Linear Algebra

DMTH502

LOVELY
PROFESSIONAL
UNIVERSITY

LINEAR ALGEBRA

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

SYLLABUS

Linear Algebra

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
1	Vector Space over fields, Subspaces, Bases and Dimension, Coordinates, Summary of Row-Equivalence, Computation Concerning Subspaces
2	Linear Transformations, The algebra of linear transformations, The transpose of a linear transformation, Isomorphism, Representation of Transformation by matrices
3	Linear Functional, The double dual, Introduction and Characteristic Values, Annihilating Polynomials
4	Invariant Subspaces, Simultaneous triangulation, Simultaneous diagonalization, Direct-Sum Decompositions
5	Invariant Direct Sums, The Primary Decomposition Theorem, Cyclic Subspaces and Annihilators, Cyclic Decomposition and the rational Form
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

CONTENTS

Notes

Unit 1: Vector Space over Fields

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand the concept of abstract sets
- Explain the concept of functions
- Discuss the abstract groups and their properties
- State the properties of rings and fields
- Understand abstract vector space. This will help you to understand sub-spaces, bases and dimension in the next units
- Know that this unit is a prerequisite to understand the next few units.

Introduction

In this unit the idea of set theory is explained. The unit also deals with functions and mapping.

The ideas of rings and fields help us to study vector spaces and their structure. This unit briefly explains the properties of vector spaces which are useful in understanding the vector sub-spaces, bases dimensions and co-ordinates.

1.1 Sets

The concept of set is fundamental in all branches of mathematics. A set according to the German mathematician George Cantor, is a *collection of definite well-defined objects of perception or thought*. By a well defined collection we mean that there exists a rule with the help of which it is possible to tell whether a given object belongs or does not belong to the given collection. The objects in sets may be anything: numbers, people, animals etc. The objects constituting the set are called elements or members of the set.

Notes

One should note carefully the difference between a collection and a set. Every collection is not a set. For a collection to be a set, it must be well defined. For example the collection of "any four natural numbers" is not a set. The members of this collection are not well defined. The natural number 5 may belong or may not belong to this collection. But the collection of "the first four natural numbers" is a set. Obviously, the members of the collection are well-defined. They are 1, 2, 3 and 4.

A set is usually denoted by a capital letter, such as A, B, C, X, Y, Z etc. and an element of a set by the small letter such as a, b, c, x, y, z etc.

A set may be described by actually listing the objects belonging to it. For example, the set A of single digit positive integers is written as

$$A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

Here the elements are separated by commas and are enclosed in brackets { }. This is called the *tabular form* of the set.

A set may also be specified by stating properties which its elements must satisfy. The set is then described as follows:

$A = \{x : P(x)\}$ and we say that A is the set consisting of the elements x such that x satisfies the property $P(x)$. The symbol "." is read "such that". Thus the set X of all real numbers is simply written as

$$X = \{x : x \text{ is real}\} = \{x \mid x \text{ is real}\}.$$

This way of describing a set is called *the set builder* form of a set.

When a is an element of the set A, we write $a \in A$. If a is not an element of A, we write $a \notin A$.

When three elements, a, b and c, belong to the set A, we usually write $a, b, c \in A$, instead of writing $a \in A$, $b \in A$ and $c \in A$.

Two sets A and B are said to be equal iff every element of A is an element of b and also every element of B is an element of A, i.e. when both the sets consist of identical elements. We write "$A = B$" if the sets A and B are equal and "$A \neq B$" if the sets A and B are not equal.

If two sets A and B are such that every element of A is also an element of B, then A is said to be a *subset* of B. We write this relationship by writing $A \subset B$.

If $A \subset B$, then B is called a *superset* of A and we write $B \supset A$, which is read as 'B' is a super-set of A' or 'B contains A'.

If A is not a subset of B, we write $A \not\subset B$, which is read as 'A is not a subset of B'. Similarly $B \not\subset A$ is read as 'B is not a superset of A'.

