in V and f is a polynomial such that $f(T)\beta$ is in W. If $f(T)\beta = 0$, we let $\alpha = 0$ and then α is a vector in W with $f(T)\beta = f(T)\alpha$. If $f(T)\beta \neq 0$, the polynomial f is not divisible by the minimal polynomial p of the operator T. Since p is prime, this means that f and p are relatively prime, and there exist polynomials g and h such that $fg + ph = 1$. Because $p(T) = 0$, we then have $f(T)g(T) = I$. From this it follows that the vector β must itself be in the subspace W; for

$$\begin{aligned}\beta &= g(T)f(T)\beta \\ &= g(T)(f(T)\beta)\end{aligned}$$

while $f(T)\beta$ is in W and W is invariant under T. Take $\alpha = \beta$.

Theorem 1: Let T be a linear operator on the finite-dimensional vector space V. A necessary and sufficient condition that T be semi-simple is that the minimal polynomial p for T be of the form $p = p_1 \dots p_k$, where $p_1, \dots , p_k$ are distinct irreducible polynomials over the scalar field F.

Proof: Suppose T is semi-simple. We shall show that no irreducible polynomial is repeated in the prime factorization of the minimal polynomial p. Suppose the contrary. Then there is some non-scalar monic polynomial g such that g^2 divides p. Let W be the null space of the operator $g(T)$. Then W is invariant under T. Now $p = g^2h$ for some polynomial h. Since g is not a scalar polynomial, the operator $g(T)h(T)$ is not the zero operator, and there is some vector β in V such that $g(T)h(T)\beta \neq 0$, i.e., $(gh)\beta \neq 0$. Now $(gh)\beta$ is in the subspace W, since $g(gh\beta) = g^2h\beta = p\beta = 0$. But there is no vector α in W such that $gh\beta = qh\alpha$; for, if α is ill W

$$(gh)\alpha = (hg)\alpha = h(g\alpha) = h(0) = 0.$$

Thus, W cannot have a complementary T-invariant subspace, contradicting the hypothesis that T is semi-simple.

Now suppose the prime factorization of p is $p = p_1 \dots p_k$, where $p_1, \dots , p_k$ are distinct irreducible (non-scalar) monic polynomials. Let W be a subspace of V which is invariant under T. We shall prove that W has a complementary T-invariant subspace. Let $V = W_1 \oplus \dots \oplus W_k$ be the primary decomposition for T, i.e., let W_j be the null space of $p_j(T)$. Let T_j be the linear operator induced on W_j by T, so that the minimal polynomial for T_j is the prime p_j. Now $W \cap W_j$ is a subspace of W_j which is invariant under T_j (or under T). By the last lemma, there is a subspace V_j of W_j such that $W_j = (W \cap W_j) \oplus V_j$ and V_j is invariant under T_j (and hence under T). Then we have

$$\begin{aligned}V &= W_1 \oplus \dots \oplus W_k \\ &= (W \cap W_1) \oplus V_1 \oplus \dots \oplus (W \cap W_k) \oplus V_k \\ &= (W \cap W_1) + \dots + (W \cap W_k) \oplus V_1 \oplus \dots \oplus V_k.\end{aligned}$$

By the first lemma above, $W = (W \cap W_1) \oplus \dots \oplus (W \cap W_k)$ so that if $W' = V_1 \oplus \dots \oplus V_k$, then $V = W \oplus W'$ and W' is invariant under T.

Corollary: If T is a linear operator on a finite-dimensional vector space over an algebraically closed field, then T is semi-simple if and only if T is diagonalizable.

Proof: If the scalar field F is algebraically closed, the monic primes over F are the polynomials $x - c$. In this case, T is semi-simple if and only if the minimal polynomial for T is $p = (x - c_1) \dots (x - c_k)$, where $c_1, \dots , c_k$ are distinct elements of F. This is precisely the criterion for T to be diagonalizable.

We turn now to expressing a linear operator as the sum of a semi-simple operator and a nilpotent operator which commute. In this, we shall restrict the scalar field to a subfield of the complex

Notes

numbers. We will see that what is important is that the field F be a field of characteristic zero, that is, that for each positive integer n the sum 1 + ... + 1 (n times) in F should not be 0. For a polynomial f over F, we denote by $f^{(k)}$ the kth formal derivative of f. In other words, $f^{(k)} = D^k f$, where D is the differentiation operator on the space of polynomials. If g is another polynomial, $f(g)$ denotes the result of substituting g in f, i.e., the polynomial obtained by applying f to the element g in the linear algebra $F[x]$.

Lemma (Taylor's Formula): Let F be a field of characteristic zero and let g and h be polynomials over F. If f is any polynomial over F with deg $f \le n$, then

$$f(g) = f(h) + f^{(1)}(h)(g - h) + \frac{f^{(2)}(h)}{2!}(g - h)^2 + \ldots + \frac{f^{(n)}(h)}{n!}(g - h)^n,$$

Proof: What we are proving is a generalized Taylor formula. The reader is probably used to seeing the special case in which $h = c$, a scalar polynomial, and $g = x$. Then the formula says

$$f = f(x) = f(c) + f^{(1)}(c)(x - c) + \frac{f^{(2)}(c)}{2!}(x - c)^2 + \ldots + \frac{f^{(n)}(c)}{n!}(x - c)^n$$

The proof of the general formula is just an application of the binomial theorem

$$(a + b)^k = a^k + ka^{k-1}b + \frac{k(k-1)}{2!}a^{k-2}b^2 + \ldots + b^k.$$

Since substitution and differentiation are linear processes, one need only prove the formula when $f = x^k$. The formula for $f = \sum_{k=0}^{n} c_k x^k$ follows by a linear combination. In the case $f = x^k$ with $k \le n$, the formula says

$$g^k = h^k + kh^{k-1}(g - h) + \frac{k(k-1)}{2!}h^{k-2}(g - h)^2 + \ldots + (g - h)^k$$

which is just the binomial expansion of

$$g^k = [h + (g - h)]^k.$$

Lemma: Let F be a subfield of the complex numbers, let f be a polynomial over F, and let f' be the derivative of f. The following are equivalent:

(a) f is the product of distinct polynomials irreducible over F.

(b) f and f' are relatively prime.

(c) As a polynomial with complex coefficients, f has no repeated root.

Proof: Let us first prove that (a) and (b) are equivalent statements about f. Suppose in the prime factorization of f over the field F that some (non-scalar) prime polynomial p is repeated. Then $f = p^2h$ for some h in $F[x]$. Then

$$f' = p^2h' + 2pp'h$$

and p is also a divisor of f'. Hence f and f' are not relatively prime. We conclude that (b) implies (a).

Now suppose $f = p_1 \ldots p_k$, where $p_1, \ldots, p_k$ are distinct non-scalar irreducible polynomials over F. Let $f_j = f/p_j$. Then

$$f' = P_1' f_1 + P_2' f_2 + \ldots + P_k' f_k$$

Let p be a prime polynomial which divides both f and f'. Then $p = p_i$, for some i. Now p_i divides f_j for $j \ne i$, and since p_i also divides

Notes

$$f' = \sum_{j=1}^{n} p_j' f_j$$

we see that p_i must divide $p_i' f_i$. Therefore p_i divides either f_i or p_i'. But p_i does not divide f_i, since p_1, ... , p_k are distinct. So p_i divides p_i'. This is not possible, since p_i' has degree one less than the degree of p_i. We conclude that no prime divides both f and f', or that $(f, f') = 1$.

To see that statement (c) is equivalent to (a) and (b), we need only observe the following: Suppose f and g are polynomials over F, a subfield of the complex numbers. We may also regard f and g as polynomials with complex coefficients. The statement that f and g are relatively prime as polynomials over F is equivalent to the statement that f and g are relatively prime as polynomials over the field of complex numbers. We use this fact with $g = f'$. Note that (c) is just (a) when f is regarded as a polynomial over the field of complex numbers. Thus (b) and (c) are equivalent, by the same argument that we used above.

Theorem 2: Let F be a subfield of the field of complex numbers, let V be a finite-dimensional vector space over F, and let T be a linear operator on V. Let $\mathcal{B}$ be an ordered basis for V and let A be the matrix of T in the ordered basis $\mathcal{B}$. Then T is semi-simple if and only if the matrix A is similar over the field of complex numbers to a diagonal matrix.

Proof: Let p be the minimal polynomial for T. According to Theorem 1, T is semi-simple if and only if $p = p_1 \ldots p_k$ where $p_1, \ldots , p_k$, are distinct irreducible polynomials over F. By the last lemma, we see that T is semi-simple if and only if p has no repeated complex root.

Now p is also the minimal polynomial for the matrix A. We know that A is similar over the field of complex numbers to a diagonal matrix if and only if its minimal polynomial has no repeated complex root. This proves the theorem.

Theorem 3: Let F be a subfield of the field of complex numbers, let V be a finite-dimensional vector space over F, and let T be a linear operator on V. There is a semi-simple operator S on V and a nilpotent operator N on V such that

(i) $T = S + N$;

(ii) $SN = NS$.

Furthermore, the semi-simple S and nilpotent N satisfying (i) and (ii) are unique, and each is a polynomial in T.

Proof: Let $p_1^{r_1} \cdots p_k^{r_k}$ be the prime factorization of the minimal polynomial for T, and let $f = p_1 \ldots p_k$. Let r be the greatest of the positive integers $r_1, \ldots , r_k$. Then the polynomial f is a product of distinct primes, f^r is divisible by the minimal polynomial for T, and so

$$f(T)^r = 0.$$

We are going to construct a sequence of polynomials: $g_0, g_1, g_2, \ldots$ such that

$$f\left(x - \sum_{j=0}^{n} g_j f^j\right)$$

is divisible by f^{n+1}, $n = 0, 1, 2, \ldots$. We take $g_0 = 0$ and then $f(x - g_0 f^0) = f(x) = f$ is divisible by f. Suppose we have chosen $g_0, \ldots , g_{n-1}$. Let

$$h = x - \sum_{j=0}^{n-1} g_j f^j$$

Notes

so that, by assumption, $f(h)$ is divisible by f^n. We want to choose g_n so that $f(h)$ is divisible by f^{n+1}. We apply the general Taylor formula and obtain

$$f(h - g_n f^n) = f(h) - g_n f^n f'(h) + f^{n+1} b$$

where b is some polynomial. By assumption $f(h) = qf^n$. Thus, we see that to have $f(h - g_n f^n)$ divisible by f^{n+1} we need only choose g_n in such a way that $(q - g_n f')$ is divisible by f. This can be done, because f has no repeated prime factors and so f and f' are relatively prime. If a and e are polynomials such that $af + ef' = 1$, and if we let $g_n = eq$, then $q - g_n f'$ is divisible by f.

Now we have a sequence $g_0, g_1, \ldots$, such that f^{n+1} divides $f\left(x - \sum_{j=0}^{n} g_j f^i\right)$. Let us take $n = r - 1$ and then since $f(T)^r = 0$

$$f\left(T - \sum_{j=0}^{r-1} g_j(T) f(T)^i\right) = 0.$$

Let

$$N = \sum_{j=0}^{r-1} g_j(T) f(T)^j = \sum_{j=0}^{r-1} g_j(T) f(T)^j$$

Since $\sum_{j=1}^{n} g_j f^i$ is divisible by f, we see that $N^r = 0$ and N is nilpotent. Let $S = T - N$. Then $f(S) = f(T - N) = 0$. Since f has distinct prime factors, S is semi-simple.

Now we have $T = S + N$ where S is semi-simple, N is nilpotent, and each is a polynomial in T. To prove the uniqueness statement, we shall pass from the scalar field F to the field of complex numbers. Let β be some ordered basis for the space V. Then we have

$$[T]_\beta = [S]_\beta + [N]_\beta$$

while $[S]_\beta$ is diagonalizable over the complex numbers and $[N]_\beta$ is nilpotent. This diagonalizable matrix and nilpotent matrix which commute are uniquely determined.

Self Assessment

1. If N is a nilpotent linear operator on V, show that for any polynomial f the semi-simple part of $f(N)$ is a scalar multiple of the identity operator (F a subfield of C).

2. Let T be a linear operator on R^3 which is represented by the matrix

$$\begin{bmatrix} 3 & 1 & -1 \\ 2 & 2 & -1 \\ 2 & 2 & 0 \end{bmatrix}$$

in the standard ordered basis. Show that there is a semi-simple operator S on R^3 and a nilpotent operator N on V such that $T = S + N$ and $SN = NS$.

3.3 Summary

- In this unit the idea of semi-simple linear operator is explored after a brief review of the outcome of the previous few units.
- It is shown that a linear operator is semi-simple if every T-invariant subspace W of the finite dimensional space V, has a complementary T-invariant subspace W' such that $V = W \oplus W'$.

- It is seen that for a linear operator T on V, a finite dimensional vector space over a field of complex numbers has a semi-simple operator S on V and a nilpotent operator N on V such that $T = S + N$, $SN = NS$.

3.4 Keywords

Complementary T-invariant subspace: Let T a linear operator has a T-invariant sub-space W such that $V = W \oplus W'$ then W' is a subspace which is complementary to W. However if W' is also T-invariant then W' is known as complementary T-invariant subspace.

Semi-simple operator: Let T be a linear operator on V, and suppose that the minimal polynomial for T is irreducible over the scalar field F, then T is called a semi-simple operator.

3.5 Review Questions

1. Let T be a linear operator on a finite dimensional space over a subfield of C. Prove that T is semi-simple and only if the following is true. If f is a polynomial and $f(T)$ is nilpotent, then $f(T) = 0$.

2. Let T a linear operator on V is represented by the matrix

$$A = \begin{bmatrix} 4 & 2 & -2 \\ -5 & 3 & 2 \\ -2 & 4 & 1 \end{bmatrix}$$

   Show that T is diagonalizable.

3.6 Further Readings

Books Kenneth Hoffman and Ray Kunze, *Linear Algebra*

Michael Artin, *Algebra*

Unit 4: Inner Product and Inner Product Spaces

CONTENTS

Objectives

Introduction

4.1 Inner Product

4.2 Inner Product Space

4.3 Summary

4.4 Keywords

4.5 Review Questions

4.6 Further Readings

Objectives

After studying this unit, you will be able to:

- See that there is some similarity between the scalar product in vector analysis and the concept of inner product.
- Understand that an inner product on a vector space V is a function which assigns to each ordered pair of vectors α, β in V a scalar (α/β) in the field F such a way that for all α, β, γ in V and all scalars C

$$(\alpha / c\beta + \gamma) = \bar{c}\,(\alpha|\beta) + (\alpha|\gamma)$$

- Know the importance of the construction known as Gram–Schmidt orthogonalization process to convert a set of independent vector (β_1, β_2, … β_n) into an orthogonal set of vectors (α_1, α_2, … α_n).
- Understand orthogonal projection operators and their importance.

Introduction

In this unit the concept of inner product and inner product space is introduced and a similarity is shown with the scalar product of dot product in vector analysis.

The Cauchy-Schwarz inequality is introduced.

With the help of examples it is shown how to obtain a set of orthogonal vectors (α_1, α_2, … α_n) from a set of independent vectors (β_1, β_2, … β_n) by means of a construction known as Gram-Schmidt orthogonalization process.

By introducing orthogonal projection, E of V on W, it is seen that E is an idempotent linear transformation of V onto W, $W^{\perp}$ is the null space of F and $V = W \oplus W^{\perp}$.

4.1 Inner Product

In this unit we consider the vector space V over a field of real or complex numbers. In the first case V is called a real vector space, in the second, a complex vector field. We have had some experience of a real vector space in fact both analytic geometry and the subject matter of vector analysis deal with these spaces. In these concrete examples, we had the idea of length, secondly we had the idea of the angle between two vectors. These became special cases of the notion of a dot product (often called a scalar or inner product.) of vectors in R^3. Given the vectors $v = (x_1, x_2, x_3)$ and $w = (y_1, y_2, y_3)$ in R^3 the dot product of v and w is defined as

$v.w = x_1 y_1 + x_2 y_2 + x_3 y_3$.

Note that the length of the vector v is given by $\sqrt{v.v}$ and the angle θ between v and w is given by

$$\cos\theta = \frac{v.w}{\sqrt{v.v}\sqrt{w.w}}.$$

We list a few of the properties of a dot product:

1. $v.v \geq 0$
2. $v.w = w.v$
3. $v.(aw + bw) = a\,v.w + b\,v.w$

for any vectors v, w and real numbers a, b. If now include the complex field we slightly modify the above relations and list them as follows:

1. $v.w = \overline{w.v}$
2. $v.v \geq 0$ and $v.v = 0$ if and only if $v = 0$;
3. $(au + bw).v = au.v + bw.v$
4. $u(av + bw) = \overline{a}(u.v) + \overline{b}\ u.w$

for all complex numbers a, b and all complex vectors u, v, w.

Definition. Let F be the field of real numbers or the field of complex numbers, and V a vector over F. An *inner product* on V is a function which assigns to each ordered pair of vectors α, β in V a scalar $(\alpha \mid \beta)$ in F in such a way that for all α, β, γ in V and all scalars C.

(a) $(\alpha + \beta \mid \gamma) = (\alpha \mid \gamma) + (\beta \mid \gamma)$;

(b) $(c\alpha \mid \beta) = c(\alpha \mid \beta)$

(c) $(\beta \mid \alpha) = \overline{(\alpha \mid \beta)}$, the bar denoting complex conjugation;

(d) $(\alpha \mid \alpha) > 0$ if $\alpha \neq 0$.

It should be observed that conditions (a), (b) and (c) imply that

(e) $(\alpha \mid c\beta + \gamma) = \overline{c}(\alpha \mid \beta) + (\alpha \mid \gamma)$.

In the examples that follow and throughout the unit F is either the field of real numbers or the field of complex numbers.

Example 1: In $F^{(n)}$ define, for $\alpha = (x_1, x_2, \ldots x_n)$ and $\beta = (y_1\ y_2 \ldots y_n)$, $(\alpha \mid \beta) = x_1\overline{y}_1 + x_2\,\overline{y}_2 + \ldots + x_n\overline{y}_n$ we call $(\alpha \mid \beta)$ the Standard Inner Product.

Example 2: In $F^{(2)}$ define for $\alpha = (x_1, x_2)$ and $\beta = (y_1, y_2)$,

$$(\alpha \mid \beta) = 2\,x_1\overline{y}_1 + x_1\overline{y}_2 + x_2\overline{y}_1 + x_2\overline{y}_2.$$

Notes

Since

$$(\alpha \mid \alpha) = 2|x_1|^2 + 2\overline{x_1 y_2} + |x_2|^2$$

$$= |x_1|^2 + (x_1 + x_2)(\overline{x}_1 + \overline{x}_2)$$

It follows that $(\alpha \mid \alpha) > 0$ if $\alpha \neq 0.$ Conditions (*a*), (*b*), and (*c*) of the definition are easily verified. So $(\alpha \mid \beta)$ defines an inner product on $F^{(2)}$.

Example 3: Let V be $F^{n \times n}$, the space of all $n \times n$ matrices over F. Then V is isomorphic to F^{n2} in a natural way. It follows from Example 1 that the equation

$$(A \mid B) = \sum_{j,k} A_{jk}\, \overline{B}_{jk,}$$

defines an inner product on V. Furthermore, if we introduce the conjugate transpose matrix B^*, where $B^*_{jk} = \overline{B}_{jk}$ we may express this inner product of $F^{n \times n}$ in terms of the trace function:

$$(A \mid B) = \text{tr}\,(A \mid B^*) = \text{tr}\,(B^* A).$$

For

$$\text{tr}\,(AB^*) = \sum_j (AB^*)_{jj}$$

$$= \sum_j \sum_k A_{jk}\, B^*_{kj}$$

$$= \sum_j \sum_k A_{jk}\, \overline{B}_{jk}.$$

Example 4: Let $F^{n \times 1}$ be the space of $n \times 1$ (column matrices over F, and let Q be an $n \times n$ invertible matrix over F. For X, Y in $F^{n \times 1}$ set

$$(X \mid Y) = Y^* Q^* Q X.$$

We are identifying the 1×1 matrix on the right with its single entry. When Q is the identity matrix, this inner product is essentially the same as that in Example 1; we call it the standard inner product on $F^{n \times 1}$. The reader should note that the terminology 'standard inner product' is used in two special contexts. For a general finite-dimensional vector space over F, there is no obvious inner product that one may call standard.

Example 5: Let V be the vector space of all continuous complex-valued functions on the unit interval, $0 \le t \le 1$. Let

$$(f \mid g) = \int_0^1 f(t)\overline{g(t)}\,dt.$$

The reader is probably more familiar with the space of real-valued continuous functions on the unit interval, and for this space the complex conjugate on g may be omitted.

Example 6: This is really a whole class of examples. One may construct new inner products from a given one by the following method. Let V and W be vector spaces over F and suppose (|) is an inner product on W. If T is a non-singular linear transformation from V into W, then the equation

$$pr(\alpha, \beta) = (T\alpha \mid T\beta)$$

defines an inner product pr on V. The inner product in Example 4 is a special case of this situation. The following are also special cases.

(a) Let V be a finite-dimensional vector space, and let,

$$\mathcal{B} = \{\alpha_1 \ldots, \alpha_n)$$

be an ordered basis for V. Let $\varepsilon_1, \ldots, \varepsilon_n$ be the standard basis vectors in F^n, and let T be the linear transformation from V into F^n such that $T\alpha_j = \varepsilon_j$, $j = 1, \ldots, n$. In other words, let T be the 'natural' isomorphism of V onto F^n that is determined by $\mathcal{B}$. If we take the standard inner product on F^n, then

$$pr\left(\sum_j x_j\alpha_j, \sum_k y_k\alpha_k\right) = \sum_{j=1}^{n} x_j\overline{y}_j.$$

Thus, for any basis for V there is an inner product on V with the property $(\alpha_j \mid \alpha_k) = \delta_{jk}$; in fact, it is easy to show that there is exactly one such inner product. Later we shall show that every inner product on V is determined by some basis $\mathcal{B}$ in the above manner.

(b) We look again at Example 5 and take $V = W$, the space of continuous functions on the unit interval. Let T be the linear operator 'multiplication by t,' that is, $(Tf)(t) = tf(t)$, $0 \leq t \leq 1$. It is easy to see that T is linear. Also T is non-singular; for suppose $Tf = 0$. Then $tf(t) = 0$ for $0 \leq t \leq 1$; hence $f(t) = 0$ for $t > 0$. Since f is continuous, we have $f(0) = 0$ as well, or $f = 0$. Now using the inner product of Example 5, we construct a new inner product on V by setting

$$\begin{aligned} pr(f,g) &= \int_0^1 (Tf)(t)\overline{(Tg)(t)}\,dt \\ &= \int_0^1 f(t)\overline{g(t)}t^2\,dt. \end{aligned}$$

We turn now to some general observations about inner products. Suppose V is complex vector space with an inner product. Then for all α, β in V

$$(\alpha \mid \beta) = \text{Re}\,(\alpha \mid \beta) + i\,\text{Im}\,(\alpha \mid \beta) \qquad \ldots (1)$$

where Re $(\alpha \mid \beta)$ and Im $(\alpha \mid \beta)$ are the real and imaginary parts of the complex number $(\alpha \mid \beta)$. If z is a complex number, then Im (z) = Re $(-iz)$. It follows that

$$\text{Im}\,(\alpha \mid \beta) = \text{Re}\,[-i(\alpha \mid \beta)] = \text{Re}\,(\alpha \mid i\beta).$$

Thus the inner product is completely determined by its 'real part' in accordance with

$$(\alpha \mid \beta) = \text{Re}\,(\alpha \mid \beta) + i\,\text{Re}\,(\alpha \mid i\beta) \qquad \ldots (2)$$

Occasionally it is very useful to know that an inner product on a real or complex vector space is determined by another function, the so-called quadratic form determined by the inner product. To define it, we first denote the positive square root of $(\alpha \mid \alpha)$ by $||\alpha||$; $||\alpha||$ is called the *norm* of α with respect to the inner product. By looking at the standard inner products in R^1, C^1, R^2, and R^3, the reader, should be able to convince himself that it is appropriate to think of the norm of α as the 'length' or 'magnitude' of α. The *quadratic form* determined by the inner product is the function that assigns to reach vector α the scalar $||\alpha||^2$. It follows from the properties of the inner product that

$$\|(\alpha \pm \beta)\|^2 = \|\alpha\|^2 \pm 2\,\text{Re}\,(\alpha \mid \beta) + \|\beta\|^2$$

for all vectors α and β. Thus in the real case

$$(\alpha|\beta) = \frac{1}{4}\|\alpha+\beta\|^2 - \frac{1}{4}\|\alpha-\beta\|^2 \qquad \text{... (3)}$$

In the complex case we use (2) to obtain the more complicated expression

$$(\alpha|\beta) = \frac{1}{4}\|\alpha+\beta\|^2 - \frac{1}{4}\|\alpha-\beta\|^2 + \frac{i}{4}\|\alpha+i\beta\|^2 - \frac{i}{4}\|\alpha-i\beta\|^2 \qquad \text{... (4)}$$

Equations (3) and (4) are called the *polarization identities*. Note that (4) may also be written as follows:

$$(\alpha|\beta) = \frac{1}{4}\sum_{n=1}^{4} i^n \|\alpha+i^n\beta\|^2.$$

The properties obtained above hold for any inner product on a real or complex vector space V, regardless of its dimension. We turn now to the case in which V is finite-dimensional. As one might guess, an inner product on a finite-dimensional space may always be described in terms of an ordered basis by means of a matrix.

Suppose that V is finite-dimensional, that

$$\beta = \{\alpha_1, ..., \alpha_n\}$$

is an ordered basis for V, and that we are given a particular inner product on V; we shall show that the inner product is completely determined by the values

$$G_{jk} = (\alpha_k | \alpha_j) \qquad \text{... (5)}$$

it assumes on pairs of vectors in $\mathcal{B}$. If $\alpha = \sum_k x_k\alpha_k$ and $\beta = \sum_j y_j\alpha_j$, then

$$\begin{aligned}(\alpha|\beta) &= \left(\sum_k x_n\alpha_k | \beta\right) \\ &= \sum_k x_k(\alpha_k|\beta) \\ &= \sum_k x_k \sum_j \overline{y}_j(\alpha_k|\alpha_j) \\ &= \sum_{j,k} \overline{y}_j G_{jk} x_k \\ &= Y^*GX\end{aligned}$$

where X, Y are the coordinate matrices of α, β in ordered basis $\mathcal{B}$, and G is the matrix with entries $G_{jk} = (\alpha_k | a_j)$. We call G the matrix of the inner product in the ordered basis $\mathcal{B}$. It follows from (5) that G is Hermitian i.e., that $G = G^*$; however, G is a rather special kind of Hermitian matrix. For G must satisfy the additional condition

$$X^*GX > 0, \qquad X \neq 0. \qquad \text{... (6)}$$

In particular, G must be invertible. For otherwise there exists an $X \neq 0$ such that $GX = 0$, and for any such X, (6) is impossible. More explicitly, (6) says that for any scalars $x_1, ..., x_n$ not all of which are 0.

Notes

$$\sum_{j,k} x_j G_{jk} x_k > 0 \qquad .... (7)$$

From this we see immediately that each diagonal entry of G must be positive; however, this condition on the diagonal entries is by no means sufficient to insure the validity of (6). Sufficient conditions for the validity of (6) will be given later.

The above process is reversible; that is, if G is any $n \times n$ matrix over F which satisfies (6) and the condition $G = G^*$, then G is the matrix in the ordered basis $\mathcal{B}$ of an inner product on V. This inner product is given by the equation

$$(\alpha | \beta) = Y^*GX$$

where X and Y are the coordinate matrices of α and β in the ordered basis $\mathcal{B}$.

Self Assessment

1. Let V be a vector space $(\,|\,)$ an inner product on V.
   (a) Show that $(o | \beta) = 0$ for all β in V.
   (b) Show that if $(\alpha | \beta) = 0$ for all β in V, then $\alpha = 0$.
2. Let $(\,|\,)$ be the standard inner product on R^2.
   (a) Let $\alpha = (1, 2)$, $\beta = (-1, 1)$. If γ is a vector such that $(\alpha | \gamma) = -1$ and $(\beta | \gamma) = 3$, find γ.
   (b) Show that for any α in R^2 we have

   $$\alpha = (\alpha | \varepsilon_2)\, \varepsilon_1 + (\alpha | \varepsilon_2)\, \varepsilon_2$$

   Where $\varepsilon_1 = (1, 0)$ and $\varepsilon_2 = (0,1)$.

4.2 Inner Product Space

After gaining some insight about an inner product we want to see how to combine a vector space to some particular inner product in it. We shall thereby establish the basic properties of the concept of length and orthogonality which are imposed on the space by the inner product.

Definition: *An Inner Product space* is a real or complex vector space together with a specified inner product on that space.

A finite-dimensional real inner product space is often called a *Euclidean Space*. A complex inner product space is often referred to as a *unitary space*.

We now introduce the theorem:

Theorem 1. If V is an inner product space, then for any α, β in V and any scalar

(i) $\|c\alpha\| = |c|\|\alpha\|$;

(ii) $\|\alpha\| > 0$ for $\alpha \neq 0$;

(iii) $|(\alpha | \beta)| \leq \|\alpha\| \|\beta\|$

(iv) $\|\alpha + \beta\| \leq \|\alpha\| + \|\beta\|$

Proof: Statements (i), (ii) can be proved from various definitions. The inequality in (iii) is valid for $\alpha = 0$. If $\alpha \pm 0$, put

$$\gamma = \beta - \frac{(\beta|\alpha)}{\|\alpha\|^2}\alpha, \text{ so } (\gamma|\alpha) = 0 \text{ and}$$

$$0 \le \|\gamma\|^2 = \left(\beta - \frac{(\beta|\alpha)\alpha}{\|\alpha\|^2}\middle|\beta - \frac{(\beta|\alpha)\alpha}{\|\alpha\|^2}\right)$$

$$= (\beta|\beta) - \frac{(\beta|\alpha)(\alpha|\beta)}{\|\alpha\|^2} = \|\beta\|^2 - \frac{\|(\alpha|\beta)\|^2}{\|\alpha\|^2}$$

Hence $|(\alpha|\beta)|^2 \le \|\alpha\|^2\|\beta\|^2$. Now using (iv) we find that

$$\|\alpha+\beta\|^2 = \|\alpha\|^2 + (\alpha|\beta) + (\beta|\alpha) + \|\beta\|^2$$

$$= \|\alpha\|^2 + 2\,\mathrm{Re}(\alpha|\beta) + \|\beta\|^2$$

$$\le \|\alpha\|^2 + 2\|\alpha\|\,\|\beta\| + \|\beta\|^2$$

$$= (\|\alpha\| + \|\beta\|)^2.$$

Thus, $\|\alpha+\beta\| \le \|\alpha\| + \|\beta\|$.

The inequality in (iii) is called the **Cauchy-Schwarz inequality**. It has a wide variety of applications. The proof shows that if (for example) α is non-zero, then $|(\alpha|\beta| < \|\alpha\|\,\|\beta\|$ unless

$$\beta = \frac{(\beta|\alpha)}{\|\alpha\|^2}\alpha.$$

Thus, equality occurs in (iii) if and only if α and β are linearly dependent.

Example 7: If we apply the Cauchy-Schwarz inequality to the inner products given in Examples 1, 3, and 5, we obtain the following:

(a) $\left|\sum x_k\bar{y}_k\right| \le \left(\sum |x_k|^2\right)^{1/2}\left(\sum |y_k|^2\right)^{1/2}$

(b) $|\mathrm{tr}\,(AB^*)| \le (\mathrm{tr}\,(AA^*))^{1/2}(\mathrm{tr}\,(BB^*))^{1/2}$

(c) $\left|\int_0^1 f(x)\,\overline{g(x)}\,dx\right| \le \left(\int_0^1 |f(x)|^2\,dx\right)^{1/2}\left(\int_0^1 |g(x)|^2 dx\right)^{1/2}$.

Definitions: Let α and β be vectors in an inner product space V. Then α is orthogonal to β if $(\alpha|\beta) = 0$; since this implies β is orthogonal to α, we often simply say that α and β are orthogonal. If S is a set of vectors in V, S is called an **orthogonal set** provided all pairs of distinct vectors in S are orthogonal. An **orthonormal set** is an orthogonal set S with the additional property that $\|\alpha\| = 1$ for every α in S.

The zero vector is orthogonal to every vector in V and is the only vector with this property. It is appropriate to think of an orthonormal set as a set of mutually perpendicular vectors, each having length 1.

Notes

Example 8: The standard basis of either R^n or C^n is an orthonormal set with respect to the standard inner product.

Example 9: The vector (x, y) in R^2 is orthogonal to $(-y, x)$ with respect to standard inner product, for

$$((x, y)|(-y, x)) = -xy + yx = 0.$$

However if R^2 is equipped with the inner product of Example 2, then (x, y) and $(-y, x)$ are orthogonal if and only if

$$y = \pm x$$

Example 10: Let V be $C^{n \times n}$, the space of complex $n \times n$ matrices, and let E^{pq} be the matrix whose only non-zero entry is a 1 in row p and column q. Then the set of all such matrices E^{pq} is orthonormal with respect to the inner product given in Example 3. For

$$(E^{pq} | E^{rs}) = \operatorname{tr}(E^{pq}E^{sr}) = \delta_{qs}\operatorname{tr}(E^{pr}) = \delta_{qs}\delta_{pr}.$$

Example 11: Let V be the space of continuous complex-valued (or real-valued) functions on the interval $0 \le x \le 1$ with the inner product

$$(f|g) = \int_0^1 f(x)\overline{g(x)}\,dx.$$

Suppose $f_n(x) = \sqrt{2}\cos 2\pi nx$ and that $g_n(x) = \sqrt{2}\sin 2\pi nx$. Then $\{1, f_1, g_1, f_2, g_2, ...\}$ is an infinite orthonormal set. In the complex case, we may also form the linear combinations

$$\frac{1}{\sqrt{2}}(f_n + ig_n), \qquad n = 1, 2 \ldots.$$

In this way we get a new orthonormal set S which consists of all functions of the form

$$h_n(x) = e^{2\pi inx}, \qquad n = \pm 1, \pm 2, \ldots.$$

The set S' obtained from S by adjoining the constant function 1 is also orthonormal. We assume here that the reader is familiar with the calculation of the integrals in equation.

The orthonormal sets given in the examples above are all linearly independent. We show now that this is necessarily the case.

Theorem 2: An orthogonal set of non-zero vectors in linearly independent.

Proof: Let S be a finite or infinite orthogonal set of non-zero vectors in a given inner product space. Suppose $\alpha_1\ \alpha_2 \ldots, \alpha_m$ are distinct vectors in S and that

$$\beta = c_1\alpha_1 + c_2\alpha_2 + \ldots + c_m\alpha_m.$$

Then

$$(\beta | \alpha_k) = \left(\sum_j c_j\alpha_j | \alpha_k\right)$$

$$= \sum_j c_j(\alpha_j \mid \alpha_k)$$

$$= c_k(\alpha_k \mid \alpha_k).$$

Since $(\alpha_k \mid \alpha_k) \neq 0$, it follows that

$$c_k = \frac{(\beta \mid \alpha_k)}{\|\alpha_k\|^2}, \qquad 1 \leq k \leq m.$$

Thus, when $\beta = 0$, each $c_k = 0$; so S is an independent set.

Corollary: If α vector β is a linear combination of an orthogonal sequence of non-zero vectors $\alpha_1, \ldots, \alpha_m$, then β is the particular linear combination

$$\beta = \sum_{k=1}^{m} \frac{(\beta \mid \alpha_k)}{\|\alpha_k\|^1} \alpha_k. \qquad \ldots (8)$$

This corollary follows from the proof of the theorem. There is another corollary which although obvious, should be mentioned. If $\{\alpha_2 \ldots, \alpha_m\}$ is an orthogonal set of non-zero vectors in a finite-dimensional inner product space V, then $m \leq \dim V$. This says that the number of mutually orthogonal directions in V cannot exceed the algebraically define dimension of V. The maximum number of mutually orthogonal directions in V is what one would intuitively regard as the geometric dimension of V, and we have just seen that this is not greater than the algebraic dimension. The fact that these two dimensions are equal is a particular corollary of the next result.

Theorem 3: Let V be an inner product space and let $\beta_1 \ldots, \beta_n$ be any independent vectors in V. Then one may construct orthogonal vectors $\alpha_1, \ldots, \alpha_n$ in V such that for each $k = 1, 2, \ldots, n$ the set

$$\{\alpha_1, \ldots, \alpha_k\}$$

is a basis for the subspace spanned by $\beta_1, \ldots, \beta_k$.

Proof: The vectors $\alpha_1 \ldots, \alpha_n$ will be obtained by means of a construction known as the **Gram-Schmidt orthogonalization process.** First let $\alpha_1 = \beta_1$. The other vectors are then given inductively as follows:

Suppose $\alpha_1, \ldots, \alpha_m$ $(1 \leq m < n)$ have been chosen so that for every k

$$\{\alpha_1, \ldots, \alpha_k\}, \qquad 1 \leq k \leq m$$

is an orthogonal basis for the subspace of V that is spanned by $\alpha_1, \ldots, \beta_k$. To construct the next vector α_{m+1}, let

$$\alpha_{m+1} = \beta_{m+1} - \sum_{k=1}^{m} \frac{(\beta_{m+1} \mid \alpha_k)}{\|\alpha_k\|^2} \alpha_k. \qquad \ldots (9)$$

Then $\alpha_{m+1} \neq 0$. For otherwise β_{m+1} is a linear combination of $\alpha_1, \ldots, \alpha_m$ and hence a linear combination of $\beta_1, \ldots, \beta_m$. Futhermore, if $1 \leq j \leq m$, then

$$(\alpha_{m+1} \mid \alpha_j) = (b_{m+1} \mid \alpha_j) - \sum_{k=1}^{m} \frac{(\beta_{m+1} \mid \alpha_k)}{\|\alpha_k\|^2} (\alpha_k \mid \alpha_j)$$

Notes

$$= (\beta_{m+1} | \alpha_j) - (\beta_{m+1} | \alpha_j)$$

$$= 0.$$

Therefore $\{\alpha_1, \ldots, \alpha_{m+1}\}$ is an orthogonal set consisting of $m + 1$ non-zero vectors in the subspace spanned by $\beta_1, \ldots, \beta_{m+1}$. By theorem 2, it is a basis for this subspace. Thus the vectors $\alpha_1, \ldots, \alpha_n$ may be constructed one after the other in accordance with (9). In particular, when $n = 4$, we have

$$\alpha_1 = \beta_1$$

$$\alpha_2 = \beta_2 - \frac{(\beta_2 | \alpha_1)}{\|\alpha_1\|^2}\alpha_1 \qquad \ldots (10)$$

$$\alpha_3 = \beta_3 - \frac{(\beta_3 | \alpha_1)}{\|\alpha_1\|^2}\alpha_1 - \frac{(\beta_3 | \alpha_2)}{\|\alpha_2\|^2}\alpha_2$$

$$\alpha_4 = \beta_4 - \frac{(\beta_4 | \alpha_1)}{\|\alpha_1\|^2}\alpha_1 - \frac{(\beta_4 | \alpha_2)}{\|\alpha_2\|^2}\alpha_2 - \frac{(\beta_4 | \alpha_3)}{\|\alpha_3\|^2}\alpha_3. \qquad \ldots (11)$$

Corollary: Every finite-dimensional inner product space has an orthonormal basis.

Proof: Let V be a finite-dimensional inner product space and $\{\beta_1, \ldots, \beta_n\}$ a basis for V. Apply the Gram-Schmidt process to construct an orthogonal basis $\{\alpha_1, \ldots, \alpha_n\}$. Then to obtain an orthonormal basis, simply replace each vector α_k by $\alpha_k / \|\alpha_k\|$.

One of the main advantages which orthonormal bases have over arbitrary bases is that computations involving coordinates are simpler. To indicate in general terms why this is true, suppose that V is a finite-dimensional inner product space. Then, as in the last section, we may use Equation (5) to associate a matrix G with every ordered basis $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$ of V. Using this matrix

$$G_{jk} = (\alpha_k | \alpha_j)$$

we may compute inner products in terms of coordinates, If $\mathcal{B}$ is an orthonormal basis, then G is the identity matrix, and for any scalars x_j and y_k

$$\left(\sum_j x_j\alpha_j \middle| \sum_k y_k\alpha_k\right) = \sum_j x_j\bar{y}_j.$$

Thus in terms of an orthonormal basis, the inner product in V looks like the standard inner product in F^n.

Although it is of limited practical use for computations, it is interesting to note that the **Gram-Schmidt process** may also be used to test for linear dependence. For suppose $\beta_1, \ldots, \beta_n$ are linearly dependent vectors in an inner product space V. To exclude a trivial case, assume that $\beta_1 \neq 0$. Let m be the largest integer for which $\beta_1, \ldots, \beta_m$ are independent. Then $1 \leq m < n$. Let $\alpha_1, \ldots, \alpha_m$ be the vectors obtained by applying the orthogonalization process to $\beta_1 \ldots, \beta_m$. Then the vector α_{m+1} given by (9) is necessarily 0. For α_{m+1} is in the subspace spanned by $\alpha_1, \alpha_2, \ldots, \alpha_n$ and orthogonal to each of these vectors; hence it is 0 by (6). Conversely it $\alpha_1, \ldots, \alpha_n$ are different from 0 and $\alpha_{m+1} = 0$, then $\beta_1, \beta_2, \ldots, \beta_{m+1}$ are linearly dependent.

Example 12: Consider the vectors

$$\beta_1 = (4, 0, 3)$$

$$\beta_2 = (7, 0, -1)$$

$$\beta_3 = (1, 5, 4)$$

in R^3 equipped with the standard inner product. Applying the Gram-Schmidt process to β_1, β_2, β_3, we obtain the following vectors.

$$\alpha_1 = (4, 0, 3)$$

$$\alpha_2 = (7, 0, -1) - \frac{(7, 0, -1 | 4, 0, 3)}{25}(4, 0, 3)$$

$$= (7, 0, -1) - (4, 0, 3) = (3, 0, -4)$$

$$\alpha_3 = (1, 5, 4) - \frac{(1, 5, 4 | 3, 0, -4)}{25}(3, 0, -4) - \frac{(1, 5, 4 | 4, 0, 3)}{25}(4, 0, 3)$$

$$= (1, 5, 4) + \frac{13}{25}(3, 0, -4) - \frac{16}{25}(4, 0, 3)$$

$$= (0, 5, 0)$$

These vectors are evidently non-zero and mutually orthogonal. Hence $(\alpha_1, \alpha_2, \alpha_3)$ is an orthogonal basis for R^3. To express an arbitrary vector (x_1, x_2, x_3) in R^3 as a linear combination of α_1, α_2, α_3, it is not necessary to solve any linear equation. For it suffices to use (8).

Thus

$$(x_1, x_2, x_3) = \frac{3x_3 + 4x_1}{25}\alpha_1 + \frac{(3x_1 - 4x_3)}{25}\alpha_2 + \frac{x_2}{5}\alpha_3$$

as is readily verified. In particular,

$$(1, 2, 3) = \frac{13}{25}(4, 0, 3) - \frac{9}{25}(3, 0, -4) + \frac{2}{5}(0, 5, 0)$$

To put this point in another way, what we have shown in the following: The basis (f_1, f_2, f_3) of $(R^3)^\alpha$ which is dual to basis $(\alpha_1, \alpha_2, \alpha_3)$ is defined explicitly by the equations

$$f_1(x_1, x_2, x_3) = \frac{4x_1 + 3x_3}{25}$$

$$f_2(x_1, x_2, x_3) = \frac{3x_1 - 4x_3}{25}$$

$$f_3(x_1, x_2, x_3) = \frac{x_2}{5},$$

and these equations may be written more generally in the form

$$f_j(x_1, x_2 x_3) = \frac{(x_1, x_2, x_3 | \alpha_j)}{\|\alpha_j\|^2}.$$

Finally, note that from α_1, α_2, α_3 we get the orthonormal basis

$$\frac{1}{5}(4, 0, 3), \frac{1}{5}(3, 0, -4), (0, 1, 0).$$

Example 13: If F be the real field and V be the set of polynomials, in a variable x over F of degree 2 or less. In V we define an inner product by: If $p(x)$, $q(x) \in V$, then

$$(p(x), q(x)) = \int_{-1}^{+1} p(x)q(x)\,dx$$

Let us start with the basis $\beta_1 = 1$, $\beta_2 = x$, $\beta_3 = x^2$ of V and obtain orthogonal set by applying Gram-Schmidt process. Let

$$\alpha_1 = \frac{\beta_1}{\|\beta_1\|} = \frac{1}{\sqrt{2}}$$

as $$\|\beta_1\|^2 = \int_{-1}^{+1} 1.dx = 2.$$

$$\alpha'_2 = \beta_2 - (\beta_2, \alpha_1)\alpha_1$$

$$= x - \frac{1}{\sqrt{2}}\int_{-1}^{+1} x.1\,dx = x - \frac{1}{\sqrt{2}}\left.\frac{x^2}{2}\right|_{-1}^{+1}$$

So the orthonormal α_2 is given by

$$\alpha_2 = \frac{x}{\|\alpha'_2\|} = \frac{x}{\left[\int_{-1}^{+1} x^2 dx\right]^{1/2}} = \sqrt{\frac{3}{2}}\,x$$

Finally

$$\alpha'_3 = \beta_3 - (\beta_3, \alpha_2)\,\alpha_2 - (\beta_3, \alpha_1)\alpha_1$$

$$= x^2 - \left(x^2, \sqrt{\frac{3}{2}}\,x\right)\sqrt{\frac{3}{2}}\,x - \left(x^2, \frac{1}{\sqrt{2}}\right), \frac{1}{\sqrt{2}}$$

Now

$$\left(x^2, \sqrt{\frac{3}{2}}x\right) = \sqrt{\frac{3}{2}}\int_{-1}^{+1} x^2, x\,dx = \sqrt{\frac{3}{2}}\left.\frac{x^4}{4}\right|_{-1}^{+1} = 0$$

and

$$\left(x^2, \frac{1}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}\int_{-1}^{+1} x^2, 1\,dx = \frac{1}{\sqrt{2}}\left.\frac{x^3}{3}\right|_{-1}^{+1} = \frac{\sqrt{2}}{3}$$

Thus

$$\alpha'_3 = x^2 - \frac{1}{3}$$

and normalized α_3 is given by

$$\alpha_3 = \frac{x^2 - 1/3}{\|\alpha'_3\|} = \frac{x^2 = 1/3}{\left[\int_{-1}^{+1}\left(x^2 - \frac{1}{3}\right)^2 dx\right]^{1/2}} = \frac{\sqrt{10}}{4}(3x^2 - 1).$$

Notes

Thus α_1, α_2 and α_3 are orthornormal set of polynomials in V.

In essence, the Gram-Schmidt process consists of repeated applications of a basic geometric operation called orthogonal projection, and it is best understood from this point of view. The method of orthogonal projection also arises naturally in the solution of an important approximation problem.

Suppose W is a subspace of an inner product space V, and let β be an arbitrary vector in V. The problem is to find a best possible approximation to β by vectors in W. This means we want to find a vector α for which $\|\beta - \alpha\|$ is as small as possible subject to the restriction that α should belong to W. Let us make our language precise.

A **best approximation** to β by vectors in W is a vector α in W such that

$$\|\beta - \alpha\| \leq \|\beta - \gamma\|$$

for every vector γ in W.

By looking at this problem in R^2 or in R^3, one sees intuitively that a best approximation to β by vectors in W ought to be a vector α in W such that $\beta - \alpha$ is perpendicular (orthogonal) to W and that there ought to be exactly one such α. These intuitive ideas are correct for finite-dimensional subspace and for some, but not all, indefinite-dimensional subspaces. Since the precise situation is too complicated to treat here, we shall only prove the following result.

Theorem 4: Let W be a subspace of an inner product space V and let β be a vector in V.

1. The vector α in W is a best approximation to β by vectors in W if and only if $\beta - \alpha$ is orthogonal to every vector in W.
2. If a best approximation to β by vectors in W exists, it is unique.
3. If W is finite-dimensional and $\{\alpha_1 \ldots, \alpha_n\}$ is orthonormal basis for W, then the vector

$$\alpha = \sum_k \frac{(\beta | \alpha_k)}{\|\alpha_k\|^2} \alpha_k$$

is the (unique) best approximation to β by vectors in W.

Proof: First note that if γ is any vector in V, then $\beta - \gamma = (\beta - \alpha) + (\alpha - \gamma)$, and

$$\|\beta - \gamma\|^2 = \|\beta - \alpha\|^2 + 2 \operatorname{Re} (\beta - \alpha | \alpha - \gamma) + \|\alpha - \gamma\|^2.$$

Now suppose $\beta - \alpha$ is orthogonal to every vector in W, that γ is in W and that $\gamma \neq \alpha$. Then, since $\alpha - \gamma$ is in W, it follows that

$$\begin{aligned} \|\beta - \gamma\|^2 &= \|\beta - \alpha\|^2 + \|\alpha - \gamma\|^2 \\ &> \|\beta - \alpha\|^2. \end{aligned}$$

Conversely, suppose that $\|\beta - \gamma\| \geq \|\beta - \alpha\|$ for every γ in W. Then from the first equation above it follows that

$$2 \operatorname{Re}(\beta - \alpha | \alpha - \gamma) + \|\alpha - \gamma\|^2 \geq 0$$

for all γ in W. Since every vector in W may be expressed in the form $\alpha - \gamma$ with γ in W, we see that

$$2 \operatorname{Re} (\beta - \alpha | \tau) + \|\tau\|^2 \geq 0$$

for every τ in W. In particular, if γ is in W and $\gamma \neq \alpha$, we may take

$$\tau = -\frac{(\beta - \alpha | \alpha - \gamma)}{\|\alpha - \gamma\|^2}(\alpha - \gamma),$$

Then the inequality reduces to the statement

$$-2\frac{|(\beta - \alpha | \alpha - \gamma)|^2}{\|\alpha - \gamma\|^2} + \frac{|(\beta - \alpha | \alpha - \gamma)|^2}{\|\alpha - \gamma\|^2} \geq 0.$$

This holds if and only if $(\beta - \alpha | \alpha - \gamma) = 0$. Therefore, $\beta - \alpha$ is orthogonal to every vector in W. This completes the proof of the equivalence of the two conditions on a given in (i). This orthogonality condition is evidently satisfied by at most one vector in W, which proves (ii).

Now suppose that W is a finite-dimensional subspace of V. Then we know, as a corollary of Theorem 3, that W has an orthogonal basis. Let $\{\alpha_1, \ldots, \alpha_n\}$ be any orthogonal basis for W and define α by (11). Then, by the computation in the proof of Theorem 3, $\beta - \alpha$ is orthogonal to each of the vectors α_k($\beta - \alpha$ is vector obtained at the last stage when the orthogonalization process is applied to $\alpha_1, \ldots, \alpha_n, \beta$). Thus $\beta - \alpha$ is orthogonal to every linear combination of $\alpha_1, \ldots, \alpha_n$, i.e, to every vector in W. If γ is in W and $\gamma \neq \alpha$, it follows that $\|\beta - \gamma\| > \|\beta - \alpha\|$. Therfore, α is the best approximation to β that lies in W.

Definition: Let V be an inner product space and S any set of vectors in V. The **orthogonal complement** of S is the set $S^\perp$ of all vectors in V which are orthogonal to every vector in S.

The orthogonal complement of V is the zero subspace, and conversely $\{0\}^\perp = V$. If S is any subset of V, its orthogonal complement $S^\perp$ (S perp) is always a subspace of V. For S is non-empty, since it contains 0; and whenever α and β are in $S^\perp$ and c is any scalar,

$$\begin{aligned}(c\alpha + \beta | \gamma) &= c(\alpha | \gamma) + (\beta | \gamma) \\ &= c0 + 0 \\ &= 0\end{aligned}$$

for every γ in S, thus $c\alpha + \beta$ also lies in S. In Theorem 4 the characteristic property of the vector α is that it is the only vector in W such that $\beta - \alpha$ belongs to $W^\perp$.

Definition: Whenever the vector α in Theorem 4 exists it is called the orthogonal projection of β on W. If every vector in V has an orthogonal projection on W, the mapping that assigns to each vector in V its orthogonal projection on W is called the orthogonal projection of V on W.

By Theorem 4, the orthogonal projection of an inner product space on a finite-dimensional subspace always exists. But Theorem 4 also implies the following result.

Corollary: Let V be an inner product space, W a finite-dimensional subspace, and E the orthogonal projection of V on W. Then the mapping

$$\beta \to \beta - E\beta$$

is the orthogonal projection of V on $W^\perp$.

Proof: Let β be an arbitrary vector in V. Then $\beta - E\beta$ is in $W^\perp$, and for any γ in $W^\perp$, $\beta - \gamma = E\beta + (\beta - E\beta - \gamma)$. Since $E\beta$ is in W and $\beta - E\beta - \gamma$ is in $W^\perp$, it follows that

$$\|\beta - \gamma\|^2 = \|E\beta\|^2 + \|\beta - E\beta - \gamma\|^2$$

$$\geq \|\beta - (\beta - E\beta)\|^2$$

with strict inequality when $\gamma \neq \beta - E\beta$. Therefore, $\beta - E\beta$ is the best approximation to β by vectors in $W^{\perp}$.

Example 14: Given R^3 the standard inner product. Then the orthogonal projection of (– 10, 2, 8) on the subspace W that is spanned by (3, 12, –1) is vector

$$\alpha = \frac{((-10, 2, 8) \mid (3, 12, -1))}{9 + 144 + 1}(3, 12, -1)$$

$$= \frac{-14}{154}(3, 12, 1).$$

The orthogonal projection of R^3 on W is the linear transformation E defined by

$$(x_1\ x_2, x_3) \rightarrow \left(\frac{3x_1 + 12x_2 - x_3}{154}\right)(3, 12, -1).$$

The rank of E is clearly 1; hence its nullity is 2. On the other hand,

$$E(x_1, x_2, x_3) = (0, 0, 0)$$

if and only if $3x_1 + 12x_2 - x_3 = 0$. This is the case if and only if $(x_1, x_2, x_3,$ is in $W^{\perp}$. Therefore, $W^{\perp}$. is the null space of E, and $\dim\left(W^{\perp}\right) = 2$. Computing

$$\left(x_1, x_2\ x_3\right) - \left(\frac{3x_1 + 12x_2 - x_3}{154}\right)\left(3, 12, -1\right)$$

we see that the orthogonal projection of R^3 on $W^{\perp}$ is the linear transformation $I - E$ that maps the vector (x_1, x_2, x_3) onto the vector

$$\frac{1}{154}\left(145x_1 - 36x_2 + 3x_3 - 36x_1 + 10x_2 + 12x_3, 3x_1 + 12x_2 + 153x_3\right).$$

The observations made in Example 14 generalize in the following fashion.

Theorem 5: Let W be a finite-dimensional subspace of an inner product space V let E be the orthogonal projection of V on W. Then E is an idempotent linear transformation of V onto W, $W^{\perp}$ is the null space of E, and

$$V = W \oplus W^{\perp}.$$

Proof: Let β be an arbitrary vector in V. Then $E\beta$ is the best approximation to β that lies in W. In particular, $E\beta = \beta$ when β is in W. Therefore, $E(E\beta) = E\beta$ for every β in V; that is, E is idempotent: $E^2 = E$. To prove, that E is a linear transformation, let α and β be any vectors in V and c an arbitrary scalar. Then, by Theorem 4, $\alpha - E\alpha$ and $\beta - E\beta$ are each orthogonal to every vector in W. Hence the vector

$$c(\alpha - E\alpha) + (\beta - E\beta) = (c\alpha + \beta) - (cE\alpha + E\beta)$$

Notes

also belongs to $W^{\perp}$. Since $cE\alpha + E\beta$ is a vector in W, it follows from Theorem 4 that

$$E(c\alpha + \beta) = cE\alpha + E\beta.$$

Of course, one may also prove the linearity of E by using (11) . Again let β be any vector in V. Then $E\beta$ is the unique vector in W such that $\beta - E\beta$ is in $W^{\perp}$. Thus $E\beta = 0$ when β is in $W^{\perp}$. Conversely, β is in $W^{\perp}$ when $E\beta = 0$. Thus $W^{\perp}$ is the null space of E. The equation

$$\beta = E\beta + \beta - E\beta$$

show that $V = W + W^{\perp}$; moreover, $M \cap W^{\perp} = \{0\}$. For if α is vector in $M \cap W^{\perp}$, then $(\alpha \mid \alpha) = 0$. Therefore, $\alpha = 0$, and V is the direct sum of W and $W^{\perp}$.

Corollary: Under the conditions of the theorem, $I - E$ is orthogonal projection of V on $W^{\perp}$. It is an idempotent linear transformation of V onto $W^{\perp}$ with null space W.

Proof: We have already seen that the mapping $\beta \to \beta - E\beta$ is the orthogonal projection of V on $W^{\perp}$. Since E is a linear transformation, this projection on $W^{\perp}$ is the linear transformation $I - E$. From its geometric properties one sees that $I - E$ is an idempotent transformation of V onto W. This also follows from the computation

$$\begin{aligned}(I - E)(I - E) &= I - E - E + E^2 \\ &= I - E.\end{aligned}$$

Moreover, $(I - E)\beta = 0$ if and only if $\beta = E\beta$, and this is the case if and only if β is in W. Therefore W is the null space of $I - E$.

The Gram-Schmidt process may now be described geometrically in the following way. Given an inner product space V and vectors $\beta_1, \ldots, \beta_n$ in V, let P_k $(k > 1)$ be the orthogonal projection of V on the orthogonal complement of the subspace spanned by $\beta_1, \ldots, \beta_{k-1}$, and set $P_1 = I$. Then the vectors one obtains by applying the orthogonalization process to $\beta_1, \ldots, \beta_n$, are defined by the equations

$$\alpha_k = P_k\beta_k, \qquad 1 \le k \le n.$$

Theorem 5 implies another result known as **Bessel's inequality**.

Corollary: Let $\{\alpha_1, \ldots, \alpha_n\}$ be an orthogonal set of non-zero vectors in an inner product space V. If β is any vector in V, then

$$\sum_k \frac{|(\beta \mid \alpha_k)|^2}{\|\alpha_k\|^2} \le \|\beta\|^2$$

and equality holds if and only if

$$\beta = \sum_k \frac{(\beta \mid \alpha_k)}{\|\alpha_k\|^2}\alpha_k.$$

Proof: Let $\gamma = \sum_k \left[(\beta \mid \alpha_k)/\|\alpha_k\|^2\right]\alpha_k$. Then $\beta = \gamma + \delta$ where $(\gamma/\delta) = 0$. Hence

$$\|\beta\|^2 = \|\gamma\|^2 + \|\delta\|^2.$$

It now suffices to prove that

$$\|\gamma\|^2 = \sum_k \frac{|(\beta \mid \alpha_k)|^2}{\|\alpha_k\|^2}.$$

This is straightforward computation in which one uses the fact that $(\alpha_j \mid \alpha_k) = 0$ for $j \neq k$.

In the special case in which $\{\alpha_1 \ldots, \alpha_n\}$ is an orthonormal set, Bessel's inequality says that

$$\sum_k |(\beta \mid \alpha_k)|^2 \leq \|\beta\|^2 .$$

The corollary also tells us in this case that β is in the subspace spanned by $\alpha_1, \ldots, \alpha_n$ if and only if

$$\beta = \sum_k (\beta \mid \alpha_k)\, \alpha_k$$

or if and only if Bessel's inequality is actually an equality. Of course, in the event that V is finite dimensional and $\{\alpha_1, \ldots, \alpha_n\}$ is an orthogonal basis for V, the above formula holds for every vector β in V. In other words, if $\{\alpha_1, \ldots, \alpha_n\}$ is an orthonormal basis for V, the kth coordinate of β in the ordered basis $\{\alpha_1, \ldots, \alpha_n\}$ is $(\beta \mid \alpha_k)$.

Example 15: We shall apply the last corollary to the orthogonal sets described in Example 11. We find that

(a) $$\sum_{k=-n}^{n} \left| \int_0^1 f(t) e^{-2\pi ikt} dt \right|^2 \leq \int_0^1 |f(t)|^2 \, dt$$

(b) $$\int_0^1 \left| \sum_{k=-n}^{n} c_k e^{2\pi ikt} \right|^2 dt = \sum_{k=-n}^{n} |c_k|^2$$

(c) $$\int_0^1 \left(\sqrt{2} \cos 2\pi t + \sqrt{2} \sin 4\pi t\right)^2 dt = 1 + 1 = 2.$$

Self Assessment

3. Apply the Gram-Schmidt process to the vectors $\beta_1 = (1, 0, 1)$, β_2 $(1, 0, -1)$, $\beta_3 = (0, 3, 4)$ to obtain an orthonormal basis for R^3 with the standard inner product.

4. Let V be an inner product space. The distance between two vectors α and β in V is defined by

$$d(\alpha, \beta) = \|\alpha - \beta\|,$$

so that

(a) $d(\alpha, \beta) \geq 0$;

(b) $d(\alpha, \beta) = d(\beta, \alpha)$;

(c) $d(\alpha, \beta) \leq d(\alpha, \gamma) + (\gamma, \beta)$.

4.3 Summary

- The idea of an inner product is somewhat similar to the scalar product in the vector calculus.

- With the help of a few examples the concept of inner product is illustrated.
- The inner product is also related to the polarization identities.
- The relation between the vector space and the inner product is established.
- The Cauchy-Schwarz inequality is established.
- The Gram-Schmidt orthogonalization process help us to find a set of orthogonal vectors as a bases of the vector space V.

4.4 Keywords

An Inner Product Space is a real or complex vector space, together with a specified inner product on that space.

An Orthogonal Set: If S is a set of vectors in V, S is called an orthogonal set provided all pairs of distinct vectors in S are orthogonal. An orthonormal set is an orthogonal set S with the additional property that $\|\alpha\| = 1$ for every d in S.

Bessel's Inequality: Let $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ be an orthogonal set of non-zero vectors in an inner product space V. If β is any vector in V, then the *Bessel Inequality* is given by $\sum_k \frac{|(\beta \mid \alpha_k)^2|^2}{\|\alpha_k\|^2} \leq \|\beta\|^2$.

Cauchy-Schwarz Inequality: If V is an inner product space, then for any vectors α, β in V,

$$|(\alpha \mid \beta)| \leq \|\alpha\| \|\beta\|,$$

is called the Cauchy-Schwarz inequality and the above equality occurs if and only if α and β are linearly dependent.

Conjugate Transpose Matrix: The conjugate transpose matrix B^* is defined by the relation $B^*_{Kj} = \overline{B}_{jK}$, where $\overline{B}$ is complex conjugate of the matrix B.

Gram-Schmidt Orthogonalization Process: Let V be an inner product space and let $\beta_1, \beta_2, \ldots \beta_n$ be any independent set of vectors in V, then one may construct orthogonal vectors $\alpha_1, \alpha_2, \ldots \alpha_n$ in V by means of a construction known as *Gram-Schmidt orthogonalization process.*

Linearly Independent: An orthogonal set of non-zero vectors is *linearly independent*.

Polarization Identities: For the real vector space polarization identities are defined by

$$(\alpha \mid \beta) = \frac{1}{4}\|\alpha + \beta\|^2 - \frac{1}{4}\|\alpha - \beta\|^2.$$

Standard Inner Product: If $\alpha = (x_1, x_2, \ldots x_n)$, $\beta = (y_1, y_2, \ldots y_n)$ are vectors in F^n, there is an inner product which we call the standard inner product, defined by the relation

$$(\alpha \mid \beta) = \sum_{i=1}^{n} x_i \overline{y}_i.$$

The Orthogonal Complement: Let V be an inner product space and S any set of vectors in V. *The orthogonal* complement of S is the set $S^{\perp}$ of all vectors in V which are orthogonal to every vector in S.

4.5 Review Questions

1. Verify that the standard inner product on F^n is an inner product.

2. Consider R^4 with the standard inner product. Let W be the subspace of R^4 consisting of all vectors which are orthogonal to both $\alpha = (1, 0, -1, 1)$ and $\beta = (2, 3, -1, 2)$. Find the basis for W.

3. Consider C^3, with the standard inner product. Find an orthonormal basis for the subspace spanned by $\beta_1 = (1, 0, i)$ and $\beta_2 = (2, 1, 1+i)$.

Answers: Self Assessment

2. (a) $\gamma = \left(-\frac{7}{3}, \frac{2}{3}\right)$

3. $\frac{1}{\sqrt{2}}(1, 0, +1), \frac{1}{\sqrt{2}}(1, 0, -1), (0, 1, 0)$

4.6 Further Readings

Books

Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I N. Herstein, *Topics in Algebra*

Unit 5: Linear Functional and Adjoints of Inner Product Space

Notes

CONTENTS

Objectives

Introduction

5.1 Linear Functional

5.2 Adjoint of Linear Operators

5.3 Summary

5.4 Keywords

5.5 Review Questions

5.6 Further Readings

Objectives

After studying this unit, you will be able to:

- Understand that any linear functional f on a finite-dimensional inner product space is 'inner product with a fixed vector in the space'.
- Prove the existence of the 'adjoint' of a linear operator T on V, this being a linear operator T^* such that $(T\alpha \mid \beta) = (\alpha \mid T^* \beta)$ for all α and β in V.
- A linear operator T such that $T = T^*$ is called self-adjoint (or Hermitian). If β is an orthonormal basis for V, then $[T^*]_B = [T]_\beta$.

Introduction

The idea of the linear functional helps in understanding the nature of the inner product.

The concept of adjoint of a linear transformation with the help of the inner product helps in understanding the self-adjoint operators or Hermitian operators.

This unit also makes a beginning to the understanding of unitary operators and normal operators. The normal operator T has the property that $T^*T = TT^*$.

5.1 Linear Functional

In this section we treat linear functionals on inner product space and their relation to the inner product. Basically any linear functional f on a finite dimensional inner product space is 'inner product with a fixed vector in the space', i.e. that such an f has the form $f(\alpha) = (\alpha \mid \beta)$ for some fixed β in V. We use this result to prove the existence of the 'adjoint' of a linear operator T on V, this being a linear operator T^* such that $(T\alpha \mid \beta) = (\alpha \mid T^* \beta)$ for all α and β in V. Through the use of an orthonormal basis, this adjoint operation on linear operators (passing from T to T^*) is identified with the operation of forming the conjugate transpose of a matrix.

We define a function f_β from V, any inner product space into the scalar field by

$$f_\beta(\alpha) = (\alpha \mid \beta).$$

This function f_β is a linear functional on V, because by its very definition, $(\alpha \mid \beta)$ is linear as a function of α. If V is finite-dimensional, every linear functional on V arises in this way from some β.

Theorem 1: Let V be a finite-dimensional inner product space, and f a linear functional on V. Then there exists a unique vector β in V such that $f(\alpha) = (\alpha \mid \beta)$ for all α in V.

Proof: Let $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ be an orthonormal basis for V. Put

$$\beta = \sum_{j=1}^{n} \overline{f(\alpha_j)}\, \alpha_j \qquad ...(1)$$

and let f_β be the linear functional defined by

$$f_\beta(\alpha) = (\alpha \mid \beta).$$

Then

$$f_\beta(\alpha_k) = \left(\alpha_k \Big| \sum_j \overline{f(\alpha_j)}\alpha_j\right) = f(\alpha_k)$$

Since this is true for each α_k, is follows that $f = f_\beta$. Now suppose γ is a vector in V such that $(\alpha \mid \beta) = (\alpha \mid \gamma)$ for all α. Then $(\beta - \gamma \mid \beta - \gamma) = 0$ and $\beta = \gamma$. Thus there is exactly one vector β determining the linear functional f in the stated manner.

The proof of this theorem can be reworded slightly, in terms of the representation of linear functionals in a basis. If we choose on orthonormal basis $\{\alpha_1, ..., \alpha_n)$ for V, the inner product of $\alpha = x_1\alpha_1 + ... + x_n\alpha_n$ and $\beta = y_1\alpha_1 + ...+ y_n\alpha_n$ will be

$$(\alpha \mid \beta) = x_1\bar{y}_1 + ... + x_n\bar{y}_n.$$

If f is any linear functional on V, then f has the form

$$f(\alpha) = c_1x_1 + ... + c_nx_n$$

for some fixed scalars $c_1, ..., c_n$ determined by the basis. Of course $c_j = f(\alpha_j)$. If we wish to find a vector β in V such that $(\alpha \mid \beta) = f(\alpha)$ for all α, then clearly the coordinates y_j of β must satisfy $\bar{y}_i = c_j$ or $y_i = \overline{f(\alpha_j)}$. Accordingly,

$$\beta = \overline{f(\alpha_1)}\, \alpha_1 + ... + \overline{f(\alpha_n)}\, \alpha_n$$

is the desired vector.