From the definition of subset, it is obvious that every set is a subset of itself, i.e., $A \subset A$. We call B a proper subset of A if, first, B is a subset of A and secondly, if B is not equal to A. More briefly, B is a proper subset of A, if

$$B \subset A \text{ and } B \neq A.$$

Another improper subset of A is the set with no element in it. Such a set is called the *null set* or the *empty set*, and is denoted by the symbol ϕ. The null set ϕ is a subset of every set, i.e., $\phi \subset A$.

If A is any set, then the family of all the subsets of A is called the *power set* of A. The power set of A is denoted by $P(A)$. Obviously ϕ and A are both elements of $P(A)$. If a finite set A has n elements, then the power set of A has 2^n elements.

Notes

Example 1: If $A = \{a, b, c\}$ then $P(A) =$

$$\{\phi, \{a\}, \{b\}, \{c\}, \{a, b\}\ \{b, c\}, \{a, c\}, \{a, b, c\}\ \}.$$

The total number of these elements of power set is 8, i.e. 2^3.

The sets A and B are equal if A is a subset of B and also B is a subset of A.

If U be the universal set, the set of those elements of U which are not the elements of A is defined to be the *complement* of A. It is denoted by A'. Thus

$$A' = \{x : x \in U \text{ and } x \notin A\}$$

Obviously, $\{A'\}' = A$, $\phi' = U$, $U' = \phi$.

It is easy to see that if $A \subset B$, then $A' \supset B'$.

The difference of two sets A and B in that order is the set of elements which belong to A but which do not belong to B. We denote the difference of A and B by $A \sim B$ or $A - B$, which is read as "A difference B" or "A minus B". Symbolically $A - B = \{x : x \in A \text{ and } x \notin B\}$. It is obvious that $A - A = \phi$, and $A - \phi = A$.

Union and Intersection

Let A and B be two sets. The union of A and B is the set of all elements which are in set A or in set B. We denote the union of A and B by $A \cup B$, which is usually read as "A union B".

Symbolically, $A \cup B = \{x : x \in A \text{ or } x \in B\}$

On the other hand, the intersection of A and B is the set of all elements which are both in A and B. We denote the intersection of A and B by $A \cap B$, which is usually read as "A intersection B". Symbolically,

$$A \cap B = \{x : x \in A \text{ or } x \in B\}$$

or

$$A \cap B = \{x : x \in A, x \in B\}.$$

The union and intersection of sets have the following simple properties:

(i) $\left.\begin{array}{l} A \cup B = B \cup A \text{ and} \\ A \cap B = B \cap A \end{array}\right\}$ Commutative laws

(ii) $\left.\begin{array}{l} A \cup (B \cup C) = (A \cup B) \cup C \text{ and} \\ A \cap (B \cap C) = (A \cap B) \cap C \end{array}\right\}$ Associative laws

(iii) $\left.\begin{array}{l} A \cup A = A \text{ and} \\ A \cap A = A \end{array}\right\}$ Idempotent laws

(iv) $\left.\begin{array}{l} A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \text{ and} \\ A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \end{array}\right\}$ Distributive laws

(v) $\left.\begin{array}{l} A - (B \cup C) = (A - B) \cap (A - C) \text{ and} \\ A - (B \cap C) = (A - B) \cup (A - C) \end{array}\right\}$ De Morgan's laws

Notes

Two results which interrelate union and intersection of sets with their complements are as follows:

(i) the complement of the union is intersection of the complements, i.e.,

$(A \cup B)' = A' \cap B'$, and

(ii) the complement of the intersection is the union of the complements, i.e.,

$(A \cap B)' = A' \cup B'$.

Suppose A and B are two sets. Then the set $(A - B) \cup (B - A)$ is called the symmetric difference of the set A and B and is denoted by $A \Delta B$.

Since $(A - B) \cup (B - A) = (B - A) \cup (A - B)$

$\therefore$ $A \Delta B = B \Delta A$.

Product Set

Let A and B be two sets, $a \in A$ and $b \in B$. Then (a, b) denotes what we may call *an ordered pair*. The element a is called the first coordinate of the ordered pair (a, b) and the element b is called its second coordinate.

If (a, b) and (c, d) are two ordered pairs

then $(a, b) = (c, d)$ iff $a = c$ and $b = d$.