Some further comments are in order. The proof of Theorem 1 that we have given is admirably brief, but it fails to emphasize the essential geometric fact that β lies in the orthogonal complement of the null space of f. Let W be the null space of f. Then $V = W + W^\perp$, and f is completely determined by its values on $W^\perp$. In fact, if P is the orthogonal projection of V on $W^\perp$, then

$$f(\alpha) = f(P\alpha)$$

for all α in V. Suppose $f \neq 0$. Then f is of rank 1 and dim $(W^\perp) = 1$. If γ is any non-zero vector in $W^\perp$, it follows that

$$P\alpha = \frac{(\alpha \mid \gamma)}{\|\gamma\|^2}\gamma$$

for all α in V. Thus

$$f(\alpha) = (\alpha \mid \gamma) . \frac{f(\gamma)}{\|\gamma\|^2}$$

Notes

for all α, and $\beta = [\overline{f(\gamma)} / \|\gamma\|^2]\gamma$.

Example 1: We should give one example showing that Theorem 1 is not true without the assumption that V is finite dimensional. Let V be the vector space of polynomials over the field of complex numbers, with the inner product

$$(f|g) = \int_0^1 f(t)\overline{g(t)}\,dt.$$

This inner product can also be defined algebraically. If $f = \Sigma\, a_k x^k$ and $g = \Sigma\,.\, b_k x^k$, then

$$(f|g) = \sum_{j.k} \frac{j}{j+k+1} a_j \overline{b_k}.$$

Let z be a fixed complex number, and let L be the linear functional 'evaluation at z':

$$L(f) = f(z).$$

Is there a polynomial g such that $(f | g) = L(f)$ for every f? The answer is no; for suppose we have

$$f(z) = \int_0^1 f(t)\overline{g(t)}\,dt$$

for every f. Let $h = x - z$, so that for any f we have $(hf)(z) = 0$. Then

$$0 = \int_0^1 h(t) f(t)\overline{g(t)}\,dt$$

for all f. In particular this holds when $f = \overline{h}g$ so that

$$\int_0^1 |h(t)|^2 |g(t)|^2\,dt = 0$$

and so $hg = 0$. Since $h \neq 0$, it must be that $g = 0$. But L is not the zero functional; hence, no such g exists.

One can generalize the example somewhat, to the case where L is a linear combination of point evaluations. Suppose we select fixed complex numbers $z_1, \ldots, z_n$ and scalars $c_1, \ldots, c_n$ and let

$$L(f) = c_1 f(z_1) + \ldots + c_n f(z_n).$$

Then L is a linear functional on V, but there is no g with $L(f) = (f | g)$, unless $c_1 = c_2 = \ldots = c_n = 0$. Just repeat the above argument with $h = (x - z_1) \ldots (x - z_n)$ in the Example 1.

We turn now to the concept of the adjoint of a linear operator.

5.2 Adjoint of Linear Operators

Theorem 2: For any linear operator T on a finite-dimensional inner product space V, there exists a unique linear operator T^* on V such that

$$(T\alpha \mid \beta) = (\alpha \mid T^*\beta) \qquad \ldots(2)$$

for all α, β in V.

Proof: Let β be any vector in V. Then $\alpha \to (T\,\alpha|\beta)$ is a linear functional on V. By Theorem 1 there is a unique vector β' in V such that $(T\,\alpha|\beta) = (\alpha \mid \beta')$ for every α in V. Let T^* denote the mapping

$\beta \rightarrow \beta'$:

$$\beta' = T^*\beta.$$

We have (2), but we must verify that T^* is a linear operator. Let β, γ be in V and let c be a scalar. Then for any α,

$$\begin{aligned} (\alpha|T^* (c\beta + \gamma)) &= (T\alpha \mid c\beta + \gamma) \\ &= (T\alpha \mid c\beta) + (T\alpha \mid \gamma) \\ &= \bar{c}(T\alpha \mid \beta) + (T\alpha \mid \gamma) \\ &= \bar{c}(\alpha \mid T^*\beta) + (\alpha \mid T^*\gamma) \\ &= (\alpha \mid cT^* \beta) + (\alpha \mid T^*\gamma) \\ &= (\alpha \mid c\, T^*\beta + T^*\gamma). \end{aligned}$$

Thus $T^* (c\beta + \gamma) = cT^* \beta + T^*\gamma$ and T^* is linear operator.

The uniqueness of T^* is clear. For any β in V, the vector $T^*\beta$ is uniquely determined as the vector β' such that $(T\alpha \mid \beta') = (\alpha \mid \beta')$ for every α.

Theorem 3: Let V be a finite-dimensional inner product space and let $\mathcal{B} = \{\alpha_1, ..., \alpha_n\}$ be an (ordered) orthonormal basis for V. Let T be a linear operator on V and let A be the matrix of T in the ordered basis $\mathcal{B}$. Then $A_{kj} = (T\alpha_j \mid \alpha_k)$.

Proof: Since $\mathcal{B}$ is an orthonormal basis, we have

$$\alpha = \sum_{k=1}^{n} (\alpha \mid \alpha_k)\alpha_k.$$

The matrix A is defined by

$$T\alpha_j = \sum_{k=1}^{n} A_{k_j}\alpha_k$$

and since

$$T\alpha_j = \sum_{k=1}^{n} (T\alpha_j \mid \alpha_k)\alpha_k$$

we have $A_{k_j} = (T\alpha_j \mid \alpha_k)$.

Corollary: Let V be a finite-dimensional inner product space, and let T be a linear operator on V. In any orthonormal basis for V, the matrix of T^* is the conjugate transpose of the matrix of T.

Proof: Let $\mathcal{B} = \{\alpha_1, ..., \alpha_n\}$ be an orthonormal basis for V, let $A = [T]_{\mathcal{B}}$ and $B = [T^*]_{\mathcal{B}}$. According to Theorem 3,

$$\begin{aligned} A_{kj} &= (T\alpha_j \mid \alpha_k) \\ B_{kj} &= (T^* \alpha_j \mid \alpha_k). \end{aligned}$$

By the definition of T^* we then have

$$\begin{aligned} B_{kj} &= (T^* \alpha_j \mid \alpha_k) \\ &= \overline{(\alpha_k \mid T^* \alpha_j)} \end{aligned}$$

$$= \overline{(T\alpha_k \mid \alpha_j)}$$

$$= \overline{A_{jk}}.$$

Example 2: Let V be a finite-dimensional inner product space and E the orthogonal projection of V on a subspace W. The for any vectors α and β in V.

$$\begin{aligned}(E\alpha|\beta) &= (E\alpha|E\beta + (1 - E)\beta)\\ &= (E\alpha|E\beta)\\ &= (E\alpha + (1 - E)\alpha|E\beta)\\ &= (\alpha|E\beta)\end{aligned}$$

From the uniqueness of the operator E^* it follows that $E^* = E$. Now consider the projection E described in Example 14 of unit 24. Then

$$A = \frac{1}{154}\begin{bmatrix} 9 & 36 & -3 \\ 36 & 144 & -12 \\ -3 & -12 & 1 \end{bmatrix}$$

is the matrix of E in the standard orthonormal basis. Since $E = E^*$, A is also the matrix of E^*, and because $A = A^*$, this does not contradict the preceding corollary. On the other hand, suppose

$$\begin{aligned}\alpha_1 &= (154, 0, 0)\\ \alpha_2 &= (145, -36, 3)\\ \alpha_3 &= (-36, 10, 12)\end{aligned}$$

Then $\{\alpha_1, \alpha_2, \alpha_3\}$ is a basis, and

$$\begin{aligned}E\alpha_1 &= (9, 36, -3)\\ E\alpha_2 &= (0, 0, 0)\\ E\alpha_3 &= (0, 0, 0)\end{aligned}$$

Since $(9, 36, -3) = -(154, 0, 0) - (145, -36, 3)$, the matrix B of E in the basis $\{\alpha_1, \alpha_2, \alpha_3\}$ is defined by the equation

$$B = \begin{bmatrix} -1 & 0 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

In this case $B \neq B^*$, and B^* is not the matrix of $E^* = E$ in the basis $\{\alpha_1, \alpha_2, \alpha_3\}$. Applying the corollary, we conclude that $\{\alpha_1, \alpha_2, \alpha_3\}$ is not an orthonormal basis. Of course this is quite obvious anyway.

Definition: Let T be a linear operator on an inner product space V. Then we say that T has an adjoint on V if there exists a linear operator T^* on V such that $(T\alpha|\beta) = (\alpha|T^*\beta)$ for all α and β in V.

By Theorem 2 every linear operator on a finite-dimensional inner product space V has an adjoint on V. In the finite-dimensional case this is not always true. But in any case there is at most one such operator T^*; when it exists, we call it the adjoint of T.

Two comments should be made about the finite-dimensional case.

1. The adjoint of T depends not only on T but on the inner product as well.

2. As shown by example 2, in an arbitrary ordered basis $\mathcal{B}$, the relation between $[T]_{\mathcal{B}}$ and $[T^*]_{\mathcal{B}}$ is more complicated than that given in the corollary above.

Example 3: Let V be $C^{n\times 1}$, the space of complex $n \times 1$ matrices, with inner product $(X/Y) = Y * X$. If A is an $n \times n$ matrix with complex entries, the adjoint of the linear operator $X \to AX$ is the operator $X \to A * X$. For

$$(AX|Y) = Y^*AX = (A^*Y)^*X = (X|A^*Y)$$

Example 4: This is similar to Example 3. Let V be $C^{n\times n}$ with the inner product $(A|B) = \text{tr}\,(B^*A)$. Let M be a fixed $n \times n$ matrix over C. The adjoint of left multiplication by M is left multiplication by M^*. Of course, 'left multiplication by M' is the linear operator L_M defined by $L_M(A) = MA$.

$$\begin{aligned}(L_M(A)|B) &= \text{tr}\,(B^*(MA)) \\ &= \text{tr}\,(MAB^*) \\ &= \text{tr}\,(AB^*M) \\ &= \text{tr}\,(A(M^*B)^*) \\ &= (A|L_M^*(B)).\end{aligned}$$

Thus $(L_M)^* = L_{M^*}$. In the computation above, we twice used the characteristic property of the trace function: $\text{tr}\,(AB) = \text{tr}\,(BA)$.

Example 5: Let V be the space of polynomials over the field of complex numbers, with the inner product.

$$(f|g) = \int_0^1 f(t)\overline{g(t)}dt.$$

If f is a polynomial, $f = \Sigma\, a_k x^k$, we let $\bar{f} = \Sigma \bar{a}_k x^k$. That is, $\bar{f}$ is the polynomial whose associated polynomial function is the complex conjugate of that for f:

$$\bar{f}(t) = \overline{f(t)}, \qquad t \text{ real}$$

Consider the operator 'multiplication by f,' that is, the linear operator M_f defined by $M_f(g) = fg$. Then this operator has an adjoint, namely, multiplication by $\bar{f}$. For

$$\begin{aligned}(M_f(g)|h) &= (fg|h) \\ &= \int_0^1 f(t)g(t)\overline{h(t)}\,dt \\ &= \int_0^1 g(t)[\overline{\overline{f(t)}h(t)}]\,dt \\ &= (g\,|\,\bar{f}h) \\ &= (g\,|\,M_{\bar{f}}(h))\end{aligned}$$

and so $(M_{\bar{f}})^* = M_f$.

Notes

Example 6: In Example 5, we saw that some linear operators on an infinite-dimensional inner product space do have an adjoint. As we commented earlier, some do not. Let V be the inner product space of Example 6, and let D be the differentiation operator on $C[x]$. Integration by parts shows that

$$(Df|g) = f(1)g(1) - f(0)\,g(0) - (f|Dg).$$

Let us fix g and inquire when there is a polynomial D^*g such that $(Df|g) = (f|D^*g)$ for all f. If such a D^*g exists, we shall have

$$(f|D^*g) = f(1)\,g(1) - f(0)\,g(0) - (f|Dg)$$

or

$$(f|D^*g + Dg) = f(1)\,g(1) - f(0)\,g(0).$$

With g fixed, $L(f) = f(1)\,g(1) - f(0)\,g(0)$ is a linear functional of the type considered in Example 1 and cannot be of the form $L(f) = (f|h)$ unless $L = 0$. If D^*g exists, then with $h = D^*g + Dg$ we do have $L(f) = (f|h)$, and so $g(0) = g(1) = 0$. The existence of a suitable polynomial D^*g implies $g(0) = g(1) = 0$. Conversely, if $g(0) = g(1) = 0$, the polynomial $D^*g = -Dg$ satisfies $(Df|g) = (f|D^*g)$ for all f. If we choose any g for which $g(0) \neq 0$ or $g(1) \neq 0$, we cannot suitable define D^*g, and so we conclude that D has no adjoint.

We hope that these examples enhance the reader's understanding of the adjoint of a linear operator. We see that the adjoint operation, passing from T to T^*, behaves somewhat like conjugation on complex numbers. The following theorem strengthens the analogy.

Theorem 4: Let V be a finite-dimensional inner product space. If T and U are linear operators on V and c is a scalar,

(i) $(T + U)^* = T^* + U^*$;

(ii) $(cT)^* = \bar{c}\,T^*$;

(iii) $(TU)^* = U^*T^*$;

(iv) $(T^*) = T$.

Proof: To prove (i), let α and β be any vectors in V.

Then

$$\begin{aligned}((T + U)\,\alpha|\beta) &= (T\alpha + U\,\alpha|\beta)\\ &= (T\alpha|\beta) + (U\,\alpha|\beta)\\ &= (\alpha|T^*\beta) + (\alpha\,|\,U^*\beta)\\ &= (\alpha|T^*\beta + U^*\beta)\\ &= (\alpha|\,(T^* + U^*)\,\beta)\end{aligned}$$

From the uniqueness of the adjoint we have $(T + U)^* = T^* + U^*$. We leave the proof of (ii) to the reader. We obtain (iii) and (iv) from the relations

$$(TU\alpha|\beta) = (U\alpha|T^*\beta) = (\alpha|U^*T^*\beta)$$

$$(T^*\alpha|\beta) = \overline{(\beta\,|\,T^*\alpha)} = \overline{(T\beta/\alpha)} = (\alpha\,|\,T\beta).$$

Theorem 4 is often phrased as follows: the mapping $T \to T^*$ is a conjugate-linear anti-isomorphism of period 2. The analogy with complex conjugation which we mentioned above is, of course,

Notes

based upon the observation that complex conjugation has the properties $\overline{(z_1 + z_2)} = \overline{z}_1 + \overline{z}_2, \overline{(z_1 z_2)} = \overline{z}_1\overline{z}_2, \overline{\overline{z}} = z$. One must be careful to observe the reversal of order in a product, which the adjoint operation imposes: $(UT)^* = T^*U^*$. We shall mention extensions of this analogy as we continue our study of linear operators on an inner product space. We might mention something along these lines now. A complex number z is real if the only if $z = \overline{z}$. One might expect that the linear operators T such that $T = T^*$ behave in some way like the real numbers. This is in fact the case. For example, if T is a linear operator on a finite-dimensional *complex* inner product space, then

$$T = U_1 + iU_2$$

where $U_1 = U_1^*$ and $U_2 = U_2^*$. Thus, in some sense, T has a 'real part' and an 'imaginary part.' The operators U_1 and U_2 satisfying $U_1 = U_1^*$, and $U_2 = U_2^*$, and are unique, and are given by

$$U_1 = \frac{1}{2}(T + T^*)$$

$$U_2 = \frac{1}{2i}(T - T^*).$$

A linear operator T such that $T = T^*$ is called **self-adjoint** (for **Hermitian**). If $\mathcal{B}$ is an orthonormal basis for V, then

$$[T^*]_{\mathcal{B}} = [T]_{\mathcal{B}}^*$$

and so T is self-adjoint if and only if its matrix in every orthonormal basis is a self-adjoint matrix. Self-adjoint operators are important, not simply because they provide us with some sort of real and imaginary part for the general linear operator, but for the following reasons: (1) Self-adjoint operators have many special properties. For example, for such an operator there is an orthonormal basis of characteristic vectors. (2) Many operators which arise in practice are self-adjoint. We shall consider the special properties of self-adjoint operators later.

Self Assessment

1. Let V be a finite-dimensional inner product space T a linear operator on V. If T is invertible, show that T^* is invertible and $(T^*)^{-1} = (T^{-1})^*$.
2. Show that the product of two self-adjoint operators is self-adjoint if any only if the two operators commute.

5.3 Summary

- The linear functional f concept is also a form of inner product on a finite-dimensional inner product space.
- The fact that f has the form $f(\alpha) = (\alpha|\beta)$ for some β in V helps us to prove the existence of the 'adjoint' of a linear operator T on V.
- A linear operator T such that $T = T^*$ is called self-adjoint (or Hermitian) and so T is self- adjoint if and only if its matrix in every orthonormal basis is a self-adjoint matrix.

5.4 Keywords

A linear functional f on a finite dimensional inner product space is 'inner-product with a fixed vector in the space'. Let β be some fixed vector in any inner product space V, we then define a function f_β from V into the scalar field by

$$f_\beta(\alpha) = (\alpha \mid \beta)$$

A linear operator T^* is an adjoint of T on V, such that $(T\alpha|\beta) = (\alpha|T^*\beta)$ for all α and β in V.

Self-adjoint (or Hermitian): A linear operator T such that $T = T^*$ is called self-adjoint (or Hermitian). If β is an orthonormal basis for V, then $[T^*] = [T]^*_\beta$ and so a self-adjoint if and only if its matrix in every orthonormal basis is a self-adjoint matrix.

5.5 Review Questions

1. Let T be the linear operator on C^2 defined by $T\varepsilon_1 = (1 + i, 2)$, $T\varepsilon_2 = (i, i)$. Using the standard inner product, find the matrix of T^* in the standard ordered basis.

2. Let V be a finite-dimensional inner product space and T a linear operator V. Show that the range of T^* is the orthogonal complement of the null space of T.

5.6 Further Readings

Books

Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I N. Herstein, *Topics in Algebra*

Michael Artin, *Algebra*

Unit 6: Unitary Operators and Normal Operators

CONTENTS

Objectives

Introduction

6.1 Unitary Operators

6.2 Normal Operators

6.3 Summary

6.4 Keywords

6.5 Review Questions

6.6 Further Readings

Objectives

After studying this unit, you will be able to:

- Understand the meaning of unitary operators, i.e. a unitary operator on an inner product space is an isomorphism of the space onto itself.
- See that unitary and orthogonal matrices are explained with the help of some examples.
- Understand that for each invertible $n \times n$ matrix B in the general linear group $GL(n)$ there exist unique unitary matrix U and lower triangular matrix M such that $U = MB$.
- Know that the linear operator T is normal if it commutes with its adjoint $TT^* = T^*T$.
- Understand that for every normal matrix A there is a unitary matrix P such that $P^{-1}AP$ is a diagonal matrix.

Introduction

In this unit there are two sections – one dealing with unitary operators on finite dimensional inner product spaces and other dealing with the normal operators.

It is shown that if an $n \times n$ matrix B belongs to $GL(n)$ then there exist unique matrices N and U such that N is in $T^+(n)$, U is in $U(n)$, and $B = N.U$.

In the second section properties of normal operators are studied. It is seen that a complex $n \times n$ matrix A is said to be normal if $A^*A = AA^*$.

With the help of some theorems it is shown that for a normal operator T on V, a finite dimensional complex inner product space, V has an orthonormal basis consisting of characteristic vectors for T.

6.1 Unitary Operators

In this unit we first of all consider the concept of an isomorphism between two inner product spaces. An isomorphism of two vector spaces V onto W is a one-one linear transformation from V onto W. Now an inner product space consists of a vector space and a specified inner product on that space. Thus, when V and W are inner product spaces, we shall require an isomorphism from

V onto W not only to preserve the linear operations, but also to preserve products. An isomorphism of an inner product space onto itself is called a '*unitary operator*' on that space. Some of the basic properties of unitary operators are being established in the section along with some examples.

Definition: Let V and W be inner product spaces over the same field and let T be a linear transformation from V onto W. We say that T-preserves inner products if $(T\alpha \backslash T\beta) = (\alpha \backslash \beta)$ for all α, β in V. An isomorphism of V onto W is a vector space isomorphism T of V onto W which also preserves inner products.

If T preserves inner products then $\| T\alpha \| = \| \alpha \|$ and so T is non-singular. Thus if T is an isomorphism of V onto W, then T^{-1} is an isomorphism of W onto V; hence, when such a T exists, we shall simply say V and W are isomorphic. Of course, isomorphism of inner product spaces is an equivalence relation.

Theorem 1: Let V and W be finite-dimensional inner product spaces over the same field, having the same dimension. If T is a linear transformation from V into W, the following are equivalent.

(i) T preserves inner products.

(ii) T is an (inner product space) isomorphism.

(iii) T carries every orthonormal basis for V onto an orthonormal basis for W.

(iv) T carries some orthonormal basis for V onto an orthonormal basis for W.

Proof: (i) $\to$ (ii) If T preserves inner products, then $\| T\alpha \| = \| \alpha \|$ for all α in V. Thus T is non-singular, and since dim V = dim W, we know that T is a vector space isomorphism.

(ii) $\to$ (iii) Suppose T is an isomorphism. Let $\{\alpha_1, \ldots, \alpha_n\}$ be an orthonormal basis for V. Since T is a vector space isomorphism and dim W = dim V, it follows that $\{T\alpha_1, \ldots, T\alpha_n\}$ is a basis for W. Since T also preserves inner products, $\{T\alpha_1 \mid T\alpha_k\} = (\alpha_j \mid \alpha_k) = \delta_{jk}$.

(iii) $\to$ (iv) This requires no comment.

(iv) $\to$ (i) Let $\{\alpha_1, \ldots, \alpha_n\}$ be an orthonormal basis for V such that $\{T\alpha_1, \ldots, T\alpha_n\}$ is an orthonormal basis for W. Then

$$(T\alpha_j \mid T\alpha_k) = (\alpha_j \mid \alpha_k) = \delta_{jk}.$$

For any $\alpha = x_1\alpha_1 + \ldots + x_n\alpha_n$ and $\beta = y_1\alpha_1 + \ldots + y_n\alpha_n$ in V, we have

$$(\alpha \mid \beta) = \sum_{j=1}^{n} x_j \bar{y}_j$$

$$(T\alpha \mid T\beta) = \left(\sum_j x_j T\alpha_j \middle| \sum_k y_k T\alpha_k \right)$$

$$= \sum_j \sum_k x_j \bar{y}_k (T\alpha_j \mid T\alpha_k)$$

$$= \sum_{j=1}^{n} x_j \bar{y}_j$$

and so T preserves inner products.

Notes

Example 1: If V is an n-dimensional inner product space, then each ordered orthonormal basis $\beta = \{\alpha_1, \ldots, \alpha_n\}$ determines an isomorphism of V onto F^n with the standard inner product. The isomorphism is simply

$$T(x_1\alpha_1 + \ldots + x_n\alpha_n) = (x_1, \ldots, x_n).$$

There is the superficially different isomorphism which β determines of V onto the space $F^{n\times 1}$ with $(X|Y) = Y^*X$ as inner product. The isomorphism is

$$\alpha \to [\alpha]_B$$

i.e., the transformation sending α into its coordinate matrix in the ordered basis β. For any ordered basis β, this is a vector space isomorphism; however, it is an isomorphism of the two inner product spaces if and only if β is orthonormal.

Example 2: Here is a slightly less superficial isomorphism. Let W be the space of all 3×3 matrices A over R which are skew-symmetric, i.e., $A^t = -A$. We equip W with the inner product $(A|B) = \frac{1}{2}\,\mathrm{tr}\,(AB^t)$, the $\frac{1}{2}$ being put in as a matter of convenience. Let V be the space R^3 with the standard inner product. Let T be the linear transformation from V into W defined by

$$T(x_1, x_2, x_3) = \begin{bmatrix} 0 & -x_3 & x_2 \\ x_3 & 0 & -x_1 \\ -x_2 & x_1 & 0 \end{bmatrix}$$

Then T maps V onto W, and putting

$$A = \begin{bmatrix} 0 & -x_3 & x_2 \\ x_3 & 0 & -x_1 \\ -x_2 & x_1 & 0 \end{bmatrix}, \; B = \begin{bmatrix} 0 & -y_3 & y_2 \\ y_3 & 0 & -y_1 \\ -y_2 & y_1 & 0 \end{bmatrix}$$

we have

$$\begin{aligned} tr\,(AB^t) &= x_3y_3 + x_2y_2 + x_3y_3 + x_2y_2 + x_1y_1 \\ &= 2\,(x_1y_1 + x_2y_2 + x_3y_3). \end{aligned}$$

Thus $(\alpha|\beta) = (T\alpha|T\beta)$ and T is a vector space isomorphism. Note that T carries the standard basis $(\in_1, \in_2, \in_3)$ onto the orthonormal basis consisting of the three matrices

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix}, \; \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix}, \; \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Example 3: It is not always particularly convenient to describe an isomorphism in terms of orthonormal bases. For example, suppose $G = P^*P$ where P is an invertible $n \times n$ matrix with complex entries. Let V be the space of complex $n \times 1$ matrices, with the inner product $[X|Y] = Y^*GX$.

Let W be the same vector space, with the standard inner product $(X|Y) = Y^*X$. We know that V and W are isomorphic inner product spaces. It would seem that the most convenient way to describe an isomorphism between V and W is the following: Let T be the linear transformation from V into W defined by $T(X) = PX$. Then

$$(TX|TY) = (PX|PY)$$

$$= (PY)^*(PX)$$
$$= Y^*P^*PX$$
$$= Y^*GX$$
$$= [X \mid Y].$$

Hence T is an isomorphism.

Example 4: Let V be the space of all continuous real-valued functions on the unit interval, $0 \leq t \leq 1$, with the inner product

$$[f \mid g] = \int_0^1 f(t)g(t)t^2\, dt\,.$$

Let W be the same vector space with the inner product

$$(f \mid g) = \int_0^1 f(t)g(t)\, dt\,.$$

Let T be the linear transformation from V into W given by

$$(Tf)(t) = tf(t).$$

Then $(Tf \mid Tg) = [f \mid g]$, and so T preserves inner products; however, T is not an isomorphism of V onto W, because the range of T is not all of W. Of course, this happens because the underlying vector space is not finite dimensional.

Theorem 2: Let V and W be inner product spaces over the same field, and let T be a linear transformation from V into W. Then T preserves inner products if and only if $\| T\alpha \| = \| \alpha \|$ for every α in V.

Proof: If T preserves inner products, T 'preserves norms'. Suppose $\| T\alpha \| = \| \alpha \|$ for every α in V. Then $\| T\alpha \|^2 = \| \alpha \|^2$. Now using the appropriate polarization identity and the fact that T is linear, one easily obtains $(\alpha \mid \beta) = (T\alpha \mid T\beta)$ for all α, β in V.

Definition: A unitary operator on an inner product space is an isomorphism of the space onto itself.

The product of two unitary operators is unitary. For, if U_1 and U_2 are unitary, then U_2U_1 is invertible and $\| U_2U_1\alpha \| = \| U_1\alpha \| = \| \alpha \|$ for each α. Also, the inverse of a unitary operator is unitary, since $\| U\alpha \| = \| \alpha \|$ says $\| U^{-1}\beta \| = \| \beta \|$, where $\beta = U\alpha$. Since the identity operator is clearly unitary, we see that the set of all unitary operators on an inner product space is a group, under the operation of composition.

If V is a finite-dimensional inner product space and U is a linear operator on V, Theorem 1 tells us that U is unitary if and only if $(U\alpha \mid U\beta) = (\alpha \mid \beta)$ for each α, β in V; or, if and only if for some (every) orthonormal basis $\{\alpha_1, \ldots, \alpha_n\}$ it is true that $\{U\alpha_1, \ldots, U\alpha_n\}$ is an orthonormal basis.

Theorem 3: Let U be a linear operator on an inner product space V. Then U is unitary if and only if the adjoint U^* of U exists and $UU^* = U^*U = I$.

Proof: Suppose U is unitary. Then U is invertible and

$$(U\alpha \mid \beta) = (U\alpha \mid UU^{-1}\beta) = (\alpha \mid U^{-1}\beta)$$

for all α, β. Hence U^{-1} is the adjoint of U.

Conversely, suppose U^* exists and $UU^* = U^*U = I$. Then U is invertible, with $U^{-1} = U^*$. So, we need only show that U preserves inner products.

Notes

We have

$$(U\alpha \mid U\beta) = (\alpha \mid U^*U\beta)$$
$$= (\alpha \mid I\beta)$$
$$= (\alpha \mid \beta)$$

for all α, β.

Example 5: Consider $C^{n\times 1}$ with the inner product $(X \mid Y) = Y^*X$. Let A be an $n \times n$ matrix over C, and let U be the linear operator defined by $U(X) = AX$. Then

$$(UX \mid UY) = (AX \mid AY) = Y^*A^*AX$$

for all X, Y. Hence, U is unitary if and only if $A^*A = I$.

Definition: A complex $n \times n$ matrix A is called unitary, if $A^*A = I$.

Theorem 4: Let V be a finite-dimensional inner product space and let U be a linear operator on V. Then U is unitary if and only if the matrix of U in some (or every) ordered orthonormal basis is a unitary matrix.

Proof: At this point, this is not much of a theorem, and we state it largely for emphasis. If $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$ is an ordered orthonormal basis for V and A is the matrix of U relative to $\mathcal{B}$, then $A^*A =$ I if and only if $U^*U = I$. The result now follows from Theorem 3.

Let A be an $n \times n$ matrix. The statement that A is unitary simply means

$$(A^*A)_{jk} = \delta_{jk}$$

or

$$\sum_{r=1}^{n} \overline{A_{rj}} A_{rk} = \delta_{jk}$$

In other words, it means that the columns of A form an orthonormal set of column matrices, with respect to the standard inner product $(X \mid Y) = Y^*X$. Since $A^*A = I$ if and only if $AA^* = I$, we see that A is unitary exactly when the rows of A comprise an orthonormal set of n-tuples in C_n (with the standard inner product). So, using standard inner products, A is unitary if and only if the rows and columns of A are orthonormal sets. One sees here an example of the power of the theorem which states that a one-sided inverse for a matrix is a two-sided inverse. Applying this theorem as we did above, say to real matrices, we have the following: Suppose we have a square array of real numbers such that the sum of the squares of the entries in each row is 1 and distinct rows are orthogonal. Then the sum of the squares of the entries in each column is 1 and distinct columns are orthogonal. Write down the proof of this for a 3×3 array, without using any knowledge of matrices, and you should be reasonably impressed.

Definition: A real or complex $n \times n$ matrix A is said to be orthogonal, if $A^tA = I$.

A real orthogonal matrix is unitary; and, a unitary matrix is orthogonal if and only if each of its entries is real.

Example 6: We give some examples of unitary and orthogonal matrices.

(a) A 1×1 matrix $[c]$ is orthogonal if and only if $c = \pm 1$, and unitary if and only if $\bar{c}c = 1$. The latter condition means (of course) that $|c| = 1$, or $c = e^{i\theta}$, where θ is real.

(b) Let

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Then A is orthogonal if and only if

$$A^t = A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

The determinant of any orthogonal matrix is easily seen to be ± 1. Thus A is orthogonal if and only if

$$A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

or $$A = \begin{bmatrix} a & b \\ b & -a \end{bmatrix}$$

where $a^2 + b^2 = 1$. The two cases are distinguished by the value of det A.

(*c*) The well-known relations between the trigonometric functions show that the matrix

$$A_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

is orthogonal. If θ is a real number, then A_θ is the matrix in the standard ordered basis for R^2 of the linear operator U_θ, rotation through the angle θ. The statement that A_θ is a real orthogonal matrix (hence unitary) simply means that U_θ is a unitary operator, i.e., preserves dot products.

(*d*) Let

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Then A is unitary if and only if

$$\begin{bmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{bmatrix} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

The determinant of a unitary matrix has absolute value 1, and is thus a complex number of the form $e^{i\theta}$, θ real. Thus A is unitary if and only if

$$A = \begin{bmatrix} a & b \\ -e^{i\theta}\bar{b} & e^{i\theta}\bar{a} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}\begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}$$

where θ is a real number, and a, b are complex numbers such that $|a|^2 + |b|^2 = 1$.

As noted earlier, the unitary operators on an inner product space form a group. From this and Theorem 4 it follows that the set $U(n)$ of all $n \times n$ unitary matrices is also a group. Thus the inverse of a unitary matrix and the product of two unitary matrices are again unitary. Of course this is easy to see directly. An $n \times n$ matrix A with complex entries is unitary if and only if $A^{-1} = A^*$. Thus, if A is unitary, we have $(A^{-1})^{-1} = A = (A^*)^{-1} = (A^{-1})^*$. If A and B are $n \times n$ unitary matrices, then $(AB)^{-1} = B^{-1}A^{-1} = B^*A^* = (AB)^*$.

The Gram-Schmidt process in C^n has an interesting corollary for matrices that involves the group $U(n)$.

Theorem 5: For every invertible complex $n \times n$ matrix B there exists a unique lower-triangular matrix M with positive entries on the main diagonal such that MB is unitary.

Notes

Proof: The rows $\beta_1, \ldots, \beta_n$ of B form a basis for C^n. Let $\alpha_1, \ldots, \alpha_n$ be the vectors obtained from $\beta_1, \ldots, \beta_n$ by the Gram-Schmidt process. Then, for $1 \le k \le n$, $\{\alpha_1, \ldots, \alpha_k\}$ is an orthogonal basis for the subspace spanned by $\{\beta_1, \ldots, \beta_k\}$, and

$$\alpha_k = \beta_k - \sum_{j<k} \frac{(\beta_k \mid \alpha_j)}{\|\alpha_j\|^2} \alpha_j .$$

Hence, for each k there exist unique scalars C_{k_j} such that

$$\alpha_k = \beta_k - \sum_{j<k} C_{k_j} \beta_j .$$

Let U be the unitary matrix with rows

$$\frac{\alpha_1}{\|\alpha_1\|}, \ldots, \frac{\alpha_n}{\|\alpha_n\|}$$

and M the matrix defined by

$$M_{k_j} = \begin{cases} -\dfrac{1}{\|\alpha_k\|} \cdot C_{k_j}, & \text{if } j < k \\ \dfrac{1}{\|\alpha_k\|}, & \text{if } j = k \\ 0, & \text{if } j > k \end{cases}$$

Then M is lower-triangular, in the sense that its entries above the main diagonal are 0. The entries M_{kk} of M on the main diagonal are all > 0, and

$$\frac{\alpha_k}{\|\alpha_k\|} = \sum_{j=1}^{n} M_{kj} \beta_j, \quad 1 \le k \le n .$$

Now these equations simply say that

$$U = MB.$$

To prove the uniqueness of M, let $T^+(n)$ denote the set of all complex $n \times n$ lower-triangular matrices with positive on the main diagonal. Suppose M_1 and M_2 are elements of $T^+(n)$ such that M_iB is in $U(n)$ for $i = 1, 2$. Then because $U(n)$ is a group

$$(M_1B)\ (M_2B)^{-1} = M_1M_2^{-1}$$

lies in $U(n)$. On the other hand, although it is not entirely obvious, $T^+(n)$ is also a group under matrix multiplication. One way to see this is to consider the geometric properties of the linear transformations

$$X \to MX, \ (M \text{ in } T^+(n))$$

on the space of column matrices. Thus M_2^{-1}, $M_1M_2^{-1}$, and $(M_1M_2^{-1})^{-1}$ are all in $T^+(n)$. But, since $M_1M_2^{-1}$ is in U(n), $(M_1M_2^{-1})^{-1} = (M_1M_2^{-1})^*$. The transpose or conjugate transpose of any lower-triangular matrix is an upper-triangular matrix. Therefore, $M_1M_2^{-1}$ is simultaneously upper and lower-triangular, i.e., diagonal. A diagonal matrix is unitary if and only if each of its entries on the main diagonal has absolute value 1; if the diagonal entries are all positive, they must equal 1. Hence $M_1M_2^{-1} = I$ and $M_1 = M_2$.

Notes

Let $GL(n)$ denote the set of all invertible complex $n \times n$ matrices. Then $GL(n)$ is also a group under matrix multiplication. This group is called the **general linear group**. Theorem 5 is equivalent to the following result.

Corollary: For each B in $GL(n)$ there exist unique matrices N and U such that N is in $T^{+}(n)$, U is in $U(n)$, and

$$B = N \cdot U.$$

Proof: By the theorem there is a unique matrix M in $T^{+}(n)$ such that MB is in $U(n)$. Let $MB = U$ and $N = M^{-1}$. Then N is in $T^{+}(n)$ and $B = N \cdot U$. On the other hand, if we are given any elements N and U such that N is in $T^{+}(n)$, U is in $U(n)$, and $B = N \cdot U$, then $N^{-1}B$ is in $U(n)$ and N^{-1} is the unique matrix M which is characterized by the theorem; furthermore U is necessarily $N^{-1}B$.

Example 7: Let x_1 and x_2 be real numbers such that $x_1^2 + x_2^2 = 1$ and $x_1 \neq 0$. Let

$$B = \begin{bmatrix} x_1 & x_2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Applying the Gram-Schmidt process to the rows of B, we obtain the vectors

$$\begin{aligned} \alpha_1 &= (x_1, x_2, 0) \\ \alpha_2 &= (0, 1, 0) - x_2 (x_1, x_2, 0) \\ &= x_1 (-x_2, x_1, 0) \\ \alpha_3 &= (0, 0, 1). \end{aligned}$$

Let U be the matrix with rows α_1, (α_2/x_1), α_3. Then U is unitary, and

$$U = \begin{bmatrix} x_1 & x_2 & 0 \\ -x_2 & x_1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ -\dfrac{x_2}{x_1} & \dfrac{1}{x_1} & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 & x_2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Now multiplying by the inverse of

$$M = \begin{bmatrix} 1 & 0 & 0 \\ -\dfrac{x_2}{x_1} & \dfrac{1}{x_1} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

we find that

$$\begin{bmatrix} x_1 & x_2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ x_2 & x_1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 & x_2 & 0 \\ -x_2 & x_1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Let us now consider briefly change of coordinates in an inner product space. Suppose V is a finite-dimensional inner product space and that $\beta = \{\alpha_1, \ldots, \alpha_n\}$ and $\beta' = \{\alpha'_1, \ldots, \alpha'_n\}$ are two ordered orthonormal bases for V. There is a unique (necessarily invertible) $n \times n$ matrix P such that

$$[\alpha]_{\beta'} = P^{-1}[\alpha]_{\beta}$$

for every α in V. If U is the unique linear operator on V defined by $U\alpha_j = \alpha'_j$, then P is the matrix of U in the ordered basis B:

$$\alpha'_k = \sum_{j=1}^{n} P_{jk}\alpha_j \ .$$

Since β and β' are orthonormal bases, U is a unitary operator and P is a unitary matrix. If T is any linear operator on V, then

$$[\mathrm{T}]_{\beta'} = P^{-1}[T]_{\beta}P = P^{*}[T]_{\beta}P.$$

Definition: Let A and B be complex $n \times n$ matrices. We say that B is unitarily equivalent to A if there is an $n \times n$ unitary matrix P such that $B = P^{-1}AP$. We say that B is orthogonally equivalent to A if there is an $n \times n$ orthogonal matrix P such that $B = P^{-1}AP$.

With this definition, what we observed above may be stated as follows: If β and β' are two ordered orthonormal bases for V, then, for each linear operator T on V, the matrix $[T]_{B'}$ is unitarily equivalent to the matrix $[T]_{B}$. In case V is a real inner product space, these matrices are orthogonally equivalent, via a real orthogonal matrix.

Self Assessment

1. Let B given by

$$B = \begin{bmatrix} 3 & 0 & 4 \\ -1 & 0 & 7 \\ 2 & 9 & 11 \end{bmatrix}$$

is 3 × 3 invertible matrix. Show that there exists a unique lower triangular matrix M with positive entries on the main diagonal such that MB is unitary. Find M and MB.

2. Let V be a complex inner product space and T a self-adjoint linear operator on V. Show that

   (i) $I + i\,T$ is non-singular

   (ii) $I - i\,T$ is non-singular

   (iii) $(I - i\,T)\,(I + i\,T)^{-1}$ is unitary.

6.2 Normal Operators

In this section we are interested in finding out the fact that there is an orthonormal basis β for V such that the matrix of the linear operator T on a finite dimensional inner product space V, in the basis β is diagonal.

We shall begin by deriving some conditions on T which will be subsequently shown to be sufficient. Suppose $\beta = (\alpha_1, \ldots, \alpha_n)$ is an orthonormal basis for V with the property

$$T\alpha_j = C_j a_j,\ j = 1, 2, \ldots n \qquad \ldots (1)$$

This simply says that T in this ordered basis is a diagonal matrix with diagonal entries $c_1, c_2, \ldots$ c_n. If V is a real inner product space, the scalars $c_1, \ldots, c_n$ are (of course) real, and so it must be that $T = T^*$. In other words, if V is a finite-dimensional real inner product space and T is a linear operator for which there is an orthonormal basis of characteristic vectors, then T must be self-adjoint. If V is a complex inner product space, the scalars $c_1, \ldots, c_n$ need not be real, i.e., T need not be self-adjoint. But notice that T must satisfy

$$TT^* = T^*T. \qquad \ldots (2)$$

For, any two diagonal matrices commute, and since T and T^* are both represented by diagonal matrices in the ordered basis β, we have (2). It is a rather remarkable fact that in the complex case this condition is also sufficient to imply the existence of an orthonormal basis of characteristic vectors.

Definition: Let V be a finite-dimensional inner product space and T a linear operator on V. We say that T is normal if it commutes with its adjoint i.e., $TT^* = T^*T$.

Any self-adjoint operator is normal, as is any unitary operator. Any scalar multiple of a normal, operator is normal; however, sums and products of normal operators are not generally normal. Although it is by no means necessary, we shall begin our study of normal operators by considering self-adjoint operators.

Theorem 6: Let V be an inner product space and T a self-adjoint linear operator on V. Then each characteristic value of T is real, and characteristic vectors of T associated with distinct characteristic values are orthogonal.

Proof: Suppose c is a characteristic value of T, i.e., that $T\alpha = c\alpha$ for some non-zero vector α. Then

$$\begin{aligned} c(\alpha\,|\,\alpha) &= (c\alpha\,|\,\alpha) \\ &= (T\alpha\,|\,\alpha) \\ &= (\alpha\,|\,T\alpha) \\ &= (\alpha\,|\,c\alpha) \\ &= \bar{c}(\alpha\,|\,\alpha) \end{aligned}$$

Since $(\alpha\,|\,\alpha) \neq 0$, we must have $c = \bar{c}$. Suppose we also have $T\beta = d\beta$ with $\beta \neq 0$. Then

$$\begin{aligned} c(\alpha\,|\,\beta) &= (T\alpha\,|\,\beta) \\ &= (\alpha\,|\,T\beta) \\ &= (\alpha\,|\,d\beta) \\ &= \bar{d}(\alpha\,|\,\beta) \\ &= d(\alpha\,|\,\beta) \end{aligned}$$

If $c \neq d$, then $(\alpha\,|\,\beta) = 0$.

It should be pointed out that Theorem 6 says nothing about the existence of characteristic values or characteristic vectors.

Theorem 7: On a finite-dimensional inner product space of positive dimension, every self-adjoint operator has a (non-zero) characteristic vector.

Proof: Let V be an inner product space of dimension n, where $n > 0$, and let T be a self-adjoint operator on V. Choose an orthonormal basis $\mathcal{B}$ for V and let $A = [T]_{\mathcal{B}}$. Since $T = T^*$, we have $A = A^*$. Now let W be the space of $n \times 1$ matrices over C, with inner product $(X\,|\,Y) = Y^*X$. Then $U(X) = AX$ defines a self-adjoint linear operator U on W. The characteristic polynomial, det $(xI - A)$, is a polynomial of degree n over the complex numbers; every polynomial over C of positive degree has a root. Thus, there is a complex number c such that det $(cI - A) = 0$. This means that $A - cI$ is singular, or that there exists a non-zero X such that $AX = cX$. Since the operator U (multiplication by A) is self-adjoint, it follows from Theorem 6 that c is real. If V is a real vector space, we may choose X to have real entries. For then A and $A - cI$ have real entries, and since $A - cI$ is singular, the system $(A - cI)X = 0$ has a non-zero real solution X. It follows that there is a non-zero vector α in V such that $T\alpha = c\alpha$.

There are several comments we should make about the proof.

1. The proof of the existence of a non-zero X such that $AX = cX$ had nothing to do with the fact that A was Hermitian (self-adjoint). It shows that any linear operator on a finite-dimensional complex vector space has a characteristic vector. In the case of a real inner product space, the self-adjointness of A is used very heavily, to tell us that each characteristic value of A is real and hence that we can find a suitable X with real entries.

2. The argument shows that the characteristic polynomial of a self-adjoint matrix has real coefficients, in spite of the fact that the matrix may not have real entries.

3. The assumption that V is finite-dimensional is necessary for the theorem; a self-adjoint operator on an infinite-dimensional inner product space need not have a characteristic value.

Example 8: Let V be the vector space of continuous complex-valued (or real-valued) continuous functions on the unit interval, $0 \le t \le 1$, with the inner product

$$(f|g) = \int_0^1 f(t)\overline{g(t)}\,dt\,.$$

The operator 'multiplication by t,' $(Tf)(t)$, is self-adjoint. Let us suppose that $Tf = cf$. Then

$$(t - c)\,f(t) = 0, \quad 0 \le t \le 1$$

and so $f(t) = 0$ for $t \ne c$. Since f is continuous, $f = 0$. Hence T has no characteristic values (vectors).

Theorem 8: Let V be a finite-dimensional inner product space, and let T be any linear operator on V. Suppose W is a subspace of V which is invariant under T. Then the orthogonal complement of W is invariant under T^*.

Proof: We recall that the fact that W is invariant under T does not mean that each vector in W is left fixed by T; it means that if α is in W then $T\alpha$ is in W. Let β be in $W^\perp$. We must show that $T^*\beta$ is in $W^\perp$, that is, that $(\alpha\,|\,(T^*\beta) = 0$ for every α in W. If α is in W, then $T\alpha$ is in W, so $(T\alpha\,|\,\beta) = 0$. But $(T\alpha\,|\,\beta) = (\alpha\,|\,T^*\beta)$.

Theorem 9: Let V be a finite-dimensional inner product space, and let T be a self-adjoint linear operator on V. Then there is an orthonormal basis for V, each vector of which is a characteristic vector for T.

Proof: We are assuming dim $V > 0$. By Theorem 7, T has a characteristic vector α. Let $\alpha_1 = \alpha/\|\alpha\|$ so that α_1 is also a characteristic vector for T and $\|\alpha_1\| = 1$. If dim $V = 1$, we are done. Now we proceed by induction on the dimension of V. Suppose the theorem is true for inner product spaces of dimension less than dim V. Let W be the one-dimensional subspace spanned by the vector α_1. The statement that α_1 is a characteristic vector for T simply means that W is invariant under T. By Theorem 8, the orthogonal complement $W^\perp$ is invariant under $T^* = T$. Now $W^\perp$, with the inner product from V, is an inner product space of dimension one less than the dimension of V. Let U be the linear operator induced on $W^\perp$ by T, that is the restriction of T to $W^\perp$. Then U is self-adjoint and by induction hypothesis, $W^\perp$ has an orthonormal basis $\{\alpha_2, \ldots, \alpha_n\}$ consisting of characteristic vectors for U. Now each of these vectors is also a characteristic vector for T, and since $V = W \oplus W^\perp$, we conclude that $\{\alpha_1, \ldots, \alpha_n\}$ is the desired basis for V.

Corollary: Let A be an $n \times n$ Hermitian (self-adjoint) matrix. Then there is a unitary matrix P such that $P^{-1}AP$ is diagonal (A is unitary equivalent to a diagonal matrix). If A is real symmetric matrix, there is a real orthogonal matrix P such that $P^{-1}AP$ is diagonal.

Proof: Let V be $C^{n\times 1}$, with the standard inner product, and let T be the linear operator on V which is represented by A in the standard ordered basis. Since $A = A^*$, we have $T = T^*$. Let $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$

be an ordered orthonormal basis for V, such that $T\alpha_j = c_j \alpha_j$, $j = 1, \ldots, n$. If $D = [T]_{B'}$ then D is the diagonal matrix with diagonal entries $c_1, \ldots, c_n$. Let P be the matrix with column vectors $\alpha_1, \ldots, \alpha_n$. Then $D = P^{-1}AP$.

In case each entry of A is real, we can take V to be R^n, with the standard inner product, and repeat the argument. In this case, P will be a unitary matrix with real entries, *i.e.*, a real orthogonal matrix.

Combining Theorem 9 with our comments at the beginning of this section, we have the following: If V is a finite-dimensional real inner product space and T is a linear operator on V, then V has an orthonormal basis of characteristic vectors for T if and only it T is self-adjoint. Equivalently, if A is an $n \times n$ matrix with real entries, there is a real orthogonal matrix P such that P^tAP is diagonal if and only if $A = A^t$. There is no such result for complex symmetric matrices. In other words, for complex matrices there is a significant difference between the conditions $A = A^t$ and $A = A^*$.

Having disposed of the self-adjoint case, we now return to the study of normal operators in general. We shall prove the analogue of Theorem 9 for normal operators, in the complex case. There is a reason for this restriction. A normal operator on a real inner product space may not have any non-zero characteristic vectors. This is true, for example, of all but two rotations in R^2.

Theorem 10: Let V be a finite-dimensional inner product space and T a normal operator on V. Suppose α is a vector in V. Then α is a characteristic vector for T with characteristic value c if and only if α is a characteristic vector for T^* with characteristic value $\bar{c}$.

Proof: Suppose U is any normal operator on V. Then $\| U\alpha \| = \| U^*\alpha \|$. For using the condition $UU^* = U^*U$ one sees that

$$\begin{aligned} \| U\alpha \|^2 &= (U\alpha \mid U\alpha) = (\alpha \mid U^*U\alpha) \\ &= (\alpha \mid UU^*\alpha) = (U^*\alpha \mid U^*\alpha) = \| U^*\alpha \|^2. \end{aligned}$$

If c is any scalar, the operator $U = T - cI$ is normal. For $(T - cI)^* = T^* - \bar{c}\, I$, and it is easy to check that $UU^* = U^*U$. Thus

$$\| (T - cI)\alpha \| = \| (T^* - cI)\alpha \|$$

so that $\quad (T - cI)\alpha = 0$ if and only if $(T^* - \bar{c}\, I)\alpha = 0$.

Definition: A complex n x n matrix A is called normal if $AA^* = A^*A$.

It is not so easy to understand what normality of matrices or operators really means; however, in trying to develop some feeling for the concept, the reader might find it helpful to know that a triangular matrix is normal if and only if it is diagonal.

Theorem 11: Let V be a finite-dimensional inner product space, T a linear operator on V, and β on orthonormal basis for V. Suppose that the matrix A of T in the basis β is upper triangular. Then T is normal if and only if A is a diagonal matrix.

Proof: Since β is an orthonormal basis, A^* is the matrix of T^* in β. If A is diagonal, then $AA^* = A^*A$, and this implies $TT^* = T^*T$. Conversely, suppose T is normal, and let $\beta = \{\alpha_1, \ldots, \alpha_n\}$. Then, since A is upper-triangular, $T\alpha_1 = A_{11}\alpha_1$. By Theorem 10 this implies, $T^*\alpha_1 = \bar{A}_{11}\alpha_1$. On the other hand,

$$\begin{aligned} T^*\alpha_1 &= \sum_j (A^*)_{j1} \alpha_j \\ &= \sum_j \bar{A}_{1j} \alpha_j \end{aligned}$$

Therefore, $A_{1j} = 0$ for every $j > 1$. In particular, $A_{12} = 0$, and since A is upper-triangular, it follows that

$$T\alpha_2 = A_{22}\alpha_2.$$

Thus $T^*\alpha_2 = \bar{A}_{22}\alpha_2$ and $A_{2j} = 0$ for all $j \neq 2$. Continuing in this fashion, we find that A is diagonal.

Theorem 12: Let V be a finite-dimensional complex inner product space and let T be any linear operator on V. Then there is an orthonormal basis for V in which the matrix of T is upper triangular.

Proof: Let n be the dimension of V. The theorem is true when $n = 1$, and we proceed by induction on n, assuming the result is true for linear operators on complex inner product spaces of dimension $n - 1$. Since V is a finite-dimensional complex inner product space, there is a unit vector α in V and a scalar c such that

$$T^*\alpha = c\alpha.$$

Let W be the orthogonal complement of the subspace spanned by α and let S be the restriction of T to W. By Theorem 10, W is invariant under T. Thus S is a linear operator on W. Since W has dimension $n - 1$, our inductive assumption implies the existence of an orthonormal basis $\{\alpha_1, \ldots, \alpha_{n-1}\}$ for W in which the matrix of S is upper-triangular; let $\alpha_n = \alpha$. Then $\{\alpha_1, \ldots, \alpha_n\}$ is an orthonormal basis of V in which the matrix of T is upper-triangular.

This theorem implies the following result for matrices.

Corollary: For every complex $n \times n$ matrix A there is unitary matrix U such that $U^{-1}AU$ is upper-triangular.

Now combining Theorem 12 and Theorem 11, we immediately obtain the following analogue of Theorem 9 for normal operators.

Theorem 13: Let V be a finite-dimensional complex inner product space and T a normal operator on V. Then V has an orthonormal basis consisting of characteristic vectors for T.

Also for every normal matrix A, there is a unitary matrix P such that $P^{-1}AP$ is a diagonal matrix.

Self Assessment

3. For each of the following real symmetric matrices A, find a real orthogonal matrix P such that $P^{-1}AP$ is diagonal

   (i) $A = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$

   (ii) $A = \begin{bmatrix} 4/3 & \sqrt{2}/3 \\ \sqrt{2}/3 & 5/3 \end{bmatrix}$

   (iii) $A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

4. Prove that T is normal if $T = T_1 + i\,T_2$, where T_1 and T_2 are self-adjoint operators which commute.

6.3 Summary

- In this unit we have studied unitary operators and normal operators.

- With the help of a few theorems and examples the properties of unitary operators are explained.
- The distinction between unitary operators, orthogonal operators and normal operators is established.
- With the help of a few theorem it is shown that for every normal matrix A, there is a unitary matrix P such that $P^{-1}AP$ is a diagonal matrix.

6.4 Keywords

General Linear Group: A general linear group denotes the set of all invertible complex $n \times n$ matrices and is denoted by $GL(n)$.

Isomorphism: An isomorphism of inner product spaces V onto W is a vector space isomorphism of the linear operator T of V onto W which also preserves inner products.

Orthogonal: A real or complex $n \times n$ matrix A is said to be orthogonal if $A^tA = I$.

Unitary: A complex $n \times n$ matrix A is called unitary if $A^*A = 1$.

Unitary Operator: A unitary operator on an inner product space is isomorphism of the space onto itself.

6.5 Review Questions

1. For $A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{bmatrix}$

   there is a real orthogonal matrix P such that $P^{-1}AP = D$ is diagonal. Find such a diagonal matrix D.

2. If T is a normal operator. Prove that characteristic vectors for T which are associated with distinct characteristic values are orthogonal.

6.6 Further Readings

Books

Michael Artin *Algebra*

I N. Herstein *Topics in Algebra*

Kenneth Hoffman and Ray Kunze *Linear Algebra*

Richa Nandra, Lovely Professional University

Notes

Unit 7: Introduction and Forms on Inner Product Spaces

CONTENTS

Objectives

Introduction

7.1 Overview

7.2 Forms on Inner Product Spaces

7.3 Summary

7.4 Keywords

7 .5 Review Questions

7 .6 Further Readings

Objectives

After studying this unit, you will be able to:

- See that the material covered in this unit on inner product spaces is more sophisticated and generally more involved technically
- Understand more clearly sesquilinear form as well as bilinear forms
- See that the map $f \rightarrow T$ isomorphism of the space of forms onto $L(V, V)$ is understood well
- Know how to obtain the matrix of f in the ordered basis β.

Introduction

In this unit the topics covered in the units 24, 25 and unit 26 are reviewed.

It is seen that these ideas can further be elaborated on an advanced stage.

It is shown that the section devotes to the relation between forms and linear operators.

One can see that for every Hermitian form f on a finite dimensional inner product space V, there is an orthonormal basis of V in which f is represented by a diagonal matrix with real entries.

7.1 Overview

In the units 24, 25, 26 we have covered topics which are quite fundamental in nature. It covered basically a lot of topics like inner products, inner product spaces, adjoint operators, unitary operators and linear functionals. However, in the next few units we shall deal with inner product spaces and spectral theory, forms on inner product spaces, positive forms and properties of the normal operators. Apart from the formulation of the principal axis theorem or the orthogonal diagonalization of self-adjoint operators the material covered in these units is sophisticated and generally more technically involved. In these units the arguments and proofs are written in a more condensed forms. Units 27 and 28 are devoted to results concerning forms on inner product spaces and the relations between forms and linear operators. Unit 2 deals with spectral theory, i.e. with the implication of the ideas of units 24, 25 and 26 concerning the diagonalization of self-adjoint and normal operators.

7.2 Forms on Inner Product Spaces

Notes

If T is a linear operator on a finite-dimensional inner product space V the function f defined on $V \times V$ by

$$f(\alpha, \beta) = (T\alpha \mid \beta)$$

may be regarded as a kind of substitute of T. Many questions about T are equivalent to questions concerning f. In fact, it is easy to see that f determines T. For if $\beta = \{\alpha_1, ..., \alpha_n\}$ is an orthonormal basis for V, then the entries of the matrix of T in β are given by

$$A_{jk} = f(\alpha_k, \alpha_j)$$

It is important to understand why f determines T from a more abstract point of view. The crucial properties of f are described in the following definition.

Definition: A (sesquilinear) form on a real or complex vector space V is a function f on $V \times V$ with values in the field of scalars such that

(a) $f(c\alpha + \beta, \gamma) = cf(\alpha, \gamma) + f(\beta, \gamma)$

(b) $f(\alpha + c\beta, \gamma) = \bar{c}\, f(\alpha, \beta) + f(\alpha, \gamma)$

for all α, β, γ in V and all scalars c.

Thus, a sesquilinear form is a function on $V \times V$ such that $f(\alpha, \beta)$ is a linear function of α for fixed β and a conjugate-linear function of β for fixed α. In the real case, $f(\alpha, \beta)$ is linear as a function of each argument; in other words, f is a bilinear form. In the complex case, the sesquilinear form f is not bilinear unless $f = 0$. In the remainder of this chapter, we shall omit the adjective 'sesquilinear' unless it seems important to include it.

If f and g are forms on V and c is a scalar, it is easy to check that $cf + g$ is also a form. From this it follows that any linear combination of forms on V is again a form. Thus the set of all forms on V is a subspace of the vector space of all scalar-valued functions on $V \times V$.

Theorem 1: Let V be a finite-dimensional inner product space and f a form on V. Then there is a unique linear operator T on V such that

$$f(\alpha, \beta) = (T\alpha \mid \beta)$$

for all α, β, in V and the map $f \to T$ is an isomorphism of the space of forms onto $L(V, V)$.

Proof: Fix a vector β in V. Then $a \to f(\alpha, \beta)$ is a linear function on V. By theorem 6 in unit 26 there is a unique vector β' in V such that $f(\alpha, \beta) = (\alpha \mid \beta')$ for every α. We define a function U from V into V by setting $U\beta = \beta'$. Then

$$\begin{aligned} f(\alpha \mid c\beta + \gamma) &= (\alpha \mid U(c\beta + \gamma)) \\ &= \bar{c}f(\alpha, \beta) + f(\alpha, \gamma) \\ &= \bar{c}(\alpha \mid U\beta) + (\alpha \mid U\gamma) \\ &= (\alpha \mid c\,U\beta + U\gamma) \end{aligned}$$

for all α, β, γ in V and all scalars c. Thus U is a linear operator on V and $T = U^*$ is an operator such that $f(\alpha, \beta) = (T\alpha \mid \beta)$ for all α and β. If we also have $f(\alpha, \beta) = (T'\alpha \mid \beta)$, then

$$(T\alpha - T'\alpha \mid \beta) = 0$$

for all α and β; so $T\alpha = T'\alpha$ for all α. Thus for each form f there is a unique linear operator T_f such that

$$f(\alpha, \beta) = (T_j\alpha \mid \beta)$$

Notes

for all α, β in V. If f and g are forms and c a scalar, then

$$\begin{aligned}(cf + g)(\alpha, \beta) &= (T_{cf+g}\alpha \mid \beta) \\ &= cf(\alpha, \beta) + g(\alpha, \beta) \\ &= c(T_f\alpha \mid \beta) + (T_g\alpha \mid \beta) \\ &= (cT_f + T_g \mid \alpha \mid \beta)\end{aligned}$$

for all α and β in V. Therefore,

$$T_{cf+g} = cT_1 + T_g$$

so $f \to T_f$ is a linear map. For each T in $L(V, V)$ the equation

$$f(\alpha, \beta) = (T\alpha \mid \beta)$$

defines a form such that $T_f = T$, and $T_f = 0$ if and only if $f = 0$. Thus $f \to T_f$ is an isomorphism.

Corollary: The equation

$$(f \mid g) = tr(T_f T^*_g)$$

defines an inner product on the space of forms with the property that

$$(f \mid g) = \sum_{j,k} f(\alpha_k, \alpha_j)\overline{g(\alpha_k, \alpha_j)}$$

for every orthonormal basis $\{\alpha_1, ..., \alpha_n\}$ of V.

Proof: It follows easily from Example 3 of unit 24 that $(T, U) \to \text{tr}\,(TU^*)$ is an inner product on $L(V, V)$. Since $f \to T_f$ is an isomorphism, Example 6 of unit 24 shows that

$$(f \mid g) = \text{tr}\,(T_f T^*_g)$$

is an inner product. Now suppose that A and B are the matrices of T_f and T_g in the orthonormal basis $\beta = \{\alpha_1, ..., \alpha_n\}$. Then

$$A_{jk} = (T_f\alpha_k \mid \alpha_j) = f(\alpha_k, \alpha_j)$$

and $B_{jk} = (T_g\alpha_k \mid \alpha_j) = g(\alpha_k, \alpha_j)$. Since AB^* is the matrix of $T_f T^*_g$ in the basis β, it follows that

$$(f \mid g) = \text{tr}\,(AB^*) = \sum_{j,k} A_{jk} B_{jk}$$

Definition: If f is a form and $\beta = \{\alpha_1, ..., \alpha_n\}$ an arbitrary ordered basis of V, the matrix A with entries

$$A_{jk} = f(\alpha_k, \alpha_j)$$

is called the matrix of f in the ordered basis β.

When β is an orthonormal basis, the matrix of f in β is also the matrix of the linear transformation T_f, but in general this is not the case.

If A is the matrix of f in the ordered basis $\beta = (\alpha_1, ... \alpha_n)$, if follows that

$$f\left(\sum_s x_s\alpha_s \sum_r y_r\alpha_r\right) = \sum_{r,s} \overline{y}_r A_{rs} x_s \quad ...(1)$$

for all scalars x, and y ($1 \leq r, s \leq n$). In other words, the matrix A has the property that

$$f(\alpha, \beta) = Y^*AX$$

where X and Y are the respective coordinate matrices of α and β in the ordered basis β.

The matrix of f in another basis

$$\alpha'_j = \sum_{i=1}^{n} P_{ij}\alpha_i\ , \qquad (1 \le j \le n)$$

is given by the equation

$$A' = P^*AP. \tag{2}$$

For

$$A'_{jk} = f(\alpha'_k, \alpha'_j)$$

$$= f\left(\sum_s P_{sk}\alpha_s, \sum_r P_{rj}\alpha_r\right)$$

$$= \sum_{r,s} \overline{P_{rj}} A_{rs} P_{sk}$$

$$= (P^*AP)_{jk}.$$

Since $P^* = P^{-1}$ for unitary matrices, it follows from (2) that results concerning unitary equivalence may be applied to the study of forms.

Theorem 2: Let f be a form on a finite-dimensional complex inner product space V. Then there is an orthonormal basis for V in which the matrix of f is upper-triangular.

Proof: Let T be the linear operator on V such that $f(\alpha, \beta) = (T\alpha \mid \beta)$ for all α and β. By Theorem 12 of unit 26 there is an orthonormal basis $(\alpha_1, ..., \alpha_n)$ in which the matrix of T is upper-triangular. Hence.

$$f(\alpha_k, \alpha_j) = (T\alpha_k \mid \alpha_j) = 0$$

when $j > k$.

Definition: A form f on a real or complex vector space V is called **Hermitian** if

$$f(\alpha, \beta) = \overline{f(\beta, \alpha)}$$

for all α and β in V.

If T is a linear operator on a finite-dimensional inner product space V and f is the form

$$f(\alpha, \beta) = (T\alpha \mid \beta)$$

then $\overline{f(\beta, \alpha)} = (\alpha \mid T\beta) = (T^*\alpha \mid b)$; so f is Hermitian if and only if T is self-adjoint.

When f is Hermitian $f(\alpha, \alpha)$ is real for every α, and on complex spaces this property characterizes Hermitian forms.

Theorem 3: Let V be a complex vector space and f a form on V such that $f(\alpha, \alpha)$ is real for every α. Then f is Hermitian.

Proof: Let α and β be vectors in V. We must show that $f(\alpha, \beta) = \overline{f(\beta, \alpha)}$. Now

$$f(\alpha + \beta, \alpha + \beta) = f(\alpha, \beta) + f(\alpha, \beta) + f(\beta, \alpha) + f(\beta, \beta).$$

Since $f(\alpha + \beta, \alpha + \beta) = f(\alpha, \alpha)$, and $f(\beta, \beta)$ are real, the number $f(\alpha, \beta) + f(\beta, \alpha)$ is real. Looking at the same argument with $\alpha + i\beta$ instead of $\alpha + \beta$, we see that – if (α, β) + if (β, α) is real. Having concluded that two numbers are real, we set them equal to their complex conjugates and obtain

$$f(\alpha, \beta) + f(\beta, \alpha) = \overline{f(\alpha, \beta)} + \overline{f(\beta, \alpha)}$$

$$-if(\alpha, \beta) + if(\beta, \alpha) = \overline{if(\alpha, \beta)} - \overline{if(\beta, \alpha)}$$

Notes

If we multiply the second equation by i and add the result to the first equation, we obtain

$$2f(\alpha, \beta) = 2f(\beta, \alpha).$$

Corollary: Let T be a linear operator on a complex finite-dimensional inner product space V. Then T is self-adjoint if and only if $(T\alpha\,|\,\alpha)$ is real for every α in V.

Theorem 4 (Principal Axis Theorem): For every Hermitian form f on a finite-dimensional inner product space V, there is an orthonormal basis of V in which f is represented by a diagonal matrix with real entries.

Proof: Let T be the linear operator such that $f(\alpha, \beta) = (T\alpha\,|\,\beta)$ for all α and β in V. Then, since $f(\alpha, \beta) = \overline{f(\beta, \alpha)}$ and $\overline{(T\beta\,|\,\alpha)} = (\alpha\,|\,T\beta)$, it follows that

$$(T\alpha\,|\,\beta) = \overline{f(\beta, \alpha)} = (\alpha\,|\,T\beta)$$

for all α and β; hence $T = T^*$. By Theorem 5 of unit 24, there is an orthonormal basis of V which consists of characteristic vectors for T. Suppose $\{\alpha_1, ..., \alpha_n\}$ is an orthonormal basis and that

$$T\alpha_j = c_j\alpha_j$$

for $1 \le j \le n$. Then

$$f(\alpha_k, \alpha_j) = (T\alpha_k\,|\,\alpha_j) = \delta_{kj}c_k$$

and by Theorem 2 of unit 24 each c_k is real.

Corollary: Under the above conditions

$$f\Big(\sum_j x_j\alpha_j, \sum_k y_k\alpha_k\Big) = \sum_j c_j x_j \overline{y}_j$$

Self Assessment

1. Which of the following functions f, defined on vectors $\alpha = (x_1, x_2)$ and β (y_1, y_2) = in c^2, are sesquilinear forms on c^2

   (a) $f(\alpha, \beta) = (x_1 - \overline{y}_1)^2 + x_2\overline{y}_2$

   (b) $f(\alpha, \beta) = x\,\overline{y}_2 - \overline{x}_2 y_1$

   (c) $f(\alpha, \beta) = x_1\overline{y}_1$

2. Let f be a non-degenerate form on a finite-dimensional space V. Show that each linear operator S has an 'adjoint' relative to f', i.e., an operator S' such that $f(S\alpha, \beta) = f(\alpha, S'\beta)$ for all α, β.