If A and B are two sets, the set of all distinct ordered pairs whose first coordinate is an element of A and whose second coordinate is an element of B is called the *Cartesian product* of A and B (in that order) and is denoted by $A \times B$. Symbolically,

$$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}.$$

In general $A \times B \neq B \times A$. If A has n elements and B has m elements, then the product set $A \times B$ has nm elements. If either A or B is a null set, the $A \times B = \phi$. If either A or B is infinite and the other is not empty, the $A \times B$ is infinite.

We may generalise the definition of the product sets. Let $A_1, A_2, \ldots, A_n$ be n given sets. The set of ordered n-tuples $(a_1, a_2, \ldots, a_n)$ where $a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n$ is called the Cartesian product of $A_1, A_2, \ldots, A_n$ and is denoted by $A_1 \times A_2 \times A_3 \times \ldots \times A_n$.

Functions or Mappings

Let A and B be two given sets. Suppose there is a correspondence, denoted by f, which associates to each members of A, a unique member of B. Then f is called *a function* or a *mapping* from A to B. The mapping f from A to B is denoted by

$$f : A \to B \text{ or by } A \xrightarrow{f} B.$$

Suppose f is a function from A to B. The set A is called the *domain* of the function f and B is called the *co-domain* of f. The element $y \in B$ which the mapping f associates to an element $x \in A$ is denoted by $f(x)$ and is called the f-image of x or the value of the function f for x. The element x may be referred to as a pre-image of $f(x)$. Each element of A has a unique image and each element of B need not appear as the image of an element in A. There can be more than one element of A which have the same image in B. We define the *range* of f to consist of those elements of B which appear as the image of at least one element in A. We denote the range of $f : A \to B$ by $f(A)$. Thus

$$f(A) = \{f(x) : x \in A\}.$$

Notes

Obviously, $f(x) \subset B$.

If A and B are any two non-empty sets, then a function f from A to B is a subset f of $A \times B$ satisfying the following condition:

(i) $\forall a \in A$, $(a, b) \in f$ for some $b \in B$;

(ii) $(a, b) \in f$ and $(a, b') \in f \Rightarrow b = b'$

The first condition ensures that each element in A will have image. The second condition guarantees that the image is unique.

If the domain and co-domain of a function f are both the same set say $f : A \to A$, then f is often called an *Operator* or *Transformation* of A.

Two functions f and g of $A \to B$ are said to be equal iff $f(x) = g(x)$ $\forall x \in A$ and we write $f = g$. For two unequal mappings from A to B, there must exist at least one element $x \in A$ such that $f(x) \neq g(x)$.

Types of Functions

If the function $f : A \to B$ is such that there is at least one element in B which is not the f-image of any element in A, then we say that f is a function of A '*into*' B. In this case the range of f is a proper subset of the co-domain of f.

If the function $f : A \to B$ is such that each element in B is the f-image of at least one element in A, then we say that f is a function of A '*onto*' B. In this case the range of f is equal to the co-domain of f, i.e., $f(A) = B$. Onto mapping is also sometimes known as *surjection*.

A function $f : A \to B$ is said to be *one-one* or *one-to-one* if different elements in A have different f-images in B, i.e., if

$$f(x) = f(x') \Rightarrow x = x' \ (x \text{ and } x' \in A).$$

One-to-one mapping is also sometimes known as injection.

A mapping $f : A \to B$ is said to be many-one if two (or more than two) distinct elements in A have the same f-image in B.

If $f : A \to B$ is one-one and onto B, then f is called a one-to-one correspondence between A and B. One-one onto mapping is also sometimes known as bijection.

Two sets A and B are said to be have the same number of elements iff a one-to-one correspondence of A onto B exists. Such sets are said to be cardinally equivalent and we write $A \sim B$.

Let A be any set. Let the mapping $f : A \to A$ be defined by the formula $f(x) = x$, $\forall x \in A$, i.e. each element of A be mapped on itself. Then f is called the identity mapping on A. We shall denote this function by I_A.

Inverse Mapping

Let f be a function from A to B and let $b \in B$. Then the inverse image of the element b under f denoted by $f^{-1}(b)$ consists of those elements in A which have b as their f-image.