7.3 Summary

- In the introduction a review of the last units 24, 25, 26 is done. It is stated that the ideas covered in these units are fundamental.
- In this unit forms on inner product space are studied and the relation between the forms and the linear operator is established.
- A sesquilinear form is introduced and explained for all α, β, γ in the finite vector space V and its relation with the linear operators.
- When the basis β is an orthonormal basis, the matrix of the form f in β is also matrix of the linear transformation T_{fi}.

Notes

7.4 Keywords

A Sesquilinear Form: A sesquilinear form on a real or complex vector space V is a function f on $V \times V$ with values in the field of scalars such that

$$f(c\alpha + \beta, \gamma) = cf(\alpha, \gamma) + f(\beta, \gamma)$$

$$f(\alpha + c\beta, \gamma) = cf(\alpha, \beta) + f(\alpha, \gamma)$$

for all α, β, γ in V and all scalars c.

Hermitian: A form f on a real or complex vector space V is called Hermitian if

$$f(\alpha, \beta) = \overline{f(\beta, \alpha)}$$

for all α and β in V.

***Self-adjoint*:** The linear operator T is self-adjoint on a complex finite-dimensional inner product space V, if and only if $(T\alpha|\alpha)$ is real for every α in V.

7.5 Review Questions

1. Let

   $$A = \begin{bmatrix} 1 & i \\ -i & 2 \end{bmatrix}$$

   and let g be the form (on the space of 2 × 1 complex matrices) defined by $g(X, Y) = Y^*AX$. Is g an inner product?

2. Let f be the form on R^2 defined by

   $$f[(x_1, y_1), (y_2, y_2)] = x_1y_1 + x_2y_2$$

   Find the matrix of f in each of the following bases:

   {(1, –1), (1, 1)}, {(1, 2), (3, 4)}

Answer: Self Assessment

1. (b), (c)

7.6 Further Readings

Books Kenneth Hoffman and Ray Kunze, *Linear Algebra*

Michael Artin, *Algebra*

Unit 8: Positive Forms and More on Forms

CONTENTS

Objectives

Introduction

8.1 Positive Forms

8.2 More on Forms

8.3 Summary

8.4 Keywords

8.5 Review Questions

8.6 Further Readings

Objectives

After studying this unit, you will be able to:

- Understand when a form f on a real or complex vector space v is non-negative. If the form f is Hermitian and $f(\alpha, \alpha) > 0$ for every α in v, the form f is positive.
- Know that f is a positive form if and only if $A = A^*$ and the principal minors of the matrix A of f are all positive.
- See that if A is the matrix of the form f in the ordered basis $\{\alpha_1, ..., \alpha_n\}$ of v and the principal minors of A are all different from 0, then there is a unique upper triangular matrix P with $P_{kk} = 1(1 \le k \le n)$ such that P^*AP is upper triangular.

Introduction

In this unit the form f on a real or complex vector space is studied and seen under what conditions the form f is positive.

On the basis of the principal minors of A being all different from 0, the positive form f, it is seen that there is an upper-triangular matrix P with $P_{kk} = 1$ $(1 \le k \le n)$ such that $B = AP$ is lower triangular.

8.1 Positive Forms

In this unit we study non-negative (sesqui) forms and their relation to a given inner product on the given finite vector space.

A form f on a real or complex vector space v is non-negative if it is Hermitian and $f(\alpha, \alpha) \ge 0$ for every α in v. The form f is positive if it is Hermitian and $f(\alpha, \alpha) > 0$ for all $\alpha \ne 0$.

A positive form on v is simply an inner production v. Let f be a form on the finite dimensional space. Let $\beta = (\alpha_1, \alpha_2, ...\alpha_n)$ be an ordered basis of v, and let A be the matrix of f on the basis β, i.e., $A_{jk} = f(\alpha_k, \alpha_j)$. If $\alpha = x_1\alpha_1 + ... + x_n\alpha_n$, then

$$f(\alpha, \alpha) = f(\sum_j x_j\alpha_j, \sum_k x_k\alpha_k)$$

Notes

$$= (\sum_j \sum_k x_j \bar{x}_k f(\alpha_j, \alpha_k)$$

$$= (\sum_j \sum_k A_{kj} x_j \bar{x}_k) \qquad ...(1)$$

So we see that f is non-negative if and only if

and

$$A = A^*$$

$$\sum_j \sum_k A_{kj} x_j \bar{x}_k \geq 0 \text{ for all scalars } x_1, x_2, \ldots x_n \qquad ..(2)$$

For positive f, the relation should be true for all $(x_1, x_2, \ldots x_n) \neq 0$. The above conditions on positive f form are true if

$$g(X, Y) = Y^*AX \qquad ...(3)$$

is a positive form on the space of $n \times 1$ column matrices over the scalar field.

Theorem 1: Let F be the field of real number or the field of complex numbers. Let A be an $n \times n$ matrix over F. The function g defined by

$$g(X, Y) = Y^*AX \qquad ...(4)$$

is a positive form on the space $F^{n\times 1}$ if and only if there exists an invertible $n \times n$ matrix P with entries in F such that $A = P^*P$.

Proof: For any $n \times n$ matrix A, the function g in (4) is a form on the space of column matrices. We are trying to prove that g is positive if and only if $A = P^*P$. First, suppose A = P*P. Then g is Hermitian and

$$\begin{aligned} g(X, X) &= X^*P^*PX \\ &= (PX)^*PX \\ &\geq 0. \end{aligned}$$

If P is invertible and $X \neq 0$, then $(PX)^*PX > 0$.

Now, suppose that g is a positive form on the space of column matrices. Then it is an inner product and hence there exist column matrices $Q_1, \ldots, Q_n$ such that

$$\begin{aligned} \delta_{jk} &= g(Q_1, Q_k) \\ &= Q^*_k A Q_j. \end{aligned}$$

But this just says that, if Q is the matrix with columns $Q_1, \ldots, Q_n$, then $A^*AQ = I$. Since $\{Q_1, \ldots, Q_n\}$ is a basis, Q is invertible. Let $P = Q^{-1}$ and we have $A = P^*P$.

In practice, it is not easy to verify that a given matrix A satisfies the criteria for positivity which we have given thus far. One consequence of the last theorem is that if g is positive then det $A > 0$, because det A = det (P^*P) = det P^* det P = $|\det P|^2$. The fact that det $A > 0$ is by no means sufficient to guarantee that g is positive; however, there are n determinants associated with A which have this property: If $A = A^*$ and if each of those determinants is positive, then g is a positive form.

Definition: Let A be an $n \times n$ matrix over field F. The principal minors of A are the scalars $\Delta_k(A)$ defined by

$$\Delta_k(A) = \det\begin{bmatrix} A_n & \cdots & A_{1k} \\ \vdots & & \vdots \\ A_{k1} & \cdots & A_{kk} \end{bmatrix}, 1 \le k \le n.$$

Lemma: Let A be an invertible $n \times n$ matrix with entries in a field F. The following two statements are equivalent:

(a) There is an upper triangular matrix P with $P_{kk} = 1$ $(1 \le k \le n)$ such that the matrix $B = AP$ is lower-triangular.

(b) The principal minors of A are all different from 0.

Proof: Let P be any $n \times n$ matrix and set $B = AP$. Then

$$B_{jk} = \sum_r A_{jr}, P_{rk}$$

If P is upper-triangular and $P_{kk} = 1$ for every k, then

$$\sum_{r=1}^{k-1} A_{jr} P_{rk} = B_{jk} - A_{kk}, \qquad k > 1$$

Now B is lower-triangular provided $B_{jk} = 0$ for $j < k$. Thus B will be lower-triangular if and only if

$$\sum_{r=1}^{k-1} A_{jr} P_{rk} = -A_{kk}, \qquad 1 \le j \le k-1$$

$$2 \le k \le n. \qquad \text{...(5)}$$

So, we see that statement (a) in the lemma is equivalent to the statement that there exist scalars P_{rk}, $1 \le r \le k$, $1 \le k \le n$, which satisfy (5) and $P_{kk} = 1$, $1 \le k \le n$.

In (5) for each $k > 1$ we have a system of $k - 1$ linear equations for the unknowns $P_{1k}, P_{2k}, \ldots, P_{k-1,k}$. The coefficient matrix of that system is

$$\begin{bmatrix} A_n & \cdots & A_{1,k-1} \\ \vdots & & \vdots \\ A_{k-1} & \cdots & A_{k-1,k-1} \end{bmatrix}$$

and its determinant is the principal minor $\Delta_{k-1}(A)$. If each $\Delta_{k-1}(A) \ne 0$, the systems (5) have unique solutions. We have shown that statement (b) implies statement (a) and that the matrix P is unique.

Now suppose that (a) holds. Then, as we shall see,

$$\begin{aligned} \Delta_k(A) &= \Delta_k(B) \\ &= B_{11} B_{22} \ldots B_{kk}, \ k = 1, \ldots, n. \end{aligned} \qquad \text{...(6)}$$

To verify (6), let $A_1, \ldots, A_n$ and $B_1, \ldots B_n$ be the columns of A and B, respectively. Then

$$B_1 = A_1$$

$$B_r = \sum_{j=1}^{r-1} P_{jr} A_j + A_r, \quad r > 1. \qquad \text{...(7)}$$

Fix k, $1 \le k \le n$. From (7) we see that the rth column of the matrix

$$\begin{bmatrix} B_{11} & \cdots & B_{kk} \\ \vdots & & \vdots \\ B_{k1} & \cdots & B_{kk} \end{bmatrix}$$

Notes

is obtained by adding to the rth column of

$$\begin{bmatrix} A_{11} & \cdots & A_{1k} \\ \vdots & & \vdots \\ A_{k1} & \cdots & A_{kk} \end{bmatrix}$$

a linear combination of its other columns. Such operations do not change determinants. That proves (6), except for the trivial observation that because B is triangular $\Delta_k(B) = B_{11} \ldots B_{kk}$. Since A and P are invertible, B is invertible. Therefore

$$\Delta(B) = B_{11} \ldots B_{nn} \neq 0$$

and so $\Delta_k(A) \neq 0$, $k = 1, \ldots, n$.

Theorem 2: Let f be a form on a finite dimensional vector space V and let A be the matrix of f in an ordered basis B. Then f is a positive form if and only if $A = A^*$ and the principal minors of A are all positive.

Proof: Suppose that $A = A^*$ and $\Delta_k(A) > 0$, $1 \leq k \leq n$. By the lemma, there exists an (unique) upper-triangular matrix P with $P_{kk} = 1$ such that $B = AP$ is lower triangular. The matrix P^* is lower-triangular, so that $P^*B = P^*AP$ is also lower triangular. Since A is self-adjoint, the matrix $D = P^*AP$ is self-adjoint. A self-adjoint triangular matrix is necessarily a diagonal matrix. By the same reasoning which led to (6),

$$\begin{aligned} \Delta_k(D) &= \Delta_k(P^*B) \\ &= \Delta_k(B) \\ &= \Delta_k(A). \end{aligned}$$

Since D is diagonal, its principal minors are

$$\Delta_k(D) = D_{11} \ldots D_{kk}.$$

From $\Delta_k(D) > 0$, $1 \leq k \leq n$, we obtain $D_{kk} > 0$ for each k.

If A is the matrix of the form f in the ordered basis $B = \{\alpha_1, \ldots, \alpha_n\}$, then $D = P^*AP$ is the matrix of f in the basis $\{\alpha'_1, \ldots, \alpha'_n\}$ defined by

$$\alpha' j = \sum_{i=1}^{n} P_{ij}\alpha_i$$

Since D is diagonal with positive entries on its diagonal, it is obvious that

$$X^*DX > 0. \quad X \neq 0$$

from which it follows that f is a positive form.

Now, suppose we start with a positive form f. We know that $A = A^*$. How do we show that $\Delta_k(A) > 0$, $1 \leq k \leq n$? Let V_k be the subspace spanned by $\alpha_1, \ldots, \alpha_k$ and let f_k be the restriction of f to $V_k \times V_k$. Evidently f_k is a positive form on V_k and, in the basis $\{\alpha_1, \ldots, \alpha_k\}$ it is represented by the matrix.

$$\begin{bmatrix} A_{11} & \cdots & A_{1k} \\ \vdots & & \vdots \\ A_{k1} & \cdots & A_{kk} \end{bmatrix}$$

As a consequence of Theorem 1, we noted that the positivity of a form implies that the determinant of any representing matrix is positive.

There are some comments we should make, in order to complete our discussion of the relation between positive forms and matrices. What is it that characterizes the matrices which represent positive forms? If f is a form on a complex vector space and A is the matrix of f in some ordered basis, then f will be positive if and only if $A = A^*$ and

$$X^*AX > 0 \qquad \text{for all complex } X \neq 0 \qquad \text{....(8)}$$

It follows from Theorem 3 of unit 27 that the condition $A = A^*$ is redundant, i.e., that (8) implies $A = A^*$. One the other hand, if we are dealing with a real vector space the form f will be positive if and only if $A = A^t$ and

$$X^*AX > 0 \qquad \text{for all real } X \neq 0 \qquad \text{....(9)}$$

We want to emphasize that if a real matrix A satisfies (9), it does not follow that $A = A^t$. One thing which is true is that, if $A = A^t$ and (9) holds, then (8) holds as well. That is because

$$\begin{aligned}(X + iY)^*A(X + iY) &= (X^t - iY^t)A(X + iY)\\ &= X^tAX + Y^tAY + i[X^tAY - Y^tAX]\end{aligned}$$

and if $A = A^t$ then $Y^tAX = X^tAY$.

If A is an $n \times n$ matrix with complex entries and if A satisfies (9), we shall call A a positive matrix.

Now suppose that V is a finite-dimensional inner product space. Let f be a non-negative form on V. There is a unique self-adjoint linear operator T on V such that

$$f(\alpha, \beta) = (T\alpha \mid \beta) \qquad \text{...(10)}$$

and T has the additional property that $(T\alpha \mid \alpha) \geq 0$

Definition: A linear operator T on a finite-dimensional inner product space V is non-negative if $T = T^*$ and $(T\alpha \mid \alpha) \geq 0$ for all α in V. A positive linear operator is one such that $T = T^*$ and $(T\alpha \mid \alpha) > 0$ for all $\alpha \neq 0$.

If V is a finite-dimensional (real or complex) vector space and if $(.\mid.)$ is an inner product on V, there is an associated class of positive linear operators on V. Via (10) there is a one-one correspondence between that class of positive operators and the collection of all positive forms on V. Let us summarise as:

If A is an $n \times n$ matrix over the field of complex numbers, the following are equivalent:

1. A is positive, i.e. $\sum_j \sum_k A_{kj} x_j \bar{x}_k < 0$ whenever $x_1, ..., x_n$ are complex numbers, not all 0.
2. $(X \mid Y) = Y^*AX$ is an inner product on the space of $n \times 1$ complex matrices.
3. Relative to the standard inner product $(X \mid Y) = Y^*X$ on $n \times 1$ matrices, the linear operator $X \to AX$ is positive.
4. $A = P^*P$ for some invertible $n \times n$ matrix P over C.
5. $A = A^*$, and the principal minors of A are positive.

If each entry of A is real, these are equivalent to:

1. $A = A^t$, and $\sum_j \sum_k A_{kj} x_j x_k < 0$ whenever $x_1, ..., x_n$ are real numbers, not all 0.
2. $(X \mid Y) = Y^tAX$ is an inner product on the space of $n \times 1$ real matrices.
3. Relative to the standard inner product $(X \mid Y) = Y^tX$ on $n \times 1$ real matrices, the linear operator $X \to AX$ is positive.
4. There is an invertible $n \times n$ matrix P, with real entries, such that $A = P^tP$.

8.2 More on Forms

Notes

Theorem 3: Let f be a form on a real or complex vector space V and $\{\alpha_1, ..., \alpha_r\}$ a basis for the finite dimensional subspace W of V. Let M be the $r \times r$ matrix with entries

$$M_{jk} = f(\alpha_k, \alpha_j)$$

and W' the set of all vectors β in V such that $f(\alpha, \beta)$ for all α in W. Then W' is subspace of V, and $W \cap W' = \{0\}$ if and only if M is invertible. When this is the case, $V = W + W'$.

Proof: If β and γ are vectors in W' and c is a scalar, then for every α in W

$$\begin{aligned} f(\alpha, c\beta + \gamma) &= \bar{c}\, f(\alpha, \beta) + f(\alpha, \gamma) \\ &= 0. \end{aligned}$$

Hence, W′ is a subspace of V.

Now suppose $\alpha = \sum_{k=1}^{r} x_x \alpha_k$ and that $\beta = \sum_{j=1}^{r} y_j \alpha_j$. Then

$$\begin{aligned} f(\alpha, \beta) &= \sum_{j,k}^{r} \bar{y}, M_{jk} x_k \\ &= \sum_k \left(\sum_j \bar{y}_j M_{jk} \right) x_k. \end{aligned}$$

It follows from this that $W \cap W' \neq \{0\}$ if and only if the homogeneous system

$$\sum_{j=1}^{r} \bar{y}_j M_{jk} = 0, 1 \le k \le r$$

has a non-trivial solution $(y_1 ..., y_r)$. Hence $W \cap W'$ $\{0\}$ if and only if M^* is invertible. But the invertibility of M^* is equivalent to the invertibility of M.

Suppose that M is invertible and let

$$\begin{aligned} A &= (M^*)^{-1} = (M^{-1})^* \\ g_j(\beta) &= \sum_{k=1}^{r} A_{jk} \overline{f(\alpha_k, \beta)} \end{aligned}$$

Then

$$\begin{aligned} g_j(c\beta + \gamma) &= \sum_k \delta_{kn} \overline{f(\alpha_k, c\beta + \gamma)} \\ &= c \sum_k A_{jk} f(\alpha_k, \beta) + \sum_k A_{jk} f(\alpha_k, \gamma) \\ &= c g_j(\beta) + g_j(\gamma) \end{aligned}$$

Hence, each g_j is a linear function on V. Thus we may define a linear operator E on V by setting

$$E\beta = \sum_{j=1}^{r} g_j(\beta) \alpha_j$$

Since

$$g_j(\alpha_n) = \sum_k A_{jk}\overline{f(\alpha_k, \alpha_n)}$$

$$= \sum_k A_{jk}(M^*)_{kn}$$

$$= \delta_{jn}$$

it follows that $E(\alpha_n) = \alpha_n$ for $1 \le n \le r$. This implies $E\alpha = \alpha$ for every α in W. Therefore, E maps V onto W and $E^2 = E$. If β is an arbitrary vector in V, then

$$f(\alpha_n, E\beta) = f\left(\alpha_n \sum_j g_j(\beta)\alpha_j\right)$$

$$= \sum_j \overline{g_j(\beta)} f(\alpha_n, a_j)$$

$$= \sum_j \left(\sum_k \overline{A}_{jk} f(\alpha_k, \beta)\right) f(\alpha_n, \alpha_j)$$

Since $A^* = M^{-1}$, it follows that

$$f(\alpha_n, E\beta) = \sum_k \left(\sum_j (M^{-1})_{kj} M_{jn}\right) f(\alpha_k, \beta)$$

$$= \sum_k \delta_{kn} f(\alpha_k, \beta)$$

$$= f(\alpha_n, \beta).$$

This implies $f(\alpha, E\beta) = f(\alpha, \beta)$ for every α in W. Hence

$$f(\alpha, \beta - E\beta) = 0$$

for all α in W and β in V. Thus $1 - E$ maps V into W'. The equation

$$\beta = E\beta + (1 - E)\beta$$

shows that $V = W + W'$. One final point should be mentioned. Since $W \cap W' = \{0\}$, every vector in V is uniquely the sum of a vector in W and a vector in W'. If β is in W', it follows that $E\beta = 0$. Hence $I - E$ maps V onto W'.

The projection E constructed in the proof may be characterized as follows: $E\beta = \alpha$ if and only if α is in W and $\beta - \alpha$ belongs to W'. Thus E is independent of the basis of W that was used in its construction. Hence we may refer to E as the projection of V on W that is determined by the direct sum decomposition

$$V = W \oplus W'.$$

Note that E is an orthogonal projection if and only if $W' = W^{\perp}$.

Theorem 4: Let f be a form on a real or complex vector space V and A the matrix of f in the ordered basis $\{\alpha_1, ..., \alpha_n\}$ of V. Suppose the principal minors of A are all different from 0. Then there is a unique upper triangular matrix P with $P_{kk} = 1$ $(1 \le k \le n)$ such that

$$P^*AP$$

is upper-triangular.

Proof: Since $\Delta_k(A^*) = \overline{\Delta_k(A)}$ $(1 \le k \le n)$, the principal minors of A are all different from 0. Hence, by the lemma used in the proof of Theorem 2, there exists an upper-triangular matrix P with $P_{kk} = 1$ such that A^*P is lower-triangular. Therefore, $P^*A = (A^*P)^*$ is upper-triangular. Since the product of two upper-triangular matrices is again upper triangular, it follows that P^*AP is upper-triangular. This shows the existence but not the uniqueness of P. However, there is another more geometric argument which may be used to prove both the existence and uniqueness of P.

Let W_k be the subspace spanned by $\alpha_1, ..., \alpha_k$ and W'_k the set of all β in V such that $f(\alpha, \beta) = 0$ for every α in W_k. Since $\Delta_k(A) \neq 0$, the $k \times k$ matrix M with entries

$$M_{ij} = f(\alpha_j, \alpha_i) = A_{ij}$$

$(1 \le i, j \le k)$ is invertible. By Theorem 3

$$V = W_k \oplus W'_k.$$

Let E_k be the projection of V on W_k which is determined by this decomposition, and set $E_0 = 0$. Let

$$\beta_k = \alpha_k - E_{k-1}\alpha_k, \qquad (1 \le k \le n)$$

Then $\beta_1 = \alpha_1$, and $E_{k-1}\alpha_k$ belongs to W_{k-1} for $k > 1$. Thus when $k > 1$, there exist unique scalars P_{jk} such that

$$E_{k-1}\alpha_k = -\sum_{j=1}^{k-1} P_{jk}\alpha_j$$

Setting $P_{kk} = 1$ and $P_{jk} = 0$ for $j < k$, we then have an $n \times n$ upper triangular matrix P with $P_{kk} = 1$ and

$$B_k = \sum_{j=1}^{k} P_{jk}\alpha_j$$

for $k = 1, ..., n$. Suppose $1 \le i \le k$. Then B_k is in $W_i \subset W_{k-1}$ since B_k belongs to W'_{k-1}, it follows that $f(\beta_i, \beta_k) = 0$. Let B denote the matrix of f in the ordered basis $(\beta_1, ... \beta_n)$. Then

$$B_{ki} = f(\beta_i, \beta_k)$$

so $B_{ki} = 0$ when $k > i$. Thus B is upper-triangular. On the other hand,

$$B = P^*AP.$$

Self Assessment

1. Which of the following matrices are positive?

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, \begin{bmatrix} 1 & 1+i \\ 1-i & 3 \end{bmatrix}, \begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 1 \\ 3 & -1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1/2 & 1/3 \\ 1/2 & 1/2 & 1/4 \\ 1/3 & 1/4 & 1/5 \end{bmatrix}$$

2. Prove that the product of two positive linear operators is positive if and only if they commute.

3. Let S and T be positive operators. Prove that every characteristic value of ST is positive.

8.3 Summary

- In this unit we are studying the form f on a finite vector space being non-negative.
- We obtain certain equivalent properties and show that when the matrix A of linear operator is Hermitian i.e. $A + A^*$ as well as the principal minors of the matrix A are all positive.

Notes

- It is shown that if A is the matrix of the form f in the ordered basis $\{\alpha_1, \ldots \alpha_n\}$ of V and the principal minors are all different from zero, then there exists a unique upper-triangular matrix P with $P_{kk} = 1$ $(1 \leq k \leq n)$ such that P^*AP is upper triangular.

8.4 Keywords

Non-negative Form: A form f on real or complex vector space V is non-negative if it is Hermitian and $f(\alpha, \alpha) \geq 0$.

Positive Form: A form f is positive if it is Hermitian and $f(\alpha, \alpha) > 0$

Upper Triangular Matrix: A matrix P is upper triangular one if its elements P_{ij} satisfy the relations: $P_{kk} = 1$, $1 \leq k \leq n$ and $P_{ij} = 0$ for $j > k$.

8.5 Review Questions

1. Let

$$A = \begin{bmatrix} 1 & 1/2 \\ 1/2 & 1/4 \end{bmatrix}$$

   (a) Show that A is positive

   (b) Find an invertible real matrix P such that

$$A = P^t P.$$

2. Does

   $\left[(x_1, x_2) \mid (y_1, y_2)\right] = x_1\overline{y}_1 + 2x_2\overline{y}_1 + 2x_1\overline{y}_2 + x_2\overline{y}_2$ define an inner product on c^2?

8.6 Further Readings

Books Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I N. Herstein, *Topics in Algebra*

Notes

Unit 9: Spectral Theory and Properties of Normal Operators

CONTENTS

Objectives

Introduction

9 .1 Spectral Theory

9 .2 Properties of Normal Operators

9 .3 Summary

9 .4 Keywords

9 .5 Review Questions

9 .6 Further Readings

Objectives

After studying this unit, you will be able to:

- Understand that Theorems 9 and 13 of unit 26 are pursued further concerning the diagonalization of self-adjoint and normal operators.
- See that if T is a normal operator or a self-adjoint operator on a finite dimensional inner product space V. Let C_1, C_k be the distinct characteristic values of T and W_i be the characteristic space associated with C_i and E_i be the orthogonal projection of V on W_i, then V is the direct sum of $W_1, W_2, \dots W_k$ and $T = C_1E_1 + C_2E_2 + \dots + C_k E_k$ which is called spectral resolution of T.
- See that if A is a normal matrix with real (complex) entries, then there is a real orthogonal (unitary) matrix P such that $P^{-1}AP$ is in rational canonical form.

Introduction

In this unit the properties of the normal operators or the self-adjoint operator are studied further.

The spectral resolution of the linear operator T is given by the decomposition $T = C_1E_1 + C_2E_2 + E_k C_k$, where $C_1, C_2 \dots C_k$ are the distinct characteristic values of T and $E_1, E_2 \dots E_k$ are the orthogonal projections of V on $W_1, W_2 \dots W_k$.

If T is a diagonalizable normal operator on a finite dimensional inner product space V, then T is self-adjoint, non-negative or unitary according as each characteristic value of T is real, non-negative or of absolute value 1.

The family of orthogonal projections $(P_1, P_2, \dots P_k)$ is called the resolution of the identity determined bF, and $T = \sum_j r_j(T)P_j$ is the spectral resolution of T in terms of this family.

9.1 Spectral Theory

In this unit we try to implement the findings of the Theorems 9 and 13 of unit 26 regarding the diagonalization of self-adjoint and normal operators.

We start with the following spectral theorem:

Theorem 1 (Spectral Theorem): Let T be a normal operator on a finite dimensional complex inner product space V or a self-adjoint operator on a finite dimensional real inner product space. Let $C_1, \ldots C_k$ be the distinct characteristic values of T. Let W_j be the characteristic space associated with C_j and E_j, the orthogonal projection of V on W_j. Then W_i is orthogonal to W^*_j when $i \neq j$, V is the direct sum of $W_1, W_2, \ldots W_k$ and

$$T = C_1E_1 + C_2E_2 + \ldots + C_k E_k \qquad \ldots(1)$$

Proof: Let α be a vector in W_j, β a vector in W_i, and suppose $i \neq j$. Then $c_i(\alpha \mid \beta) = (T\alpha \mid \beta) = (\alpha \mid T^*\beta) = (\alpha \mid \bar{c}_i\, \beta)$. Hence $(c_j - c_i)(\alpha \mid \beta) = 0$, and since. $c_j - c_i \neq 0$, it follows that $(\alpha \mid \beta) = 0$. Thus W_j is orthogonal to W_i, when $i \neq j$. From the fact that V has an orthonormal basis consisting of characteristic vectors (cf. Theorems 9 and 13 of unit 26), it follows that $V = W_1 + \ldots + W_k$. If α_j belongs to V_j $(1 \leq j \leq k)$ and $\alpha_1 + \ldots + \alpha_k = 0$, then

$$0 = (\alpha_i \mid \sum_j \alpha_j) = \sum_j (\alpha_i \mid \alpha_j)$$

$$= \|\alpha_i\|^2$$

for every i, so that V is the direct sum of $W_1, \ldots, W_k$. Therefore $E_1 + \ldots + E_k = I$ and

$$T = TE_1 + \ldots + TE_k.$$

$$= c_1E_1 + \ldots + c_kE_k$$

The decomposition (1) is called the spectral resolution of T. This terminology arose in part from physical applications which caused the spectrum of a linear operator on a finite-dimensional vector space to be defined as the set of characteristic values for the operator. It is important to note that the orthogonal projections $E_1, \ldots, E_k$ are canonically associated with T; in fact, they are polynomials in T.

Corollary: If $e_j = \prod_{i \neq j} \left(\dfrac{x - c_i}{c_j - c_i} \right)$, then $E_j = e_j(T)$ for $1 \leq j \leq k$.

Proof: Since $E_iE_j = 0$ when $i \neq j$, it follows that

$$T^2 = c_1^2E_1 + \ldots + c_k^2E_k$$

and by all easy induction argument that

$$T^n = c_1^nE_1 + \ldots + c_k^nE_k$$

for every integer $n \geq 0$. For an arbitrary polynomial

$$f = \sum_{n=0}^{r} \alpha_n x^n$$

we have

$$f(T) = \sum_{n=0}^{r} \alpha_n T^n$$

Notes

$$= \sum_{n=0}^{r} \alpha_n \sum_{j=1}^{k} c_j^n E_j$$

$$= \sum_{j=1}^{k} \left(\sum_{n=0}^{r} \alpha_n c_j^n \right) E_j$$

$$= \sum_{j=1}^{r} f(c_j) E_j$$

Since $e_j(c_m) = \delta_{jm}$, it follows that $e_j(T) = E_j$.

Because $E_1, . ., E_k$ are canonically associated with T and

$$I = E_1 + ... + E_k$$

the family of projections $(E_1, ..., E_k)$ is called the resolution of the identity defined by T.

There is a comment that should be made about the proof of the spectral theorem. We derived the theorem using Theorems 9 and 13 of unit 26 on the diagonalization of self-adjoint and normal operators. There is another, more algebraic, proof in which it must first be shown that the minimal polynomial of a normal operator is a product of distinct prime factors. Then one proceeds as in the proof of the primary decomposition theorem (Theorem 1) unit 18.

In various applications it is necessary to know whether one may compute certain functions of operators or matrices, e.g., square roots. This may be done rather simply for diagonalizable normal operators.

Definition: Let T be a diagonalizable normal operator on a finite-dimensional inner product space and

$$T = \sum_{j=1}^{k} c_j E_j$$

its spectral resolution. Suppose f is a function whose domain includes the spectrum of T that has values in the field of scalars. Then the linear operator $f(T)$ is defined by the equation

$$f(T) = \sum_{j=1}^{k} f(c_j) E_j. \qquad ...(2)$$

Theorem 2: Let T be a diagonalizable normal operator with spectrum S on a finite-dimensional inner product space V. Suppose f is a function whose domain contains S that has values in the field of scalars. Then $f(T)$ is a diagonalizable normal operator with spectrum $f(S)$. If U is a unitary map of V onto V' and $T' = UTU^{-1}$, then S is the spectrum of T' and

$$f(T) = Uf(T)U^{-1}.$$

Proof: The normality of $f(T)$ follows by a simple computation from (2) and the fact that

$$f(T)^* = \sum_j \overline{f(c_j)} E_j$$

Moreover, it is clear that for every α in $E_j(V)$

$$f(T)\alpha = f(c_j)\alpha.$$

Thus, the set $f(S)$ of all $f(c)$ with c in S is contained in the spectrum of $f(T)$. Conversely, suppose $\alpha \neq 0$ and that

$$f(T)\alpha = b\alpha.$$

Notes

Then $\alpha = \sum_j E_j\alpha$ and

$$f(T)\alpha = \sum_j f(T)\, E_j\alpha$$

$$= \sum_j f(c_j) E_j\alpha$$

$$= \sum_j bE_j\alpha$$

Hence,

$$\left\|\sum_j (f(c_j) - b)E_j\alpha\right\|^2 = \sum_j \left|f(c_j) - b\right|^2 \left\|E_j\alpha\right\|^2$$

$$= 0.$$

Therefore, $f(c_j) = b$ or $E_j\alpha = 0$. By assumption, $\alpha \neq 0$, so there exists an index i such that $E_i\alpha \neq 0$. It follows that $f(c_i) = b$ and hence that $f(S)$ is the spectrum of $f(T)$. Suppose, in fact, that

$$f(S) = \{b_1, \dots, b_r\}$$

where $b_m \neq b_n$ when $m \neq n$. Let X_m be the set of indices i such that $1 \leq i \leq k$ and $f(c_i) = b_m$. Let $P_m = \sum_j E_i$ the sum being extended over the indices i in X_m. Then P_m is the orthogonal projection of V on the subspace of characteristic vectors belonging to the characteristic value b_m of $f(T)$, and

$$f(T) = \sum_{m=1}^{r} b_m P_m$$

is the spectral resolution of $f(T)$.

Now suppose U is a unitary transformation of V onto V' and that $T' = UTU^{-1}$. Then the equation

$$T\alpha = C\alpha$$

holds if and only if

$$T'U\alpha = cU\alpha.$$

Thus S is; the spectrum of T', and U maps each characteristic subspace for T onto the corresponding subspace for T'. In fact, using (2), we see that

$$T' = \sum_j c_j E'_j, \quad E'_j = UE_jU^{-1}$$

is the spectral resolution of T'. Hence

$$f(T') = \sum_j f(c_j) E'_j$$

$$= \sum_j f(c_j) UE_jU^{-1}$$

$$= U\left(\sum_j f(c_j)E_j\right)U^{-1}$$

$$= Uf(T)^{-1}$$

In thinking about the preceding discussion, it is important for one to keep in mind that the spectrum of the normal operator T is the set

$$S = \{c_1, \dots, c_k\}$$

of distinct characteristic values. When T is represented by a diagonal matrix in a basis of characteristic vectors, it is necessary to repeat each value c_j as many times as the dimension of the corresponding space of characteristic vectors. This is the reason for the change of notation in the following result.

Corollary: With the assumptions of Theorem 2, suppose that T is represented in the ordered basis $\beta = \{\alpha_1, \dots, \alpha_n\}$ by the diagonal matrix D with entries $d_1, \dots, d_n$. Then, in the basis β, $f(T)$ is represented by the diagonal matrix $f(D)$ with entries $f(d_1), \dots, f(d_n)$. If $\beta' = \{\alpha'_1, \dots, \alpha'_n\}$ is any other ordered basis and P the matrix such that

$$\alpha'_j = \sum_j P_{ij}\alpha_i$$

then $P^{-1} f(D)P$ is the matrix of $f(T)$ in the basis β'.

Proof: For each index i, there is a unique j such that $1 \le j \le k$, α_i belongs to $E_j(V)$, and $d_i = c_j$. Hence $f(T)\alpha_i = f(d_i)\alpha_i$ for every i, and

$$\begin{aligned} f(T)\alpha'_j &= \sum_j P_{ij} f(T)\alpha_i \\ &= \sum_j d_i P_{ij}\alpha_i \\ &= \sum_j (DP)_{ij}\alpha_i \\ &= \sum_j (DP)_{ij} \sum_k P^{-1}_{ki}\alpha'_k \\ &= \sum_k (P^{-1}DP)_{kj}\alpha'_k. \end{aligned}$$

It follows from this result that one may form certain functions of a normal matrix. For suppose A is a normal matrix. Then there is an invertible matrix P, in fact a unitary P, such that PAP^{-1} is a diagonal matrix, say D with entries $d_1, \dots, d_n$; Let f be a complex-valued function which can be applied to $d_1, \dots d_n$, and let $f(D)$ be the diagonal matrix with entries $f(d_1) \dots f(d_n)$. Then $P^{-1}f(D)P$ is independent of D and just a function of A in the following sense. If Q is another invertible matrix such that QAQ^{-1} is a diagonal matrix D', then f may be applied to the diagonal entries of D' and

$$P^{-1} f(D)P = Q^{-1} f(D')Q.$$

Definition: Under the above conditions, $f(A)$ is defined as $P^{-1} f(D)P$.

Theorem 3: Let A be a normal matrix and $c_1, \dots, c_k$, the distinct complex roots of $\det(xI - A)$. Let

$$e_i = \prod_{j \ne i}\left(\frac{x - c_j}{c_i - c_j}\right)$$

and $E_i = e_i(A)$ $(1 \le i \le k)$. Then $E_iE_j = 0$ when $i \ne j$, $E_1^2 = E_i$, $E_i^* = E_i$,

and

$$I = E_1 + \dots + E_k.$$

Notes

If f is a complex-valued function whose domain includes $c_1, ..., c_k$, then

$$f(A) = f(c_1)E_1 + ... + f(c_k)E_k;$$

in particular, $A = c_1E_1 + ... + c_kE_k$.

We recall that an operator on an inner product space V is non-negative if T is self-adjoint and $(T\alpha \mid \alpha) \geq 0$ for every α in V.

Theorem 4: Let T be a diagonalizable normal operator on a finite-dimensional inner product space V. Then T is self-adjoint, non-negative, or unitary according as each characteristic value of T is real, non-negative, or of absolute value 1.

Proof: Suppose T has the spectral resolution $T = c_1E_1 + ... + c_kE_k$, then $T^* = \bar{c}_1E_1 + ... + \bar{c}_kE_k$. To say T is self-adjoint is to say $T = T^*$, or

$$(c_1 - \bar{c}_1)E_1 + ... + (c_k - \bar{c}_k)E_k = 0.$$

Using the fact that $E_iE_j = 0$ for $i \neq j$, and the fact that no E_j, is the zero operator, we see that T is self-adjoint if and only if $c_j = \bar{c}_j$, j = 1, ... , k. To distinguish the normal operators which are non-negative, let us look at

$$(T\alpha \mid \alpha) = \left(\sum_{j=1}^{k} c_jE_j\alpha \mid \sum_{i=1}^{k} E_i\alpha\right)$$

$$= \sum_i \sum_j c_j(E_j\alpha \mid E_i\alpha)$$

$$= \sum_j c_j \|E_j\alpha\|^2$$

We have used the fact that $(E_j\alpha \mid E_i\alpha) = 0$ for $i \neq$ j. From this it is clear that the condition $(T\alpha \mid \alpha) \geq 0$ is satisfied if and only if $c_j \geq 0$ for each j. To distinguish the unitary operators, observe that

$$TT^* = c_1c_1E_1 + ... + c_kc_kE_k.$$

$$= |c_1|^2E_1 + ... + |c_k|^2E_k.$$

If $TT^* = I$, then $I = |c_1|^2E_1 + ... + |c_k|^2E_k$, and operating with E_j

$$Ej = |c_j|^2E_j.$$

Since $E_j \neq 0$, we have $|c_j|^2 = 1$ or $|c_j| = 1$. Conversely, if $|c_j|^2 = 1$ for each j it is clear that $TT^* = I$.

It is important to note that this is a theorem about normal operators. If T is a general linear operator on V which has real characteristic values, it does not follow that T is self-adjoint. The theorem states that if T has real characteristic values, and if T is diagonalizable and normal, then T is self-adjoint. A theorem of this type serves to strengthen the analogy between the adjoint operation and the process of forming the conjugate of a complex number. A complex number z is real or of absolute value 1 according as $z = \bar{z}$, or $\bar{z}z = 1$. An operator T is self-adjoint or unitary according as $T = T^*$ or $T^*T = I$.

We are going to prove two theorems now, which are the analogues of these two statements:

1. Every non-negative number has a unique non-negative square root.

2. Every complex number is expressible in the form ru, where r is non-negative and $|u| = 1$. This is the polar decomposition $z = re^{i\phi}$ for complex numbers.

Theorem 5: Let V be a finite-dimensional inner product space and T a non-negative operator on V. Then T has a unique non-negative square root, that is, there is one and only one non-negative operator N on V such that $N^2 = T$.

Proof: Let $T = c_1E_1 + ... + c_kE_k$ be the spectral resolution of T. By Theorem 4, each $c_j \geq 0$. If c is any non-negative real number, let $\sqrt{c}$ denote the non-negative square root of c. Then according to Theorem 3 and (2) $N = \sqrt{T}$ is a well-defined diagonalizable normal operator on V. It is non-negative by Theorem 4, and, by an obvious computation, $N^2 = T$.

Now let P be a non-negative operator on V such that $P^2 = T$. We shall prove that $P = N$. Let

$$P = d_1F_1 + ... + d_rF_r$$

be the spectral resolution of P. Then $d_j \geq 0$ for each j, since P is non-negative. From $P^2 = T$ we have

$$T = d_1^2F_1 + ... + d_r^2F_r.$$

Now $F_1, ..., F_r$ satisfy the conditions $I = F_1 + ... + F_r$, $F_iF_j = 0$ for $i \neq j$, and no F_j is 0. The numbers d_1^2 ..., d_r^2 are distinct, because distinct non-negative numbers have distinct squares. By the uniqueness of the spectral resolution of T, we must have $r = k$, and (perhaps reordering) F_j, $= E_j$, $d_j^2 = c_j$. Thus $P = N$.

Theorem 6: Let V be a finite-dimensional inner product space and let T be any linear operator on V. Then there exist a unitary operator U on V and a non-negative operator N on V such that $T = UN$. The non-negative operator N is unique. If T is invertible, the operator U is also unique.

Proof: Suppose we have $T = UN$, where U is unitary and N is non-negative. Then $T^* = (UN)^* = N^*U^* = NU^*$. Thus $T^*T = NU^*UN = N^2$. This shows that N is uniquely determined as the non-negative square root of the non-negative operator T^*T.

So, to begin the proof of the existence of U and N, we use Theorem 5 to define N as the unique non-negative square root of T^*T. If T is invertible, then so is N because

$$(N\alpha|N\alpha) = (N^2\alpha|\alpha) = (T^*T\alpha|\alpha) = (T\alpha|T\alpha).$$

In this case, we define $U = TN^{-1}$ and prove that U is unitary. Now $U^* = (TN^{-1})^* = (N^{-1})^*T^* = (N^*)^{-1}T^* = N^{-1}T^*$. Thus

$$\begin{aligned} UU^* &= TN^{-1}N^{-1}T^* \\ &= T(N^{-1})^2T^* \\ &= T(N^2)^{-1}T^* \\ &= T(T^*T)^{-1}T^* \\ &= TT^{-1}(T^*)^{-1}T^* \\ &= I \end{aligned}$$

and C is unitary.

If T is not invertible, we shall have to do a bit more work to define U. We first define U on the range of N. Let α be a vector in the range of N say $\alpha = N\beta$. We define $U\alpha = T\beta$, motivated by the fact that we want $UB\beta = T\beta$. We must verify that U is well-defined on the range of N in other words, if $N\beta' = N\beta$ then $T\beta' = T\beta$. We verified above that $||N\gamma||^2 = ||T\gamma|^2$ for every γ in V. Thus, with $\gamma = \beta - \beta'$, we see that $N(\beta - \beta') = 0$ if and only if $T(\beta - \beta') = 0$. So U is well-defined on the range of N and is clearly linear where defined. Now if W is the range of N, we are going to define U on $W^\perp$. To do this, we need the following observation. Since T and N have the same null space, their ranges have the same dimension. Thus $W^\perp$ has the same dimension as the orthogonal complement of the range of T. Therefore, there exists an (inner product space) isomorphism U_0 of $W^\perp$ onto $T(V)^\perp$. Now we have defined U on W, and we define U on $W^\perp$ to be U_0.

Notes

Let us repeat the definition of U. Since $V = W \oplus W^{\perp}$, each α in V is uniquely expressible in the form $\alpha = N\beta + \gamma$, where $N\beta$ is in the range W of N, and γ is in $W^{\perp}$. We define

$$U\alpha = T\beta + U_0\gamma.$$

This U is clearly linear, and we verified above that it is well-defined. Also

$$\begin{aligned}(U\alpha|U\alpha) &\ (T\beta + U_0\gamma|T\beta + U_0\gamma)\\ &= (T\beta|T\beta) + (U_0\gamma|U_0\gamma)\\ &= (N\beta|N\beta) + (\gamma|\gamma)\\ &= (\alpha|\alpha)\end{aligned}$$

and so U is unitary. We also have $UN\beta = T\beta$ for each β.

We call $T = UN$ a polar decomposition for T. We certainly cannot call it the polar decomposition, since U is not unique. Even when T is invertible, so that U is unique, we have the difficulty that U and N may not commute. Indeed, they commute if and only if T is normal. For example, if $T = UN = NU$, with N non-negative and U unitary, then

$$TT^* = (NU)(NU)^* = NUU^*N = N^2 = T^*T.$$

The general operator T will also have a decomposition $T = N_1U_1$, with N_1 non-negative and U_1 unitary. Here, N_1 will be the non-negative square root of TT^*. We can obtain this result by applying the theorem just proved to the operator T^*, and then taking adjoints.

We turn now to the problem of what can be said about the simultaneous diagonalization of commuting families of normal operators. For this purpose the following terminology is appropriate.

Definition: Let $\mathcal{F}$ be a family of operators on an inner product space V. A function r on $\mathcal{F}$ with values in the field $\mathcal{K}$ of scalars will be called a root of $\mathcal{F}$ if there is a non-zero α in V such that

$$T\alpha = r(T)\alpha$$

for all T in $\mathcal{F}$. For any function r from $\mathcal{F}$ to $\mathcal{K}$, let $V(r)$ be the set of all α in V such that $T\alpha = r(T)\alpha$ for every T in $\mathcal{F}$.

Then $V(r)$ is a subspace of V, and r is a root of $\mathcal{F}$ if and only if $V(r) \neq \{0\}$. Each non-zero α in $V(r)$ is simultaneously a characteristic vector for every T in $\mathcal{F}$.

Theorem 7: Let $\mathcal{F}$ be a commuting family of diagonalizable normal operators on a finite-dimensional inner product space V. Then $\mathcal{F}$ has only a finite number of roots. If $r_1, \dots, r_k$ are the distinct roots of $\mathcal{F}$, then

(i) $V(r_i)$ is orthogonal to $V(r_j)$ when $i \neq j$, and

(ii) $V = V(r_1) \oplus \dots \oplus V(r_k)$.

Proof: Suppose r and s are distinct roots of $\mathcal{F}$. Then there is an operator T in $\mathcal{F}$ such that $r(T) \neq s(T)$. Since characteristic vectors belonging to distinct characteristic values of T are necessarily orthogonal, it follows that $V(r)$ is orthogonal to $V(s)$. Because V is finite-dimensional, this implies $\mathcal{F}$ has at most a finite number of roots. Let $r_1, \dots, r_k$, be the roots of F. Suppose $\{T_1, \dots, T_m\}$ is a maximal linearly independent subset of $\mathcal{F}$, and let

$$\{E_{i1}, E_{i2}, \dots\}$$

be the resolution of the identity defined by T_i, $(1 \leq i \leq m)$. Then the projections E_{ij} form a commutative family. For each E_{ij} is a polynomial in T_i and $T_1, \dots, T_m$, commute with one another.

Since

$$I = \left(\sum_{j_1} E_{1ji}\right)\left(\sum_{j_2} E_{2j_2}\right)\left(\sum_{jm} E_{mj_m}\right)$$

each vector α in V may be written in the form

$$\alpha = \sum_{j_1 ..., j_m} E_{1j_1} E_{2j_2} ... E_{mj_m} \alpha. \qquad \text{... (3)}$$

Suppose $j_1, ..., j_m$, are indices for which $\beta = E_{1j1}E_{2j2}, ... E_{mjm}\ \alpha \neq 0$. Let

$$\beta_i = \left(\underset{n \neq i}{\text{II}}\ E_{nj_n}\right)\alpha.$$

Then $\beta = E_{ij}\beta_i$; hence there is a scalar c_i such that

$$T_1\beta = c_i\beta, \quad 1 \leq i \leq m.$$

For each T in $\mathcal{F}$, there exist unique scalars b_i such that

$$T = \sum_{i=1}^{m} b_i T_i$$

Thus

$$T\beta = \sum_i b_i T_i \beta$$

$$= \left(\sum_i b_i c_i\right)\beta.$$

The function $T \to \sum_i b_i c_i$, is evidently one of the roots, say r_i or $\mathcal{F}$, and β lies in $V(r_i)$. Therefore, each non-zero term in (3) belongs to one of the spaces $V(r_1)$, ..., $V(r_k)$. It follows that V is the orthogonal direct sum of $V(r_1)$, ...,$V(r_k)$.

Corollary: Under the assumptions of the theorem, let P_j be the orthogonal projection of V on $V(r_j)$ $(1 \leq j \leq k)$. Then $P_iP_j = 0$ when $i \neq j$,

$$I = P_1 + ... + P_k,$$

and every T in $\mathcal{F}$ may be written in the form

$$T = \sum_i r_j(T) P_j. \qquad \text{... (4)}$$

Definition: The family of orthogonal projections $\{P_1, ..., P_k\}$ is called the resolution of the identity determined by $\mathcal{F}$, and (4) is the spectral resolution of T in terms of this family.

Although the projections $P_1, ..., P_k$, in the preceding corollary are canonically associated with the family $\mathcal{F}$, they are generally not in $\mathcal{F}$ nor even linear combinations of operators in $\mathcal{F}$; however, we shall show that they may be obtained by forming certain products of polynomials in elements of $\mathcal{F}$.

In the study of any family of linear operators on an inner product space, it is usually profitable to consider the self-adjoint algebra generated by the family.

Definition: A self-adjoint algebra of operators on an inner product space V is a linear sub-algebra of $L(V, V)$ which contains the adjoint of each of its members.

An example of a self-adjoint algebra is $L(V, V)$ itself. Since the intersection of any collection of self-adjoint algebras is again a self-adjoint algebra, the following terminology is meaningful.

Definition: If $\mathcal{F}$ is a family of linear operators on a finite-dimensional inner product space, the self-adjoint algebra generated by $\mathcal{F}$ is the smallest self-adjoint algebra which contains $\mathcal{F}$.

Theorem 8: Let $\mathcal{F}$ be a commuting family of diagonalizable normal operators on a finite-dimensional inner product space V, and let $\mathcal{A}$ be the self-adjoint algebra generated by $\mathcal{F}$ and the identity operator. Let $\{P_1,..., P_k\}$ be the resolution of the identity defined by $\mathcal{F}$. Then $\mathcal{A}$ is the set of all operators on V of the form

$$T = \sum_{j=1}^{k} c_j P_j \qquad \text{… (15)}$$

where $c_1, ..., c_k$ are arbitrary scalars.

Proof: Let $\mathcal{E}$ denote the set of all operators on V of the form (15). Then $\mathcal{E}$ contains the identity operator and the adjoint

$$T^* = \sum_j \bar{c}_j P_j$$

of each of its members. If $T = \sum_j c_j P_j$ and $U = \sum_j d_j P_j$, then for every scalar a

$$aT + U = \sum_j (ac + d_j) P_j$$

and

$$\begin{aligned} TU &= \sum_{i,j} c_i d_j P_i P_j \\ &= \sum_j c_i d_j P_j \\ &= UT. \end{aligned}$$

Thus $\mathcal{E}$ is a self-adjoint commutative algebra containing $\mathcal{F}$ and the identity operator. Therefore $\mathcal{E}$ contains $\mathcal{A}$.

Now let $r_1, ..., r_k$ be all the roots of $\mathcal{F}$. Then for each pair of indices (i, n) with $i \neq n$, there is an operator T_{in} in $\mathcal{F}$ such that $r_i(T_{in}) \neq r_n(T_{in})$. Let $a_{in} = r_i(T_{in}) - r_n(T_{in})$ and $b_{in} = r_n(T_{in})$. Then the linear operator

$$Q_i = \prod_{n \neq i} a_{in}^{-1} \, (T_{in} - b_{in} I)$$

is an element of the algebra $\mathcal{A}$. We will show that $Q_i = P_i$ $(1 \leq i \leq k)$. For this, suppose $j \neq i$ and that α is an arbitrary vector in $V(r_j)$. Then

$$\begin{aligned} T_{ij}\alpha &= r_j(T_{ij})\alpha \\ &= b_{ij}\alpha \end{aligned}$$

so that $(T_{ij} - b_{ij}I)\alpha = 0$. Since the factors in Q_i all commute, it follows that $Q_1\alpha = 0$. Hence Q_i agrees with P_i on $V(r_j)$ whenever $j \neq i$. Now suppose α is a vector in $V(r_i)$. Then $T_{in}\alpha = r_i(T_{in})\alpha_j$ and

$$a_{in}^{-1}(T_{in} - b_{in}I)\alpha = a_{\text{in}}^{-1}[r_i(T_{in}) - r_n(T_{in})]\alpha = \alpha.$$

Thus $Q_i\alpha = \alpha$ and Q_i agrees with P_i on $V(r_i)$; therefore, $Q_i = P_i$ for -i = 1, ... , k. From this it follows that $\mathcal{A} = \mathcal{E}$.

Notes

The theorem shows that the algebra $\mathcal{A}$ is commutative and that each element of $\mathcal{A}$ is a diagonalizable normal operator. We show next that $\mathcal{A}$ has a single generator.

Corollary: Under the assumptions of the theorem, there is an operator T in $\mathcal{A}$ such that every member of $\mathcal{A}$ is a polynomial in T.

Proof: Let $T = \sum_{j=1}^{k} t_j P_j$ where $t_1, \ldots, t_k$ are distinct scalars. Then

$$T^n = \sum_{j=1}^{k} t_j^n P_j$$

for $n = 1, 2, \ldots$ If

$$f = \sum_{n=1}^{8} a_n x^n$$

it follows that

$$f(T) = \sum_{n=1}^{8} a_n T^n = \sum_{n=1}^{8} \sum_{j=1}^{k} a_n t_j^n P_j$$

$$= \sum_{j=1}^{k} \left(\sum_{n=1}^{8} a_n t_j^n \right) P_j$$

$$= \sum_{j=1}^{k} f(t_j) P_j$$

Given an arbitrary

$$U = \sum_{j=1}^{k} c_j P_j$$

in $\mathcal{A}$, there is a polynomial f such that $f(t_j) = c_j$ $(1 \le j \le k)$, and for any such f, $U = f(T)$.

9.2 Properties of Normal Operators

In unit 26 we developed the basic properties of self-adjoint and normal operators, using the simplest and most direct methods possible. In last section we considered various aspects of spectral theory. Here we prove some results of a more technical nature which are mainly about normal operators on real spaces.

We shall begin by proving a sharper version of the primary decomposition theorem of unit 18 for normal operators. It applies to both the real and complex cases.

Theorem 9: Let T be a normal operator on a finite-dimensional inner product space V. Let p be the minimal polynomial for T and $p_1, \ldots, p_k$ its distinct monic prime factors. Then each p_j occurs with multiplicity 1 in the factorization of p and has degree 1 or 2. Suppose W_j is the null space of $p_j(T)$. Then

(i) W_j is orthogonal to W_i when $i \neq j$;

(ii) $V = W_1 \oplus \ldots \oplus W_k$;

(iii) W_j is invariant under T, and p_j is the minimal polynomial for the restriction of T to W_j;

Notes

(iv) for every j, there is a polynomial e_j with coefficients in the scalar field such that $e_j(T)$ is the orthogonal projection of V on W_j.

In the proof we use certain basic facts which we state as lemmas.

Lemma 1: Let N be a normal operator on an inner product space W. Then the null space of N is the orthogonal complement of its range.

Proof: Suppose $(\alpha | N\beta) = 0$ for all β in W. Then $(N^*\alpha | \beta) = 0$ for all β; hence $N^*\alpha = 0$. By Theorem 10 of unit 26, this implies $N\alpha = 0$. Conversely, if $N\alpha = 0$, then $N^*\alpha = 0$, and

$$(N^*\alpha | \beta) = (\alpha | N\beta) = 0$$

for all β in W.

Lemma 2: If N is a normal operator and α is a vector such that $N^2\alpha = 0$, then $N\alpha = 0$.

Proof: Suppose N is normal and that $N^2\alpha = 0$. Then $N\alpha$ lies in the range of N and also lies in the null space of N. By Lemma 1, this implies $N\alpha = 0$.

Lemma 3: Let T be a normal operator and f any polynomial with coefficients in the scalar field. Then $f(T)$ is also normal.

Proof: Suppose $f = a_0 + a_1x + \ldots + a_nx^n$. Then

$$f(T) = a_0I + a_1T + \ldots + a_nT^n$$

and $$f(T)^* = \bar{a}_0 I + \bar{a}_1 T^* + \cdots + \bar{a}_n (T^*)^n.$$

Since $T^*T = TT^*$, it follows that $f(T)$ commutes with $f(T)^*$.

Lemma 4: Let T be a normal operator and f, g relatively prime polynomials with coefficients in the scalar field. Suppose α and β are vectors such that $f(T)\alpha = 0$ and $g(T)\beta = 0$. Then $(\alpha | \beta) = 0$.

Proof: There are polynomials a and b with coefficients in the scalar field such that $af + bg = 1$. Thus

$$a(T)\,f(T) + b(T)\,g(T) = I$$

and $\alpha = g(T)\,b(T)\alpha$. It follows that

$$(\alpha | \beta) = (g(T)\,b(T)\,\alpha | \beta) = (b(T)\,\alpha | g(T)^*\beta)$$

By assumption $g(T)\beta = 0$. By Lemma 3, $g(T)$ is normal. Therefore, by Theorem 10 of unit 26, $g(T)^*\beta = 0$; hence $(\alpha | \beta) = 0$.

Proof of Theorem 9: Recall that the minimal polynomial for T is the monic polynomial of least degree among all polynomials f such that $f(T) = 0$. The existence of such polynomials follows from the assumption that V is finite-dimensional. Suppose some prime factor p_j of p is repeated. Then $p = p_j^2 g$ for some polynomial g. Since $p(T) = 0$, it follows that

$$(p_j(T))^2\,g(T)\alpha = 0$$

for every α in V. By Lemma 3, $p_j(T)$ is normal. Thus Lemma 2 implies

$$p_j(T)g(T)\alpha = 0$$

for every α in V. But this contradicts the assumption that p has least degree among all f such that $f(T) = 0$. Therefore, $p = p_1 \ldots p_k$. If V is a complex inner product space each p_j is necessarily of the form

$$p_j = x - c_j$$

with c_j real or complex. On the other hand, if V is a real inner product space, then $p_j = x_j - c_j$ with c_j in R or

Notes

$$p_j = (x - c)(x - \bar{c})$$

where c is a non-real complex number.

Now let $f_j = p/p_j$. Then, since $f_1, \ldots, f_k$ are relatively prime, there exist polynomials g_j with coefficients in the scalar field such that

$$1 = \sum_j f_j g_j. \qquad \ldots (6)$$

We briefly indicate how such g_j may be constructed. If $p_j = x - c_j$, then $f_j(c_j) \neq 0$, and for g_j we take the scalar polynomial $1/f_j(c_j)$. When every p_j is of this form, the $f_j g_j$ are the familiar Lagrange polynomials associated with $c_1, \ldots, c_k$, and (6) is clearly valid. Suppose some $p_j = (x - c)(x - \bar{c})$ with c a non-real complex number. Then V is a real inner product space, and we take

$$g_j = \frac{x - \bar{c}}{s} + \frac{x - c}{\bar{s}}$$

where $s = (c - \bar{c}) f_j(c)$. Then

$$g_j = \frac{(s - \bar{s})x - (cs + \bar{c}s)}{s\bar{s}}$$

so that g_j is a polynomial with real coefficients. If p has degree n, then

$$1 - \sum_j f_j g_j$$

is a polynomial with real coefficients of degree at almost $n - 1$; moreover, it vanishes at each of the n (complex) roots of p, and hence is identically 0.

Now let α be an arbitrary vector in V. Then by (16)

$$\alpha = \sum_j f_j(T) g_j(T)\alpha$$

and since $p_j(T) f_j(T) = 0$, it follows that $f_j(T)\, g_j(T)\alpha$ is in W_j for every j. By Lemma 4, W_j is orthogonal to W_j whenever $i \neq j$. Therefore, V is the orthogonal direct sum of $W_1, \ldots, W_k$. If β is any vector in W_j, then

$$p_j(T)\, T\beta = Tp_j(T)\beta = 0;$$

thus W_j is invariant under T. Let T_j be the restriction of T to W_j. Then $p_j(T_j) = 0$, so that p_j is divisible by the minimal polynomial for T_j. Since p_j is irreducible over the scalar field, it follows that p_j is the minimal polynomial for T_j.

Next, let $e_j = f_j g_j$ and $E_j = e_j(T)$. Then for every vector α in V, $E_j\alpha$ is in W_j, and

$$\alpha = \sum_j E_j\alpha$$

Thus $\alpha - E_j\alpha = \sum_{j \neq i} E_j\alpha$ since W_j is orthogonal to W_j when $j \neq i$, this implies that $\alpha - E_j\alpha$ is in $W_i^{\perp}$. It now follows from Theorem 4 of unit 24 that E_i is the orthogonal projection of V on W_i.

Definition: We call the subspaces W_j $(1 \leq j \leq k)$ the primary components of V under T.

Corollary: Let T be a normal operator on a finite-dimensional inner product space V and $W_1, \ldots, W_k$ the primary components of V under T. Suppose W is a subspace of V which is invariant under T.

Notes

Then

$$W = \sum_j W \cap W_j$$

Proof: Clearly W contains $\sum_j W \cap W_j$. On the other hand, W_j being invariant under T_j is invariant under every polynomial in T. In particular, W is invariant under the orthogonal projection E_j of V on W_j. If α is in W_j it follows that $E_j\alpha$ is in $W \cap W_j$, and, at the same time, $\alpha = \sum_j E_j\alpha$. Therefore, W is contained in $\sum_j W \cap W_j$.

Theorem 9 shows that every normal operator T on a finite-dimensional inner product space is canonically specified by a finite number of normal operators T_j, defined on the primary components W_j of V under T, each of whose minimal polynomials is irreducible over the field of scalars. To complete our understanding of normal operators it is necessary to study normal operators of this special type.

A normal operator whose minimal polynomial is of degree 1 is clearly just a scalar multiple of the identity. On the other hand, when the minimal polynomial is irreducible and of degree 2 the situation is more complicated.

Example 1: Suppose $r > 0$ and that θ is a real number which is not an integral multiple of π. Let T be the linear operator on R^2 whose matrix in the standard orthonormal basis is

$$A = r\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

Then T is a scalar multiple of an orthogonal transformation and hence normal. Let p be the characteristic polynomial of T. Then

$$\begin{aligned} p &= \det(xI - A) \\ &= (x - r\cos\theta)^2 + r^2\sin^2\theta \\ &= x - 2r\cos\theta x + r^2. \end{aligned}$$

Let $a = r\cos\theta$, $b = r\sin\theta$, and $c = a + ib$. Then $b \neq 0$, $c = re^{i\theta}$

$$A = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

and $p = (x - c)(x - \bar{c})$. Hence p is irreducible over R. Since p is divisible by the minimal polynomial for T, it follows that p is the minimal polynomial.

This example suggests the following converse.

Theorem 10: Let T be a normal operator on a finite-dimensional real inner product space V and p its minimal polynomial. Suppose

$$p = (x - a)^2 + b^2$$

where a and b are real and $b \neq 0$. Then there is an integer $s > 0$ such that p^8 is the characteristic polynomial for T, and there exist subspaces $V_1, \ldots, V_s$ of V such that

(i) V_j is orthogonal to V_i when $i \neq j$;

(ii) $V = V_1 \oplus \ldots \oplus V_s$;

(iii) each V_j has an orthonormal basis $\{\alpha_j, \beta_j\}$ with the property that

$$T\alpha_j = a\alpha_j + b\beta_j$$

$$T\beta_j = -b\alpha_j + a\beta_j.$$

In other words, if $r = \sqrt{a^2 + b^2}$ and θ is chosen so that $a = r\cos\theta$ and $b = r\sin\theta$, then V is an orthogonal direct sum of two-dimensional subspaces V_j on each of which T acts as 'r times rotation through the angle θ'.

The proof of Theorem 10 will be based on the following result.

Lemma: Let V be a real inner product space and S a normal operator on V such that $S^2 + I = 0$. Let α be any vector in V and $\beta = S\alpha$. Then

$$\left.\begin{aligned} S^*\alpha &= -\beta \\ S^*\beta &= \alpha \end{aligned}\right\} \qquad \dots (1)$$

$(\alpha \mid \beta) = 0$, and $\| \alpha \| = \| \beta \|$.

Proof: We have $S\alpha = \beta$ and $S\beta = S^2\alpha = -\alpha$. Therefore $0 = \| S\alpha - \beta \|^2 + \| S\beta + \alpha \|^2 = \| S\alpha \|^2 - 2(S\alpha \mid \beta) + \| \beta \|^2 + \| S\beta \|^2 + 2(S\beta \mid \alpha) + \| \alpha \|^2$.

Since S is normal, it follows that

$0 = \| S^*\alpha \|^2 - 2(S^*\beta \mid \alpha) + \| \beta \|^2 + \| S^*\beta \|^2 + 2(S^*\alpha \mid \beta) + \| \alpha \|^2 = \| S^*\alpha + \beta \|^2 + \| S^*\beta - \alpha \|^2$.

This implies (1); hence

$$\begin{aligned} (\alpha \mid \beta) &= (S^*\beta \mid \beta) = (\beta \mid S\beta) \\ &= (\beta \mid -\alpha) \\ &= -(\alpha \mid \beta) \end{aligned}$$

and $(\alpha \mid \beta) = 0$. Similarly

$$\| \alpha \|^2 = (S^*\beta \mid \alpha) = (\beta \mid S\alpha) = \| \beta \|^2.$$

Proof of Theorem 10: Let $V_1, \dots, V_s$ be a maximal collection of two-dimensional subspaces satisfying (i) and (ii), and the additional conditions.

$$\begin{aligned} T^*\alpha_j &= a\alpha_j - b\beta_j, \\ 1 &\le j \le s. \qquad \dots (2) \\ T^*\beta_j &= b\alpha_j - a\beta_j \end{aligned}$$

Let $W' = V_1 + \dots + V_s$. Then W is the orthogonal direct sum of $V_1, \dots, V_s$. We shall show that $W = V$. Suppose that this is not the case. Then $W^\perp \neq \{0\}$. Moreover, since (iii) and (2) imply that W is invariant under T and T^*, it follows that $W^\perp$ is invariant under T^* and $T = T^{**}$. Let $S = b^{-1}(T - aI)$. Then $S^* = b^{-1}(T^* - aI)$, $S^*S = SS^*$, and $W^\perp$ is invariant under S and S^*. Since $(T - aI)^2 + b^2I = 0$, it follows that $S^2 + I = 0$. Let α be any vector of norm 1 in $W^\perp$ and set $\beta = S\alpha$. Then β is in $W^\perp$ and $S\beta = -\alpha$. Since $T = aI + bS$, this implies

$$T\alpha = a\alpha + b\beta$$

$$T\beta = -b\alpha + a\beta.$$

By the lemma, $S^*\alpha = -\beta$, $S^*\beta = \alpha$, $(\alpha \mid \beta) = 0$, and $\| \beta \| = 1$. Because $T^* = aI + bS^*$, it follows that

$$T^*\alpha = a\alpha - b\beta$$

$$T^*\beta = b\alpha + a\beta.$$

Notes

But this contradicts the fact that $V_1, \ldots V_s$ is a maximal collection of subspaces satisfying (i), (iii), and (2). Therefore, $W = V$, and since

$$\det\begin{bmatrix} x-a & b \\ -b & x-a \end{bmatrix} = (x - a)^2 + b^2$$

it follows from (i), (ii) and (iii) that

$$\det (xI - T) = [(x - a)^2 + b^2]^s.$$

Corollary: Under the conditions of the theorem, T is invertible, and

$$T^* = (a^2 + b^2)\, T^{-1}.$$

Proof: Since

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix}\begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} a^2+b^2 & 0 \\ 0 & a^2+b^2 \end{bmatrix}$$

it follows from (iii) and (2) that $TT^* = (a^2 + b^2)I$. Hence T is invertible and $T^* = (a^2 + b^2)T^{-1}$.

Theorem 11: Let T be a normal operator on a finite-dimensional inner product space V. Then any linear operator that commutes with T also commutes with T^*. Moreover, every subspace invariant under T is also invariant under T^*.

Proof: Suppose U is a linear operator on V that commutes with T. Let E, be the orthogonal projection of V on the primary component W_j $(1 \le j \le k)$ of V under T. Then E_j is a polynomial in T and hence commutes with U. Thus

$$E_jUE_j = UE_j^2 = UE_j.$$

Thus $U(W_j)$ is a subset of W_j. Let T_j and U_j denote the restrictions of T and U to W_j. Suppose I_j is the identity operator on W_j. Then U_j commutes with T_j, and if $T_j = c_jI_j$, it is clear that U_j also commutes with $T_j^* = \bar{c}_jI_j$. On the other hand, if T_j is not a scalar multiple of I_j, then T_j is invertible and there exist real numbers a_j and b_j such that

$$T_j^* = \left(a_j^2 + b_j^2\right)T_j^{-1}.$$

Since $U_jT_j = T_jU_j$, it follows that $T_j^{-1}U_j = U_jT_j^{-1}$. Therefore U_j commutes with T_j^* in both cases. Now T^* also commutes with E_j, and hence W_j is invariant under T^*. Moreover for every α and β in W_j

$$(T_j\alpha \mid \beta) = (T\alpha \mid \beta) = (\alpha \mid T^*\beta) = (\alpha \mid T_j^*\beta).$$

Since $T^*(W_j)$ is contained in W_j, this implies T_j^* is the restriction of T^* to W_j. Thus

$$UT^*\alpha_j = T^*U\alpha_j$$

for every α_j in W_j. Since V is the sum of $W_1, \ldots, W_k$, it follows that

$$UT^*\alpha = T^*U\alpha$$

for every α in V and hence that U commutes with T^*.

Now suppose W is a subspace of V that is invariant under T, and let $Z_j = W \cap W_j$. By the corollary to Theorem 9, $W = \sum_j Z_j$. Thus it suffices to show that each Z_j is invariant under T_l^*. This is clear if $T_j = c_jI$. When this is not the case, T_j is invertible and maps Z_j into and hence onto Z_j. Thus $T_j^{-1}(Z_j) = Z_j$, and since

$$T_j^* = \left(a_j^2 + b_j^2\right)T_j^{-1}$$

it follows that $T^*(Z_j)$ is contained in Z_j, for every j.

Suppose T is a normal operator on a finite-dimensional inner product space V. Let W be a subspace invariant under T. Then the preceding corollary shows that W is invariant under T^*. From this it follows that $W^\perp$ is invariant under $T^{**} = T$ (and hence under T^* as well). Using this fact one can easily prove the following strengthened version of the cyclic decomposition theorem.

Theorem 12: Let T be a normal linear operator on a finite-dimensional inner product space V ($\dim V \geq 1$). Then there exist r non-zero vectors $\alpha_1, \ldots, \alpha_r$ in V with respective T-annihilators $e_1, \ldots, e_r$ such that

(i) $V = Z(\alpha_1; T) \oplus \ldots \oplus Z(\alpha_r; T)$;

(ii) if $1 \leq k \leq r - 1$, then e_{k+1} divides e_k;

(iii) $Z(\alpha_j; T)$ is orthogonal to $Z(\alpha_k; T)$ when $j \neq k$. Furthermore, the integer r and the annihilators $e_1, \ldots, e_r$ are uniquely determined by conditions (i) and (ii) and the fact that no α_k is 0.

Corollary: If A is a normal matrix with real (complex) entries, then there is a real orthogonal (unitary) matrix P such that $P^{-1}AP$ is in rational canonical form.

It follows that two normal matrices A and B are unitarily equivalent if and only if they have the same rational form; A and B are orthogonally equivalent if they have real entries and the same rational form.

On the other hand, there is a simpler criterion for the unitary equivalence of normal matrices and normal operators.

Definition: Let V and V' be inner product spaces over the same field. A linear transformation

$$U : V \to V'$$

is called a **unitary transformation** if it maps V onto V' and preserves inner products. If T is a linear operator on V and T' a linear operator on V', then T is unitarily equivalent to T' if there exists a unitary transformation U of V onto V' such that

$$UTU^{-1} = T'.$$

Lemma: Let V and V' be finite-dimensional inner product spaces over the same field. Suppose T is a linear operator on V and that T' is a linear operator on V'. Then T is unitarily equivalent to T' if and only if there is an orthonormal basis $\mathcal{B}$ of V and an orthonormal basis $\mathcal{B}'$ of V' such that

$$[T]_{\mathcal{B}} = [T']_{\mathcal{B}'}.$$

Proof: Suppose there is a unitary transformation U of V onto V' such that $UTU^{-1} = T'$. Let $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$ be any (ordered) orthonormal basis for V. Let $\alpha'_j = U\alpha_j$ $(1 \leq j \leq n)$. Then $\mathcal{B}' = \{\alpha'_1, \ldots, \alpha'_n\}$ is an orthonormal basis for V' and setting

$$T\alpha_j = \sum_{k=1}^{n} A_{kj}\alpha_k$$

we see that

$$T'\alpha'_j = UT\alpha_j$$

$$= \sum_k A_{kj} U\alpha_k$$

$$= \sum_k A_{kj}\alpha'_k$$

Hence $[T]_{\mathcal{B}} = A = [T']_{\mathcal{B}'}$.

Conversely, suppose there is an orthonormal basis $\mathcal{B}$ of V and an orthonormal basis $\mathcal{B}'$ of V' such that

$$[T]_{\mathcal{B}} = \{T'\}_{\mathcal{B}'}$$

and let $A = [T]_{\mathcal{B}}$. Suppose $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$ and that $\mathcal{B}' = \{\alpha'_1, \ldots, \alpha'_n\}$. Let U be the linear transformation of V into V' such that $U\alpha_j = \alpha'_j$ $(1 \le j \le n)$. Then U is a unitary transformation of V onto V', and

$$UTU^{-1}\alpha'_j = UT\alpha_j$$

$$= U\sum_k A_{kj}\alpha_k$$

$$= \sum_k A_{kj}\alpha'_k\ .$$

Therefore, $UTU^{-1}\alpha'_j = T'\alpha'_j$ $(1 \le j \le n)$, and this implies $UTU^{-1} = T'$.

It follows immediately from the lemma that unitarily equivalent operators on finite-dimensional spaces have the same characteristic polynomial. For normal operators the converse is valid.

Theorem 13: Let V and V' be finite-dimensional inner product spaces over the same field. Suppose T is a normal operator on V and that T' is a normal operator on V'. Then T is unitarily equivalent to T' if and only if T and T' have the same characteristic polynomial.

Proof: Suppose T and T' have the same characteristic polynomial f. Let W_j $(1 \le j \le k)$ be the primary components of V under T and T_j the restriction of T to W_j. Suppose I_j is the identity operator on W_j. Then

$$f = \prod_{j=1}^{k} \det(xI_3 - T_j)$$

Let p_j be the minimal polynomial for T_j. If $p_j = x - c_j$ it is clear that

$$\det(xI_j - T_j) = (x - c_j)^{sj}$$

where s_j is the dimension of W_j. On the other hand, if $p_j = (x - a_j)^2 + b_j^2$ with a_j, b_j real and $b_j \neq 0$, then it follows from Theorem 10 that

$$\det(xI_j - T_j) = p_j^{sj}$$

where in this case $2s_j$ is the dimension of W_j. Therefore $f = \prod_j p_j^{s_j}$. Now we can also compute f by the same method using the primary components of V' under t'. Since $p_1, \ldots, p_k$ are distinct primes, if follows from the uniqueness of the prime factorization of f that there are exactly k primary components W'_j $(1 \le j \le k)$ of V' under T' and that these may be indexed in such a way that p_j is the minimal polynomial for the restriction T'_j of T' to W'_j. If $p_j = x - c_j$, then $T_j = c_j I_j$ and $T'_j = c_j I'_j$ where I'_j is the identity operator on W'_j. In this case it is evident that T_j is unitarily equivalent to T'_j. If $p_j = (x - a_j)^2 + b_j^2$ as above, then using the lemma and theorem 12, we again see that T_j is unitarily equivalent to T'_j. Thus for each j there are orthonormal bases B_j and B'_j of W_j and W'_j, respectively such that

$$[T_j]_{B_j} = [T'_j]_{B'_j}.$$

Now let U be the linear transformation of V into V' that maps each B_j onto B'_j. Then U is a unitary transformation of V onto V' such that $UTU^{-1} = T'$.

Self Assessment

1. If U and T are normal operators which commute, prove that $U + T$ and UT are normal.
2. Let A be an $n \times n$ matrix with complex entries such that $A^* = -A$ and let $B = e^A$. Show that
   (a) $\det B = e^{\operatorname{tr} A}$;
   (b) $B^* = e^{-A}$;
   (c) B is unitary.
3. For

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{bmatrix}$$

   there is a real orthogonal matrix p such that $P^{-1}AP = D$ is diagonal. Find such a diagonal matrix D.

9.3 Summary

- The properties of unitary operators, normal operators or self-adjoint operators are studied further. This study is an improvement of the results of unit 26.
- It is seen that a diagonalizable normal operator T on a finite dimensional inner product space is either a self-adjoint, non-negative or unitary according as each characteristic value of T is real, non-negative or of absolute value 1.
- If A is a normal matrix with real (complex) entries, then there is a real orthogonal (unitary) matrix P such that $P^{-1}AP$ is in rational canonical form.

9.4 Keywords

A Unitary Transformation: Let V and V' be inner product spaces over the same field. A linear transformation $U: V \to V'$ is called a unitary transformation if it preserves inner product.

Polar Decomposition: We call $T = UN$ a polar decomposition for T on a finite dimensional inner product space where U is a unitary operator and a unique non-negative linear operator on V.

The Non-negative: The non-negative operator T on an inner product space is self-adjoint and $(T\alpha | \alpha) \geq 0$ for every α in V.

The Spectral Resolution: The decomposition of the linear operator T as the sum of orthogonal projections, i.e.

$$T = \sum_{i=1}^{k} C_i E_i.$$

9.5 Review Questions

1. If T is a normal operator, prove that characteristic vectors for T which are associated with distinct characteristic values are orthogonal.

2. Let T be a linear operator on the finite dimensional complex inner product space V. Prove that the following statements about T are equivalent.

   (a) T is normal

   (b) $\| T\alpha \| = \| T^*\alpha \|$ for every α in V

   (c) If α is a vector and c a scalar such that $T\alpha = c\alpha$, then $T^*\alpha = \bar{c}\,\alpha$.

   (d) There is an orthonormal basis β such that $[T]_\beta$ is diagonal.

Answer: Self Assessment

3. $D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{9-\sqrt{57}}{2} & 0 \\ 0 & 0 & \frac{9+57}{2} \end{bmatrix}$

9.6 Further Readings

Books Kenneth Hoffman and Ray Kunze, *Linear Algebra*

Michael Artin, *Algebra*

Unit 10: Bilinear Forms and Symmetric Bilinear Forms

Notes

CONTENTS

Objectives

Introduction

10.1 Bilinear Forms

10.2 Symmetric Bilinear Forms

10.3 Summary

10.4 Keywords

10.5 Review Questions

10.6 Further Readings

Objectives

After studying this unit, you will be able to:

- Understand that the bilinear forms and inner products discussed in earlier units have a strong relation.
- See the isomorphism between the space of bilinear forms and the space of $n \times n$ matrices is established.
- Know that the linear transformations from V into V^* defined by $(L_f\alpha)(\beta) = f(\alpha, \beta) = (R_f\beta)(\alpha)$ (where f is a bilinear form) are such that rank (L_f) = rank (R_f).

Introduction

In this unit we are interested in studying a bilinear form f on a finite vector space of dimension n.

With the help of a number of examples it is shown how to get various forms of bilinear forms including linear functionals, bilinear forms involving $n \times 1$ matrices.

It is also established that the rank of a bilinear form is equal to the rank of the matrix of the form in any ordered basis.

10.1 Bilinear Forms

In this unit we treat bilinear forms on finite dimensional vector spaces. There are a few similarities between the bilinear forms and the inner product spaces. Let V be a real inner product space and suppose that A is a real symmetric linear transformation on V. The real valued function $f(v)$ defined on V by $f(v) = (v, A, v)$ can also be called the quadratic form i.e. bilinear form associated with A. If we assume A to be a real, $n \times n$ symmetric matrix (a_{ij}) acting on $F^{(n)}$ and for an arbitrary vector $v = (x_1, x_2 ..., x_n)$ in $F^{(n)}$, then

$$f(v) = (v, A, v) = a_{11}x_1^2 + a_{22}x_2^2 + ... + a_{nn}x_n^2 + 2\sum_{iLj} a_{ij}x_jx_j$$

In real n-dimensional Euclidean space such quadratic functions serve to define the quadratic surfaces.

Let us formally define the Bilinear form as follows:

A Bilinear Form: Let V be a vector space over the field F, a bilinear form is a function f, which assigns to each ordered pair of vectors α, β in V a scalar $f(\alpha, \beta)$ in F, and which satisfies

$$\left.\begin{aligned} f(c\alpha_1 + \alpha_2, \beta) &= cf(\alpha_1, \beta) + f(\alpha_2, \beta) \\ f(\alpha_1 + c\beta_1, \beta_2) &= cf(\alpha_1, \beta_1) + f(\alpha_2, \beta_2) \end{aligned}\right\} \quad \text{...(1)}$$

Thus a bilinear form on V is a function f from $V \times V$ into F which is linear as a function of either of its arguments when the other is fixed. The zero function from $V \times V$ into F is clearly a bilinear form. Also any linear combination of bilinear forms on V is again a bilinear form is f and g are bilinear on V, so is $cf + g$ where c is a scalar in F. So we may conclude that the set of all bilinear forms on V is a subspace of the space of all functions from $V \times V'$ into F. Let us denote the space of bilinear forms on V by $L(V, V, F)$.

Example 1: Let m, n be positive integers and F a field. Let V be the vector space of all $m \times n$ matrices over F. Let A be a fixed $m \times m$ matrix over F. Define

$$f_A(X, Y) = \text{tr}\,(X^*AY)$$

then f_A is a bilinear form on V. For, if x, y, z are $m \times n$ matrices over F,

$$\begin{aligned} f_A(CX, Z, Y) &= \text{tr}\,[(CX + Z)^+ AY] \\ &= \text{tr}\,[cX^tAY] + \text{tr}\,[Z^tAY] \\ &= cf_A(X, Y) + f_A(Z, Y) \end{aligned}$$

If we take $n = 1$, we have

$$f_A(X, Y) = X^tAY + \sum_i \sum_j A_{ij}x_iy_j$$

So every bilinear form f_A for some A is of this form on a space of $m \times 1$.

Example 2: Let F be a field. Let us find all bilinear forms on the space F^2. Suppose f is such a bilinear form. If $\alpha = (x_1, x_2)$ and $\beta = (y_1, y_2)$ are vectors in F^2, then

$$\begin{aligned} f(\alpha, \beta) &= f(x_1\varepsilon_1 + x_2\varepsilon_2, \beta) \\ &= x_1f(\varepsilon_1, \beta) + x_2f(\varepsilon_2, \beta) \\ &= x_1f(\varepsilon_1, y_1\varepsilon_1 + y_2\varepsilon_2) + x_2f(\varepsilon_2, y_1\varepsilon_1 + y_2\varepsilon_2) \\ &= x_1y_1f(\varepsilon_1, \varepsilon_1) + x_1y_2f(\varepsilon_1, \varepsilon_2) + x_2y_1f(\varepsilon_2, \varepsilon_1) + x_2y_2f(\varepsilon_2, \varepsilon_2). \end{aligned}$$

Thus f is completely determined by the four scalars $A_{ij} = f(\varepsilon_i, \varepsilon_j)$ by

$$\begin{aligned} f(\alpha, \beta) &= A_{11}x_1y_1 + A_{12}x_1y_2 + A_{21}x_2y_1 + A_{22}x_2y_2 \\ &= \sum_{i,j} A_{ij}x_iy_j \end{aligned}$$

If X and Y are the coordinate matrices of α and β, and if A is the 2×2 matrix with entries $A(i, j) = A_{ij} = f(\varepsilon_i, \varepsilon_j)$, then

$$f(\alpha, \beta) = X^tAY. \quad \text{... (2)}$$

We observed in Example 1 that if A is any 2×2 matrix over F, then (2) defines a bilinear form on F^2. We see that the bilinear forms on F^2 are precisely those obtained from a 2×2 matrix as in (2).

The discussion in Example 2 can be generalized so as to describe all bilinear forms on a finite-dimensional vector space. Let V be a finite-dimensional vector space over the field F and let $\beta = \{\alpha_1, ..., \alpha_n\}$ be an ordered basis for V. Suppose f is a bilinear form on V. If

$$\alpha = x_1\alpha_1 + ... + x_n\alpha_n \quad \text{and} \quad \beta = y_1\alpha_1 + ... + y_n\alpha_n$$

are vectors in V, then

$$\begin{aligned} f(\alpha, \beta) &= f\left(\sum_i x_i\alpha_i, \beta\right) \\ &= \sum_i x_i f(\alpha_i, \beta) \\ &= \sum_i x_i f\left(\alpha_i, \sum_j y_j a_j\right) \\ &= \sum_i \sum_i x_i\, y_i f(\alpha_i, \alpha_j) \end{aligned}$$

If we let $A_{ij} = f(\alpha_i, \alpha_j)$, then

$$\begin{aligned} f(\alpha, \beta) &= \sum_i \sum_i A_{ij} x_i y_i \\ &= X^t A Y \end{aligned}$$

where X and Y are the coordinate matrices of α and β in the ordered basis β. Thus every bilinear form on V is of the type

$$f(\alpha, \beta) = [\alpha]^t_\beta A[\beta]_\beta \qquad \text{… (3)}$$

for some $n \times n$ matrix A over F. Conversely, if we are given any $n \times n$ matrix A, it is easy to see that (3) defines a bilinear form f on V, such that $A_{ij} = f(\alpha_i, \alpha_j)$.

Definition: Let V be a finite-dimensional vector space, and let $\beta = \{\alpha_1, ..., \alpha_n\}$ be an ordered basis for V. If f is a bilinear form on V, the matrix of f in the ordered basis β is the $n \times n$ matrix A with entries $A_{ij} = f(\alpha_i, \alpha_j)$. At times, we shall denote this matrix by $[f]_\beta$.

Theorem 1: Let V be a finite-dimensional vector space over the field F. For each ordered basis β of V, the function which associates with each bilinear form on V its matrix in the ordered basis β is an isomorphism of the space $L(V, V, F)$ onto the space of $n \times n$ matrices over the field F.

Proof: We observed above that $f \rightarrow [f]_\beta$ is a one-one correspondence between the set of bilinear forms on V and the set of all $n \times n$ matrices over F. That this is linear transformation is easy to see, because

$$(cf + g)\,(\alpha_i, \alpha_j) = cf(\alpha_i, \alpha_j) + g(\alpha_i, \alpha_j)$$

for each i and j. This simply says that

$$[cf + g]_\beta = c[f]_\beta + [g]_\beta.$$

Corollary: If $\beta = \{\alpha_1, ..., \alpha_n\}$ is an ordered basis of V, and $\beta^* = \{L_1, ... L_n\}$ is the dual basis for V^*, then the n^2 bilinear forms

$$f_{ij}(\alpha, \beta) = L_i(\alpha)\, L_j(\beta), \quad 1 \le i \le n, 1 \le j \le n$$

form a basis for the space $L(V, V, F)$. In particular, the dimension of $L(V, V, F)$ is n^2.

Proof: The dual basis $\{L_1, ... L_n\}$ is essentially defined by the fact that $L_i(\alpha)$ is the ith coordinate of α in the ordered basis β (for any α in V).

Notes

Now the functions f_{ij} defined by

$$f_{ij}(\alpha, \beta) = L_i(\alpha)L_j(\beta)$$

are bilinear forms. If

$$\alpha = x_1\alpha_1 + ... + x_n\alpha_n \quad \text{and} \quad \beta = y_1\alpha_1 + ... + y_n\alpha_n$$

then

$$f_{ij}(\alpha, \beta) = x_i y_j$$

Let f be any bilinear form on V and let A be the matrix of f in the ordered basis β. Then

$$f(\alpha, \beta) = \sum_{i, j} A_{ij} x_i y_j$$

which simply says that

$$f = \sum_{i, j} A_{ij} f_{ij}$$

It is now clear that the n^2 forms f_{ij} comprise a basis for $L(V, V, F)$.

One can rephrase the proof of the corollary as follows. The bilinear from f_{ij} has as its matrix in the ordered basis β the matrix 'unit' $E^{i,j}$, whose only non-zero entry is a 1 in now i and column j. Since these matrix units comprise a basis for the space of $n \times n$ matrices, the forms f_{ij} comprise a basis for the space of bilinear forms.

The concept of the matrix of a bilinear form in an ordered basis is similar to that of the matrix of a linear operator in an ordered basis. Just as for linear operators, we shall be interested in what happens to the matrix representing a bilinear form, as we change from one ordered basis to another. So, suppose $\beta = \{\alpha_1, ... \alpha_n\}$ and $\beta' = \{\alpha'_1, ..., \alpha'_n\}$ are two ordered bases for V and that f is a bilinear form on V. How are the matrices $[f]_\beta$ and $[f]_{\beta'}$ related? Well, let P be the (invertible) $n \times n$ matrix such that

$$[\alpha]_\beta = P[\alpha]_{\beta'}$$

for all α in V. In other words, define P by

$$\alpha'_j = \sum_{i=1}^{n} P_{ij}\alpha_i$$

For any vectors α, β in V

$$\begin{aligned} f(\alpha, \beta) &= [\alpha]^t_{\beta'} [f]_{\beta'} [\beta]_\beta \\ &= (P[\alpha]_{\beta'})^t [f]_\beta P[\beta]_{\beta'} \\ &= [\alpha]^t_{\beta'} (P^t[f]_\beta P)[\beta]_{\beta'}. \end{aligned}$$

By the definition and uniqueness of the matrix representing f in the ordered basis β′, we must have

$$[f]_{\beta'} = P^t[f]_\beta P. \qquad ...(4)$$

Example 3: Let V be the vector space R^2. Let f be the bilinear form defined on $\alpha = (x_1, x_2)$ and $\beta = (y_1, y_2)$ by

$$f(\alpha, \beta) = x_1y_1 + x_1y_2 + x_2y_1 + x_2y_2$$

Now

$$f(\alpha, \beta) = [x_1, x_2]\begin{bmatrix}1 & 1\\1 & 1\end{bmatrix}\begin{bmatrix}y_1\\y_2\end{bmatrix}$$

and so the matrix of f in the standard ordered basis $\beta = \{\varepsilon_1, \varepsilon_2\}$ is

$$[f]_\beta = \begin{bmatrix}1 & 1\\1 & 1\end{bmatrix}$$

Let $\beta' = \{\varepsilon'_1, \varepsilon'_2\}$ be the ordered basis defined by $\varepsilon'_1 = (1, -1)$, $\varepsilon'_2 = (1, 1)$. In this case, the matrix P which changes coordinates from β' to β is

$$P = \begin{bmatrix}1 & 1\\-1 & 1\end{bmatrix}$$

Thus

$$\begin{aligned}[f]_{\beta'} &= P^t[f]_\beta P\\ &= \begin{bmatrix}1 & -1\\1 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\1 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\-1 & 1\end{bmatrix}\\ &= \begin{bmatrix}1 & -1\\1 & 1\end{bmatrix}\begin{bmatrix}0 & 2\\0 & 2\end{bmatrix}\\ &= \begin{bmatrix}0 & 0\\0 & 4\end{bmatrix}\end{aligned}$$

What this means is that if we express the vectors α and β by means of their coordinates in the basis β', say

$$\alpha = x'_1\varepsilon'_1 + x'_2\varepsilon'_2, \quad \beta = y'_1\varepsilon'_1 + x'_2\varepsilon'_2$$

then

$$f(\alpha, \beta) = 4x'_2y'_2$$

One consequence of the change of basis formula (4) is the following: If A and B are $n \times n$ matrices which represent the same bilinear form on V in (possibly) different ordered bases, then A and B have the same rank. For, if P is an invertible $n \times n$ matrix and $B = P^tAP$, it is evident that A and B have the same rank. This makes it possible to define the rank of a bilinear form on V as the rank of any matrix which represents the form in an ordered basis for V.

It is desirable to give a more intrinsic definition of the rank of a bilinear form. This can be done as follows: Suppose F is a bilinear form on the vector space V. If we fix a vector α in V, then $f(\alpha, \beta)$ is linear as a function of β. In this way, each fixed α determines a linear functional on V; let us denote this linear functional by $L_f(\alpha)$. To repeat, if α is a vector in V, then $L_f(\alpha)$ is the linear functional on V whose value on any vector β is $f(\alpha, \beta)$. This gives us a transformation $\alpha \to L_f(\alpha)$ form V into the dual space V^*. Since

$$f(c\alpha_1, + \alpha_2, \beta) = cf(\alpha_1, \beta) + f(\alpha_2, \beta)$$

we see that

$$L_f(c\alpha_1, + \alpha_2) = cL_f(\alpha_1) + L_f(\alpha_2)$$

that is L_f is a linear transformation from V into V^*.

In a similar manner, f determines a linear transformation R_f from V into V^*. For each fixed β in V, $f(\alpha, \beta)$ is linear as a function of α. We define $R_f(\beta)$ to be the linear functional on V whose value on the vector α is $f(\alpha, \beta)$.

Theorem 2: Let f be a bilinear form on the finite-dimensional vector space V. Let L_f and R_f be a linear transformation from V into V^* defined by $(L_f\alpha)(\beta) = f(\alpha, \beta) = (R_f\beta)(\alpha)$. Then rank (L_f) = rank (R_f).

Proof: One can give a 'coordinate free' proof of this theorem. Such a proof is similar to the proof that the row-rank of a matrix is equal to its column-rank. Some here we shall give a proof which proceeds by choosing a coordinate system (basis) and then using the 'row-rank equals column-rank' theorem.

To prove rank (L_f) = rank (R_f), it will suffice to prove that L_f and R_f have the same nullity. Let β be an ordered basis for V, and let $A = [f]_\beta$. If α and β are vectors in V, with coordinate matrices X and Y in the ordered basis β, then $f(\alpha, \beta) = X^tAY$. Now $R_f(\beta) = 0$ means that $f(\alpha, \beta) = 0$ for every α in V, i.e., that $X^tAY = 0$ for every $n \times 1$ matrix X. The latter condition simply says that $AY = 0$. The nullity of R_f is therefore equal to the dimension of the space of solutions of $AY = 0$.

Similarly, $L_f(\alpha) = 0$ if and only if $X^tAY = 0$ for every $n \times 1$ matrix Y. Thus α is in the null space of L_f if and only if $X^tA = 0$, i.e. $A^tX = 0$. The nullity of L_f is therefore equal to the dimension of the space of solutions of $A^tX = 0$. Since the matrices A and A^t have the same column-rank, we see that

$$\text{nullity } (L_f) = \text{nullity } (R_f).$$

Definition: If f is a bilinear form on the finite-dimensional space V, the rank of f is the integer r = rank (L_f) = rank (R_t).

Corollary 1: The rank of a bilinear form is equal to the rank of matrix of the form in any ordered basis.

Corollary 2: If f is a bilinear form on the n-dimensional vector space V, the following are equivalent:

(a) rank $(f) = n$

(b) For each non-zero α in V, there is α β in V such that $f(\alpha, \beta) \neq 0$.

(c) For each non-zero β in V, there is an α in V such that $f(\alpha, \beta) \neq 0$.

Proof: Statement (b) simply says that the null space of L_f is the zero subspace. Statement (c) says that the null space of R_f is the zero subspace. The linear transformations L_f and R_f have nullity 0 if and only if they have rank n, i.e., if and only if rank $(f) = n$.

Definition: A bilinear form f on a vector space V is called non-degenerate (or non-singular) if it satisfies conditions (b) and (c) of Corollary 2.

If V is finite-dimensional, then f is non-degenerate provided f satisfies any one of the three conditions of Corollary 2. In particular, f is non-degenerate (non-singular) if and only if its matrix in some (every) ordered basis for V is a non-singular matrix.

Example 4: Let $V = R^n$, and let f be the bilinear form defined on $\alpha = (x_1, ..., x_n)$ and $\beta = (y_1 ..., y_n)$ by

$$f(\alpha, \beta) = x_1y_1 + ... + x_ny_n.$$

Then f is a non-degenerate bilinear form on R^n. The matrix of f in the standard basis is the $n \times n$ identity matrix.

$$f(x, y) = X^tY.$$

Self Assessment

1. Which of the following functions f, defined on vectors $\alpha = (x_1, x_2)$ and $\beta(y_1, y_2)$ in R^2, are bilinear forms?

   (a) $f(\alpha, \beta) = (x_1 - y_1)^2 + x_2 y_2$

   (b) $f(\alpha, \beta) = (x_1 + y_1)^2 + (x_1 - y_1)^2$

   (c) $f(\alpha, \beta) = x_1 y_2 - x_2 y_1$

2. Let f be any bilinear form on a finite-dimensional space V. Let W be the subspace of all β such that $f(\alpha, \beta) = 0$ for every α. Show that

$$\text{rank } f = \dim V - \dim W.$$

10.2 Symmetric Bilinear Forms

In dealing with a bilinear form sometimes it is asked when is there an ordered basis β for V in which f is represented by a diagonal matrix. It will be seen in this part of the unit that if f is a symmetric bilinear form, i.e., $f(\alpha, \beta) = f(\beta, \alpha)$ then f will be represented by a diagonal matrix in an ordered basis of the space V.

If V is a finite-dimensional, the bilinear form f is symmetric if and only if the matrix A in some ordered basis is symmetric, $A^t = A$.

To see this, one enquires when the bilinear form

$$f(X, Y) = X^t A Y$$

is symmetric.

This happens if and only if $X^t A Y = Y^t A X$ for all column matrices X and Y. Since $X^t A Y$ is a 1×1 matrix, we have $X^t A Y = Y^t A^t X$. Thus f is symmetric if and only if $Y^t A^t X = Y^t A X$ for all X, Y. Clearly this just means that $A = A^t$. In particular, one should note that if there is an ordered basis for V in which f is represented by a diagonal matrix, then f is symmetric, for any diagonal matrix is a symmetric matrix.

If f is a symmetric bilinear form, the quadratic form associated with f is the function q from V into F defined by

$$q(\alpha) = f(\alpha, \alpha)$$

If F is a subfield of the complex numbers, the symmetric bilinear form f is completely determined by its associated quadratic form, according to the polarization identity

$$f(\alpha, \beta) = \frac{1}{4} q(\alpha + \beta) - \frac{1}{4} q(\alpha - \beta) \qquad ...(5)$$

If f is the bilinear form of Example 4, the dot product, the associated quadratic form is

$$q(x_1, \ldots x_n) = x_1^2 + \ldots + x_n^2$$

In other words, $q(\alpha)$ is the square of the length of α. For the bilinear form $f_A(X, Y) = X^t A Y$, the associated quadratic form is

$$q_A(X) = X^t A X = \sum_{i,j} A_{ij} x_i x_j$$

One important class of symmetric bilinear forms consists of the inner products on real vector spaces discussed earlier. If V is a real vector space, an inner product on V is a symmetric bilinear form f on V which satisfies

$$f(\alpha, \alpha) > 0 \text{ if } \alpha \neq 0. \qquad ...(6)$$

A bilinear form satisfying (6) is called positive definite. Thus, an inner product on a real vector space is a positive definite, symmetric bilinear form on that space. Note that an inner product is non-degenerate. Two vectors α, β are called orthogonal with respect to the inner product f if $f(\alpha, \beta) = 0$. The quadratic form $q(\alpha) = f(\alpha, \alpha)$ takes only non-negative values, and $q(\alpha)$ is usually thought of as the square of the length of α. Of course, these concepts of length and orthogonality stem from the most important example of an inner product – the dot product.

If f is any symmetric bilinear form on a vector space V, it is convenient to apply some of the terminology of inner products to f. It is especially convenient to say that α and β are orthogonal with respect to f if $f(\alpha, \beta) = 0$. It is not advisable to think of $f(\alpha, \alpha)$ as the square of the length of α; for example if V is a complex vector space, we may have $f(\alpha, \alpha) = \sqrt{-1}$ or on a real vector space, $f(\alpha, \alpha) = -2$.

Theorem 3: Let V be n finite-dimensional vector space over a field of characteristic zero, i.e. if n is a positive integer the sum 1 + 1 + ... + 1 (n times) in F is not zero, and let f be a symmetric bilinear form on V. Then there is an ordered basis for V in which f is represented by a diagonal matrix.

Proof: What we must find is an ordered basis

$$\beta = \{\alpha_1, ..., \alpha_n\}$$

such that $f(\alpha_i, \alpha_j) = 0$ for $i \neq j$. If $f = 0$ or $n = 1$, the theorem is obviously true. Thus we may suppose $f \neq 0$ and $n > 1$. If $f(\alpha, \alpha) = 0$ for every α in V, the associated quadratic form q is identically 0, and the polarization identity (5) shows that $f = 0$. Thus there is a vector α in V such that $f(\alpha, \alpha) = q(\alpha) \neq 0$. Let W be the one-dimensional subspace of V which is spanned by α, and let $W^{\perp}$ be the set of all vectors β in V such that $f(\alpha, \beta) = 0$. Now we claim that $V = W \oplus W^{\perp}$. Certainly the subspaces W and $W^{\perp}$ are independent. A typical vector in W is $c\alpha$, where c is a scalar. If $c\alpha$ is also in $W^{\perp}$, then $f(c\alpha, c\alpha) = c^2 f(\alpha, \alpha) = 0$. But $f(\alpha, \alpha) \neq 0$, thus $c = 0$. Also, each vector in V is the sum of a vector in W and a vector in $W^{\perp}$. For, Let γ be any vector in V, and put

$$\beta = \gamma - \frac{f(\gamma, \alpha)}{f(\alpha, \alpha)} \alpha.$$

Then

$$\beta(\alpha, \beta) = f(\alpha, \gamma) - \frac{f(\gamma, \alpha)}{f(\alpha, \alpha)} f(\alpha, \alpha)$$

and since f is symmetric, $f(\alpha, \beta) = 0$. Thus β is in the subspace $W^{\perp}$. The expression

$$\gamma = \frac{f(\gamma, \alpha)}{f(\alpha, \alpha)} \alpha + \beta$$

shows us that $V = W + W^{\perp}$.

The restriction of f to $W^{\perp}$ is a symmetric bilinear form on $W^{\perp}$. Since $W^{\perp}$ has dimension $(n - 1)$, we may assume by induction that $W^{\perp}$ has a basis $\{\alpha_2, ..., \alpha_n\}$ such that

$$f(\alpha_i, \alpha_j) = 0, \quad i \neq j \ (i, \geq 2, j \geq 2)$$

Putting $\alpha_1 = \alpha$, we obtain a basis $\{\alpha_1, ..., \alpha_n\}$ for V such that $f(\alpha_i, \alpha_j) = 0$ for $i \neq j$.

Corollary: Let F be a subfield of the complex numbers, and let A be a symmetric $n \times n$ matrix over F. Then there is an invertible $n \times n$ matrix P over F such that P^tAP is diagonal.

In case F is the field of real numbers, the invertible matrix P in this corollary can be chosen to be an orthogonal matrix, i.e., $P^t = P^{-1}$. In other words, if A is a real symmetric $n \times n$ matrix, there is a real orthogonal matrix P such that P^tAP is diagonal.

Theorem 4: Let V be a finite-dimensional vector space over the field of complex numbers. Let f be a symmetric bilinear form on V which has rank r. Then there is an ordered basis $\beta = \{\beta_1, ..., \beta_n\}$ for V such that

(i) the matrix of f in the ordered basis β is diagonal

(ii) $f(\beta_j, \beta_j) = \begin{cases} 1, & j = 1, ..., r \\ 0, & j > r. \end{cases}$

Proof: By Theorem 3, there is an ordered basis $(\alpha_1, ..., \alpha_n)$ for V such that

$$f(\alpha_i, \alpha_j) = 0 \quad \text{for} \quad i \neq j.$$

Since f has rank r, so does its matrix is the ordered basis $\{\alpha_1, ... , \alpha_n\}$. Thus we must have $f(\alpha_j, \alpha_j) \neq 0$ for precisely r values of j. By reordering the vectors α_j, we may assume that

$$f(\alpha_j, \alpha_j) \neq 0, \quad j = 1, ..., r.$$

Now we use the fact that the scalar field is the field of complex numbers. If $\sqrt{f(\alpha_j, \alpha_j)}$ denotes any complex square root of $f(\alpha_j, \alpha_j)$, and if we put

$$\beta_j = \begin{cases} \dfrac{1}{\sqrt{f(\alpha_j, \alpha_j)}}\alpha_j, & j = 1, ..., r \\ \alpha_j, \; j > r \end{cases}$$

the basis $\{\beta_1, ..., \beta_n\}$ satisfies conditions (i) and (ii).

Of course, Theorem 4 is valid if the scalar field is any subfield of the complex numbers in which each element has a square root. It is not valid, for example, when the scalar field is the field of real numbers. Over the field of real numbers, we have the following substitute for Theorem 4.

Theorem 5: Let V an n-dimensional vector space over the field of real numbers, and let f be a symmetric bilinear form on V which has rank r. Then there is an ordered basis $\{\beta_1, \beta_2, ..., \beta_n\}$ for V in which the matrix of f is diagonal and such that

$$f(\beta_j, \alpha_j) = \pm 1, \quad j = 1, ... r.$$

Furthermore, the number of basis vectors β_j for $f(\beta_j, \beta_j) = 1$ is independent of the choice of basis.

Proof: There is a basis $\{\alpha_1, ..., \alpha_n\}$ for V such that

$$f(\alpha_i, \alpha_j) = 0, \quad i \neq j$$

$$f(\alpha_j, \alpha_j) \neq 0, \quad 1 \leq j \leq r$$

$$f(\alpha_j, \alpha_j) = 0, \quad j > r.$$

Let

$$\beta_j = |f(\alpha_j, \alpha_j)|^{-1/2} \alpha_j, \quad 1 \leq j \leq r$$

$$\beta_j = \alpha_j, \quad j > r.$$

Then $(\beta_1, ..., \beta_n)$ is a basis with the stated properties.

Notes

Let p be the number of basis vectors, β_j for which $f(\beta_j, \beta_j) = 1$; we must show that the number p is independent of the particular basis we have, satisfying the stated conditions. Let V^+ be the subspace of V spanned by the basis vectors β_j for which $f(\beta_j, \beta_j) = 1$, and let V' be the subspace spanned by the basis vectors β_j for which $f(\beta_j, \beta_j) = -1$. Now $p = \dim V^+$, so it is the uniqueness of the dimension of V^+ which we must demonstrate. It is easy to see that if α is a non-zero vector in V^+ then $f(\alpha, \alpha) > 0$; in other words, f is positive definite on the subspace V^+. Similarly, if α is a non-zero vector in V^-, then $f(\alpha, \alpha) < 0$, i.e., f is negative definite on the subspace V^-. Now let $V^\perp$ be the subspace spanned by the basis vectors β_j for which $f(\beta_j, \beta_j) = 0$. If α is in $V^\perp$, then $f(\alpha, \beta) = 0$ for all β in V.

Since $\{\beta_1, ..., \beta_n\}$ is a basis for V, we have

$$V = V^+ \oplus V^- \oplus V^\perp.$$

Furthermore, we claim that if W is any subspace of V on which f is positive definite, then the subspaces W, V^-, and $V^\perp$ are independent. For, suppose α is in W, β is in V^-, γ is in $V^\perp$, and $\alpha + \beta + \gamma = 0$. Then

$$0 = f(\alpha, \alpha + \beta + \gamma) = f(\alpha, \alpha) + f(\alpha, \beta) + f(\alpha, \gamma)$$

$$0 = f(\beta, \alpha + \beta + \gamma) = f(\beta, \alpha) + f(\beta, \beta) + f(\beta, \gamma)$$

Since γ is in $V^\perp$, $f(\alpha, \gamma) = f(\beta, \gamma) = 0$; and since f is symmetric, we obtain

$$0 = f(\alpha, \beta) + f(\alpha, \beta)$$

$$0 = f(\beta, \beta) + f(\alpha, \beta)$$

hence $f(\alpha, \alpha) = f(\beta, \beta)$. Since $f(\alpha, \alpha) \geq 0$ and $f(\beta, \beta) \leq 0$, it follows that

$$f(\alpha, \alpha) = f(\beta, \beta) = 0$$

But f is positive definite on W and negative definite on V^-. We conclude that $\alpha = \beta = 0$, and hence that $\gamma = 0$ as well.

Since

$$V = V^+ \oplus V^- \oplus V^\perp$$

and W, V^-, $V^\perp$ are independent, we see that $\dim W \leq \dim V^+$. That is, if W is any subspace of V on which f is positive definite, the dimension of W cannot exceed the dimension of V^+. If β_1 is another ordered basis for V which satisfies the conditions of the theorem, we shall have corresponding subspaces V_1^+, V_1^-, and $V_1^\perp$ and, the argument above shows that $\dim V_1^+ \leq \dim V^+$. Reversing the argument, we obtain $\dim V^+ \leq \dim V_1^+$, and consequently

$$\dim V^+ = \dim V_1^+.$$

There are several comments we should make about the basis $(\beta_1, ..., \beta_n\}$ of Theorem 5 and the associated subspaces V^+, V^-, and $V^\perp$ First, note that $V^\perp$ is exactly the subspace of vectors which are 'orthogonal' to all of V. We noted above that $V^\perp$ is contained in this subspace; but,

$$\dim V^\perp = \dim V - (\dim V^+ + \dim V^-) = \dim V - \text{rank } f$$

so every vector a such that $f(\alpha, \beta) = 0$ for all β must be in $V^\perp$. Thus, the subspace $V^\perp$ is unique. The subspaces V^+ and V^- are not unique; however, their dimensions are unique. The proof of Theorem 5 shows us that $\dim V^+$ is the largest possible dimension of any subspace on which f is positive definite. Similarly, $\dim V^-$ is the largest dimension of any subspace on which f is negative definite.

Of course

$$\dim V^+ + \dim V^- = \text{rank } f.$$

The number

$$\dim V^+ - \dim V^-$$

is often called the signature of f. It is introduced because the dimensions of V^+ and V^- are easily determined from the rank of f and the signature of f.

Perhaps we should make one final comment about the relation of symmetric bilinear forms on real vector spaces to inner products. Suppose V is a finite-dimensional real vector space and that V_1, V_2, V_3 are subspaces of V such that

$$V = V_1 \oplus V_2 \oplus V_3$$

Suppose that f_1 is an inner product on V_1, and f_2 is an inner product on V_2. We can then define a symmetric bilinear form f on V as follows: If α, β are vectors in V, then we can write

$$\alpha = \alpha_1 + \alpha_2 + \alpha_3 \quad \text{and} \quad \beta = \beta_1 + \beta_2 + \beta_3$$

with α_j. and β_j in V_j. Let

$$f(\alpha, \beta) = f_1(\alpha_1 + \beta_1) - f_2(\alpha_2 + \beta_2)$$

The subspace $V^\perp$ for f will be V_3, V_1 is a suitable V^+ for f, and V_2 is a suitable V^-. One part of the statement of Theorem 5 is that every symmetric bilinear form on V arises in this way. The additional content of the theorem is that an inner product is represented in some ordered basis by the identity matrix.

Self Assessment

3. Let V be a finite-dimensional vector space over a subfield F of the complex numbers and let S be the set of all symmetric bilinear forms in V. Show that S is a subspace of $L(V, V, F)$.

4. The following expressions define quadratic forms q on R^2. Find the symmetric bilinear form f corresponding to each q.

   (a) ax_1^2

   (b) $x_1^2 + 9x_2^2$

   (c) bx_1x_2

10.3 Summary

- In this unit concept of bilinear form is introduced.
- It is seen that there a strong relation between bilinear forms and inner products.
- The isomorphism between the space of bilinear forms and the space of $n \times n$ matrices is established.
- The rank of a bilinear form is defined and non-degenerate bilinear forms are introduced.

10.4 Keywords

A Bilinear Form: A bilinear form on V is a function f, which assigns to each pair of vectors, α, β in V a scalar $f(\alpha, \beta)$ in F, and satisfies linear relations.

A non-degenerate bilinear form on a vector space V is a bilinear form if for each non-zero α in V, there is α β in V such that $f(\alpha, \beta) \neq 0$ as well as for each non-zero β in V, there is and α in V such that $f(\alpha, \beta) \neq 0$.

The polarization Identity helps in determining the symmetric bilinear form by its associated quadratic form.

10.5 Review Questions

1. Let V be a finite-dimensional vector space over a subfield F of the complex numbers, and let S be the set of all symmetric bilinear forms on V.

   (a) Show that S is a subspace of $L(V, V, F)$

   (b) Find Dim S'

2. Let q be the quadratic form on R^2 given by

   $q(x_1, x_2) = 2bx_1x_2$

   Find an invertible linear operator V on R^2 such that

   $(V^+q)(x_1, x_2) = 2bx_1^2 - 2bx_2^2$.

Answers: Self Assessment

1. (b) and (*c*)

4. (a) $f(\alpha, \beta) = ax_1y_1$

   (b) $f(\alpha, \beta) = x_1y_1 + 9x_2y_2$

   (c) $f(\alpha, \beta) = \dfrac{b}{2}(x_1y_2 + y_1x_2)$

   Here $\alpha = (x_1, x_2)$

   $\beta = (y_1, y_2)$

10.6 Further Readings

Books Kenneth Hoffman and Ray Kunze, *Linear Algebra*

Michael Artin, *Algebra*

Unit 11: Skew-symmetric Bilinear Forms

Notes

CONTENTS

Objectives

Introduction

11.1 Skew-symmetric Bilinear Forms

11.2 Summary

11.3 Keywords

11.4 Review Questions

11.5 Further Readings

Objectives

After studying this unit, you will be able to:

- See that skew-symmetric bilinear form is studied in a similar way as the symmetric bilinear form was studied.
- Know that here the quadratic form is given by the difference $h(\alpha, \beta) = \frac{1}{2}$ $[f(\alpha, \beta) - f[\beta, \alpha]]$
- Understand that the space $L(V, V, F)$ is the direct sum of the subspace of symmetric forms and the subspace of skew-symmetric forms.

Introduction

In this unit a bilinear form f on V called skew-symmetric form i.e. $f(\alpha, \beta) = -f(\beta, \alpha)$ is studied. Close on the steps of symmetric bilinear form of the unit 30 the skew-symmetric form is developed. It is seen that in the case of a skew-symmetric form, its matrix A in some (or every) ordered basis is skew-symmetric, $A^t = -A$.

11.1 Skew-symmetric Bilinear Forms

After discussing symmetric bilinear forms we can deal with the skew-symmetric forms with ease. Here again we are dealing wth finite vector space over a subfield F of the field of complex numbers.

A bilinear form f on V is called skew-symmetric if $f(\alpha, \beta), -f(\beta, \alpha)$ for all α, and β in V. It means that $f(\alpha, \alpha) = 0$. So we now need to introduce two different quadratic forms as follows:

If we let

$$g(\alpha, \beta) = \frac{1}{2}[f(\alpha, \beta) + f(\beta, \alpha)]$$

$$h(\alpha, \beta) = \frac{1}{2}[f(\alpha, \beta) + f(\beta, \alpha)]$$

So it is seen that g is a symmetric bilinear form on V and h is a skew-symmetric form on V. Also $f = g + h$. These expressions for V, as the symmetric and skew-symmetric form is unique. So the space $L(V, V, F)$ is the direct sum of the subspace of symmetric forms and the subspace of skew-symmetric forms.

Thus a bilinear form f is skew-symmetric if and only if its matrix A is equal to $-A^t$ in some ordered basis.

When f is skew-symmetric, the matrix of f in any ordered basis will have all its diagonal entries 0. This just corresponds to the observation that $f(\alpha, \alpha) = 0$ for every α in V, since $f(\alpha, \alpha) = -f(\alpha, \alpha)$.

Let us suppose f is a non-zero skew-symmetric bilinear form on V. Since $f \neq 0$, there are vectors α, β in V such that $f(\alpha, \beta) \neq 0$. Multiplying α by a suitable scalar, we may assume that $f(\alpha, \beta) = 1$. Let γ be any vector in the subspace spanned by α and β, say $\gamma = c\alpha + d\beta$. Then

$$f(\gamma, \alpha) = f(c\alpha + d\beta, \alpha) = df(\beta, \alpha) = -d$$

$$f(\gamma, \beta) = f(c\alpha + d\beta, \beta) = cf(\alpha, \beta) = c$$

and so

$$\gamma = f(\gamma, \beta)\alpha - f(\gamma, \alpha)\beta \qquad ...(1)$$

In particular, note that α and β are necessarily linearly independent; for, if $\gamma = 0$, then $f(\gamma, \alpha) = f(\gamma, \beta) = 0$.

Let W be the two-dimensional subspace spanned by α and β. Let $W^{\perp}$ be the set of all vectors δ in V such that $f(\delta, \alpha) = f(\delta, \beta) = 0$, that is, the set of all δ such that $f(\delta, \gamma) = 0$ for every γ in the subspace W. We claim that $V = W \oplus W^{\perp}$. For, let ε be any vector in V, and

$$\gamma = f(\varepsilon, \beta)\alpha - f(\varepsilon, \alpha)\beta$$

$$\delta = \varepsilon - \gamma.$$

Then γ is in W, and δ is in $W^{\perp}$, for

$$\begin{aligned} f(\delta, \alpha) &= f(\varepsilon - f(\varepsilon, \beta)\alpha + f(\varepsilon, \alpha)\beta, \alpha) \\ &= f(\varepsilon, \alpha) + f(\varepsilon, \alpha)f(\beta, \alpha) \\ &= 0 \end{aligned}$$

and similarly $f(\delta, \beta) = 0$. Thus every ε in V is of the form $\varepsilon = \gamma + \delta$, with γ in W and δ in $W^{\perp}$. From (1) it is clear that $W \cap W^{\perp} = \{0\}$, and so $V = W \oplus W^{\perp}$.

Now the restriction of f to $W^{\perp}$ is a skew-symmetric bilinear form on $W^{\perp}$. This restriction may be the zero form. If it is not, there are vectors α' and β' in $W^{\perp}$ such that $f(\alpha', \beta') = 1$. If we let W' be the two-dimensional subspace spanned by β' and β', then we shall have

$$V = W \oplus W' \oplus W_0$$

where W_0 is the set of all vectors δ in $W^{\perp}$ such that $f(\alpha', \delta) = f(\beta', \delta) = 0$. If the restriction of f to W_0 is not the zero form, we may select vectors α'', β'' in W_0 such that $f(\alpha'', \beta'') = 1$, and continue.

In the finite-dimensional case it should be clear that we obtain a finite sequence of pairs of vectors,

$$(\alpha_1, \beta_1), (\alpha_2, \beta_2), \dots, (\alpha_k, \beta_k)$$

with the following properties:

(a) $f(\alpha_j, \beta_j) = 1, j = 1, \dots, k$.

(b) $f(\alpha_i, \alpha_j) = f(\beta_i, \beta_j) = f[\alpha_i, \beta_j) = 0, i \neq j$.

(c) If W_j is the two-dimensional subspace spanned by β_j and β_j, then

$$V = W_1 \oplus \dots \oplus W_k \oplus W_0$$

where every vector in W_0 is 'orthogonal' to all α_j, and β_j, and the restriction of f to W_0 is the zero form.

Theorem 1: Let V be an n-dimensional vector space over a subfield of the complex numbers, and let f be a skew-symmetric bilinear form on V. Then the rank r of f is even, and if $r = 2k$ there is an ordered basis for V in which the matrix of f is the direct sum of the $(n - r) \times (n - r)$ zero matrix and k copies of the 2×2 matrix

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

Proof: Let $\alpha_1, \beta_1, \ldots \alpha_k, \beta_k$ be vectors satisfying conditions (a), (b), and (c) above. Let $\{\gamma_i, \ldots, \gamma_s\}$ be any ordered basis for the subspace W_0. Then

$$\beta = \{\alpha_1, \beta_1, \alpha_2, \beta_2, \ldots, \alpha_k\ \beta_k, \gamma_1, \ldots, \gamma_s\}$$

is an ordered basis for V. From (a), (b), and (c) it is clear that the matrix of f in the ordered basis β is the direct sum of the $(n - 2k) \times (n - 2k)$ zero matrix and k copies of the 2×2 matrix

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \qquad \ldots(2)$$

Furthermore, it is clear that the rank of this matrix, and hence the rank of f, is $2k$.

One consequence of the above is that if f is a non-degenerate, skew-symmetric bilinear form on V, then the dimension of V must be even. If dim $V = 2k$, there will be an ordered basis $\{\alpha_1, \beta_1, \ldots, \alpha_k, \beta_k\}$ for V such that

$$f(\alpha_i, \beta_j) = \begin{cases} 1, & i \neq j \\ 1, & i = j \end{cases}$$

$$f(\alpha_i, \alpha_j) = f(\beta_i, \beta_j) = 0$$

The matrix of f in this ordered basis is the direct sum of k copies of the 2×2 skew-symmetric matrix (2).

Self Assessment

1. Let f be a symmetric bilinear form on c^n and g a skew symmetric bilinear form on c^n. Suppose $f + g = 0$. Show that $f = 0$, $g = 0$.
2. Let V be an n-dimensional vector space over a subfield F of C. Prove that
   (a) The equation

   $(Pf)(\alpha, \beta) = \frac{1}{2} f(\alpha, \beta) - \frac{1}{2} f(\beta, \alpha)$ defines

   a linear operator P on $L(V, V, F)$

   (b) $P^2 = P$, i.e. P is a projection

11.2 Summary

- A bilinear form f on V is called skew-symmetric if $f(\alpha, \beta) = -f(\beta, \alpha)$
- The space $L(V, V, F)$ of the bilinear forms is the direct sum of the sub-space of symmetric forms and the subspace of skew-symmetric forms.
- In an n-dimensional vector space over a subfield of the complex numbers, the skew symmetric bilinear form f has an even rank $r = 2k$, k being an integer.

11.3 Keywords

Skew Symmetric Bilinear Form: A bilinear form f on V is called skew symmetric if $f(\alpha, \beta)\ -f(\beta, \alpha)$ for all vectors, α, β in V.

Skew-symmetric matrix: A matrix A in some (or every) ordered basis is skew-symmetric, if $A^{+} = -A$, i.e. the two by two matrix

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

is a skew-symmetric matrix.

A non-degenerate skew-symmetric bilinear form f is such that

$$f(\alpha_i, \beta_j) = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}$$

$$f(\alpha_i, \alpha_i) = f(\beta_i, \beta_i) = 0$$

the dimension of the space must be even i.e. $n = 2k$.

11.4 Review Questions

1. Let V be a vector space over a field F. Show that the set of all skew-symmetric bilinear forms on V a sub-space of $L(V, V, F)$

2. Let V be a finite dimensional vector space and L_1, L_2 linear functional on V. Show that the equation

   $$f(\alpha, \beta) = L_1(\alpha)\, L_2(\beta) - L_1(\beta)\, L_2(\alpha)$$

   denotes a skew symmetric bilinear form on V. Also show that $f = 0$ if and only if L_1, L_2 are linearly dependent.

11.5 Further Readings

Books Kenneth Hoffman and Ray Kunze, *Linear Algebra*

Michael Artin, *Algebra*

Unit 12: Groups Preserving Bilinear Forms

Notes

CONTENTS

Objectives

Introduction

12.1 Overview

12.2 Groups Preserving Bilinear Forms

12.3 Summary

12.4 Keywords

12.5 Review Questions

12.6 Further Readings

Objectives

After studying this unit, you will be able to:

- Understand that there are certain classes of linear transformations including the identity transformation that preserve the form f of bilinear forms.
- See that the collection of linear operators which preserve f, is closed under the formation of operator products.
- Know that a linear operator T preserves the bilinear form f if and only if T preserves the quadratic form

$$q(\alpha) = f(\alpha, \alpha)$$

- See that the group preserving a non-degenerate symmetric bilinear form f on V is isomorphism to an $n \times n$ pseudo-orthogonal group.

Introduction

In this unit the groups preserving certain types of bilinear forms is studied.

It is seen that orthogonal groups preserve the length of a vector.

For non-degenerate symmetric bilinear form on V the group preserving f is isomorphic to $n \times n$ pseudo-orthogonal group.

For the symmetric bilinear form f on R^4 with quadratic form

$$g(x, y, z, t) = t^2 - x^2 - y^2 - z^2$$

a linear operator T on R^4 preserving this particular bilinear form is called **Lorentz transformation** and the group preserving f is called the **Lorentz Group**.

12.1 Overview

Here we shall be concerned with some groups of transformations which preserve the form of the bilinear forms. Let T be a linear operator on V. We say that T preserves f if $f(T_\alpha, T_\beta) = f(\alpha, \beta)$ for all α and β in V. Consider a function $g(\alpha, \beta) = f(T_\alpha, T_\beta)$. If T preserves f it simply means $g = f$. The identity operator preserves every bilinear form. If S and T are two linear operators which preserve f, the product ST also preserves f; for $f(ST\alpha, ST\beta) = f(T\alpha, T\beta) = f(\alpha, \beta)$. In other words the collection of linear operators which preserve f, is closed under the formation of operator products.

Consider a bilinear form given by

$$\beta = \sum_{i,\, j=1}^{n} a_{ij} x_i y_j$$

If we introduce

$$X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix},\ Y = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}$$

then

$$B = X^t A Y$$

where n rowed square matrix A is

$$A = [a_{ij}]$$

In case $Y = X$ then we have a quadratic form

$$Q = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} x_i x_j$$

In matrix form

$$Q = X^T A X$$

We now consider certain transformation operator P such that

$$X = PX'$$

where P is non-singular (or invertible), then

$$X^t = (PX')^t = X'^t P^t$$

So

$$Q = X'^t P^t A P X'$$

Defining

$$A' = P^t A P$$

We have

$$Q = X'^t A' X'$$

If A is symmetric then

$$A^{t\prime} = (P^t A P)^t = P^t A^t P = P^t A P = A'$$

Thus symmetry of the matrix is maintained. Now if Q represents the length of the vector (x_1, x_2, ... x_n) then preservation of length means;

$$X^t X = X^{t\prime} P^t P X' = X^{t\prime} X',\ \text{if}$$

$$P^t P = I$$

which means that P is an orthogonal matrix.

One of the examples of the orthogonal transformation the rotation of co-ordinate system.

Example 1: Consider a three dimensional co-ordinates (x, y, z). Let us give a rotation along z-direction by an angle Q so that the new co-ordinates are x', y', z'

then

$$x' = x \cos \theta = y \sin \theta$$

$$y' = x \sin \theta + y \cos \theta$$

$$z' = z$$

We see that the square of the length becomes

$$x'^2 + y'^2 + z'^2 = (x \cos \theta - y \sin \theta)^2 + (x \sin \theta + y \cos \theta)^2 + z^2$$

$$= x^2 + y^2 + z^2.$$

So the rotation is a transformation that preserves the bilinear form of the length. For more details see the next section.

12.2 Groups Preserving Bilinear Forms

We start this section with a few theorems and examples.

Theorem 1: Let f be a non-degenerate bilinear form on a finite-dimensional vector space V. The set of all linear operators on V which preserve f is a group under the operation of composition.

Proof: Let G be the set of linear operators preserving f. We observed that the identity operator is in G and that whenever S and T are in G the composition ST is also in G. From the fact that f is non-degenerate, we shall prove that any operator T in G is invertible, and T^{-1} is also in G. Suppose T preserves f. Let α be a vector in the null space of T. Then for any β in V we have

$$f(\alpha, \beta) = f(T_{\alpha}, T_{\beta}) = f(0, T_{\beta}) = 0.$$

Since f is non-degenerate, $\alpha = 0$. Thus T is invertible. Clearly T^{-1} also preserves f; for

$$f(T^{-1}\alpha, T^{-1}\beta) = f(TT^{-1}\alpha, TT^{-1}\beta) = f(\alpha, \beta)$$

If f is a non-degenerate bilinear form on the finite-dimensional space V, then each ordered basis β for V determines a group of matrices 'preserving' f. The set of all matrices $[T]_{\beta}$, where T is a linear operator preserving f, will be a group under matrix multiplication. There is an alternative description of this group of matrices, as follows. Let $A = [f]_{\beta}$, so that if α and β are vectors in V with respective coordinate matrices X and Y relative to β, we shall have

$$f(\alpha, \beta) = X'AY.$$

Let T be any linear operator on V and $M = [T]_{\beta}$. Then

$$f(T\alpha, T\beta) = (MX)^t A (MY)$$

$$= X^t (M^t AM)Y.$$

Accordingly, T preserves f if and only if $M^t A M = A$. In matrix language then, Theorem 1 says the following: If A is an invertible $n \times n$ matrix, the set of all $n \times n$ matrices M such that $M^t AM = A$ is a group under matrix multiplication. If $A = [f]_{\beta}$, then M is in this group of matrices if and only if $M = [T]_{\beta}$, where T is a linear operator which preserves f.

Let f be a bilinear form which is symmetric. A linear operator T preserves f If and only if T preserves the quadratic form

$$g(\alpha) = f(\alpha, \alpha)$$

associated with f. If T preserves f, we certainly have

$$q(T\alpha) = f(T\alpha, T\alpha) = f(\alpha, \alpha) = q(\alpha)$$

for every α in V. Conversely, since f is symmetric, the polarization identity

$$f(\alpha, \beta) = \frac{1}{4} q(\alpha + \beta) - \frac{1}{4} q(\alpha - \beta)$$

shows us that T preserves f provided that $q(T\gamma) = q(\gamma)$ for each γ in V. (We are assuming here that the scalar field is a subfield of the complex numbers.)

Example 2: Let V be either the space R^n or the space C^n. Let f be the bilinear form

$$f(\alpha, \beta) = \sum_{j=1}^{n} x_i y_i$$

where $\alpha = (x_1, \ldots, x_n)$ and $\beta = (y_1, \ldots, y_n)$. The group preserving f is called the n-dimensional (real or complex) orthogonal group. The name 'orthogonal group' is more commonly applied to the associated group of matrices in the standard ordered basis. Since the matrix of f in the standard basis is I, this group consists of the matrices M which satisfy $M^tM = I$. Such a matrix M is called an $n \times n$ (real or complex) orthogonal matrix. The two $n \times n$ orthogonal groups are usually denoted $O(n, R)$ and $O(n, C)$. Of course, the orthogonal group is also the group which preserves the quadratic form

$$q(x_1, \ldots, x_n) = x_1^2 + \ldots + x^2n.$$

Example 3: Let f be the symmetric bilinear form on R^n with quadratic form

$$q(x_1 \ldots, x_n) = \sum_{j=1}^{p} x_j^2 - \sum_{j=p+1}^{n} x_j^2$$

Then f is non-degenerate and has signature $2p - n$. The group of matrices preserving a form of this type is called a **pseudo-orthogonal group**. When $p = n$, we obtain the orthogonal group $O(n, R)$ as a particular type of pseudo-orthogonal group. For each of the $n + 1$ values $p = 0, 1, 2, \ldots n$, we obtain different bilinear forms f; however, for $p = k$ and $p = n - k$ the forms are negatives of one another and hence have the same associated group. Thus, when n is odd, we have $(n + 1)/2$ pseudo-orthogonal groups of $n \times n$ matrices, and when n is even, we have $(n + 2)/2$ such groups.

Theorem 2: Let V be an n-dimensional vector space over the field of complex numbers, and let f be a non-degenerate symmetric bilinear form on V. Then the group preserving f is isomorphic to the complex orthogonal group $O(n, C)$.

Proof: Of course, by an isomorphism between two groups, we mean a one-one correspondence between their elements which 'preserves' the group operation. Let G be the group of linear operators on V which preserve the bilinear form f. Since f is both symmetric and non-degenerate, Theorem 4 of unit 30 tells us that there is an ordered basis β for V in which f is represented by the $n \times n$ identity matrix. Therefore, a linear operator T preserves f if and only if its matrix in the ordered basis β is a complex orthogonal matrix. Hence

$$T \to [T]_\beta$$

is an isomorphism of G onto $O(n, C)$.

Theorem 3: Let V be an n-dimensional vector space over the field of real numbers, and let f be a non-degenerate symmetric bilinear form on V. Then the group preserving f is isomorphic to an $n \times n$ pseudo-orthogonal group.

Proof: Repeat the proof of Theorem 2, using Theorem 5 of unit 30 instead of Theorem 4 of unit 30.

Example 4: Let f be the symmetric bilinear form on R^n with quadratic form

$$q(x, y, z, t) = t^2 - x^2 - y^2 - z^2.$$

A linear operator T on R^4 which preserves this particular bilinear (or quadratic) form is called a **Lorentz transformation**, and the group preserving f is called the **Lorentz group**. We should like to give one method of describing some Lorentz transformations.

Let H be the real vector space of all 2 × 2 complex matrices A which are Hermitian, $A = A^*$. It is easy to verify that

$$\phi(x, y, z, t) = \begin{bmatrix} t+x & y+iz \\ y-iz & t-x \end{bmatrix}$$

defines an isomorphism ϕ of R^4 onto the space H. Under this isomorphism, the quadratic form q is carried onto the determinant function, that is

$$q(x, y, z, t) = \det\begin{bmatrix} t+x & y+iz \\ y-iz & t-x \end{bmatrix}$$

or

$$q(\alpha) = \det \phi\,(\alpha).$$

This suggests that we might study Lorentz transformations on R^4 by studying linear operators on H which preserve determinants.

Let M be any complex 2 × 2 matrix and for a Hermitian matrix A define

$$U_M(A) = MAM^*.$$

Now MAM^* is also Hermitian. From this it is easy to see that U_M is a (real) linear operator on H. Let us ask when it is true that U_M 'preserves' determinants, i.e., det $[U_M(A)]$ = det A for each A in H. Since the determinant of M^* is the complex conjugate of the determinant of M, we see that

$$\det [U_M(A)] = [\det M|^2 \det A.$$

Thus U_M preserves determinants exactly when del M has absolute value 1.

So now let us select any 2 × 2 complex matrix M for which [det $M|$ = 1. Then U_M is a linear operator on H which preserves determinants. Define

$$T_M = \phi^{-1} U_M \phi.$$

Since ϕ is an isomorphism, T_M is a linear operator on R^4. Also, T_M is a Lorentz transformation; for

$$\begin{aligned} q(T_M\alpha) &= q(\phi^{-1}U_M\phi\alpha) \\ &= \det(\phi\phi^{-1}U_M\phi\alpha) \\ &= \det(U_M\phi\alpha) \\ &= \det(\phi\alpha) \\ &= q(\alpha) \end{aligned}$$

and so T_M preserves the quadratic form q.

By using specific 2 × 2 matrices M, one can use the method above to compute specific Lorentz transformations.

Self Assessment

1. Suppose M belongs $O(n, C)$. Let

$$y_i = \sum_{k=1}^{n} M_{ik} x_k$$

Show that

$$\sum_{i=1}^{n} y_i^2 = \sum_{j=1}^{n} x_j^2$$

2. If M be an $n \times n$ matrix over C with columns M_1, M_2, ... M_n. Show that M belongs to $O(n, c)$ if and only if

$$M^{+}j\, M_k = \delta_{jk}.$$

12.3 Summary

- In this unit certain groups preserving the bilinear forms is studied and seen that these set of groups is isomorphic to the $n \times n$ pseudo orthogonal group when the bilinear form is non-degenerate.
- The examples of rotation and Lorentz transformations that preserve certain bilinear forms are studied.

12.4 Keywords

Orthogonal group: The group preserving f given by

$$f(\alpha, \beta) = \sum_{i=1}^{n} x_i y_i$$

for $\alpha = (x_1, x_2, \ldots x_n)$, $\beta = (y_1, y_2, \ldots y_n)$, is called the n-dimensional (real or complex) orthogonal group.

Pseudo-orthogonal Group: For a non-degenerate bilinear form f on R^4 with quadratic form

$$q(x_1, x_2, \ldots x_n) = \sum_{j=1}^{p} x_j^2 - \sum_{i=p+1}^{n} x_i^2$$

the group of matrices preserving a form of this type is called **pseudo-orthogonal group**.

12.5 Review Questions

1. Let f be the bilinear form on C^2 defined by $f[(x_1, x_2), (y_1, y_2)] = x_1y_2 - x_2y_1$

   show that

   (a) if T is a linear operator on C^2, then $f(T\alpha, T\beta) = (\det T)\, f(\alpha, \beta)$ for α, β in C^2

   (b) T preserves f if and only if $\det T = +1$.

2. Let T be a linear operator C^2 which preserves the quadratic form $x_1^2 - x_2^2$ Show that

$$\det T = \pm 1.$$

12.6 Further Readings

Books Kenneth Hoffman and Ray Kunze, *Linear Algebra*

Michael, *Artin Algebra*