Let $f : A \to B$ be a one-one onto mapping. Then the mapping $f^{-1} : B \to A$, which associates to each element $b \in B$, the element $a \in A$, such that $f(a) = b$ is called the inverse mapping of the mapping $f : A \to B$.

It must be noted that the inverse mapping of $f : A \to B$ is defined only when f is one-one onto, and it is easy to see that the inverse mapping $f^{-1} : B \to A$ is also one-one and onto.

Notes

Product or Composite of Mappings

Let $f : X \to Y$ and $g : Y \to Z$. Then the composite of the mappings f and g denoted by $(g \circ f)$, is a mapping from X to Z given by $(g \circ f) : X \to Z$ such that $(g \circ f)(x) = g[f(x)]$, $\forall\ x \in X$.

If $f : X \to X$ and $g : X \to X$ then we can find both the composite mappings $g \circ f$ and $f \circ g$, but in general $f \circ g \neq g \circ f$.

The composite mapping possesses the following properties:

(i) The composite mapping $g \circ f$ is one-one onto if the mappings f and g are such.

(ii) If $f : X \to Y$ is a one-one onto mapping,

then $f \circ f^{-1} = I_y$ and $f^{-1} \circ f = I_x$.

(iii) If $f : X \to Y$ and $g : Y \to Z$ are two one-one onto mappings, and $f^{-1} : Y \to X$ and $g^{-1} : Z \to Y$ are their inverses, then the inverse of the mapping $g \circ f : X \to Z$ is the mapping $f^{-1} \circ g^{-1} : Z \to X$.

(iv) If $f : X \to Y$, $g : Y \to Z$, $h : Z \to U$ be any mappings, then $h \circ (g \circ f)$ and $(h \circ g) \circ f$ are equal mappings of X into U, i.e. the *composite mapping is associative.*

Relation

If a and b be two elements of a set A, a relation R between them, is symbolically written as aRb, which means a in R—related to b.

For example, if R is the relation >, the statement $a\ R\ b$ means a is greater *than* b.

A relation R is said to be well defined on the set A if for each ordered pair (a, b), where $a, b \in A$, the statement $a\ R\ b$ is either true or false. A relation in a set A is a subset of the product set $A \times A$.

Inverse Relation

Let R be a relation from A to B. The inverse relation of R denoted by R^{-1}, is a relation from B to A defined by

$$R^{-1} = \{(y, x) : y \in B, x \in A, (x, y) \in A \times B\}$$

Clearly, if R is a relation from A to B, then the domain of R is identical with the range of R^{-1} and the range of R is identical with the domain of R^{-1}.

Difference between Relations and Functions

Suppose A and B are two sets. Let f be a function from A to B. Then by the definition of function f is a subset of $A \times B$ in which each $a \in A$ appears in one and only one ordered pair belonging to f. In other words f is a subset of $A \times B$ satisfying the following two conditions:

(i) for each $a \in A$, $(a, b) \in f$ for some $b \in B$,

(ii) if $(a, b) \in f$ and $(a, b') \in f$, then $b = b'$.

On the other hand every subset of $A \times B$ is a relation from A to B. *Thus every function is a relation but every relation is not a function*. If R is a relation from A to B, then domain of R may be a subset of A. But if f is a function from A to B, then domain of f is equal to A. In a relation from A to B an element of A may be related to more than one element in B. Also there may be some elements of A which may not be related to any element in B. But in a function from A to B each element of A must be associated to one and only one element of B.

Notes

Equivalence Relation

The relation R defined on a set A is to be *reflexive* if aRa holds for every a belonging to A, i.e.,

$$(a, a) \in R, \text{ for every } a \in A.$$

The relation R is said to be symmetric if

$$a\ R\ b \Rightarrow b\ R\ a$$

for every ordered pair $(a, b) \in R$, i.e.,

$$(a, b) \in R \Rightarrow (b, a) \in R.$$

The relation R is said to be transitive if

$$(a\ R\ b, b\ R\ c) \Rightarrow a\ R\ c$$

for every a, b, c belonging to A i.e.,

$$[(a, b) \in R, (b, c) \in R] \Rightarrow (a, c) \in R.$$

A relation R defined on a set is called *an equivalence relation if it is* reflexive, symmetric and transitive.

Natural Numbers

The properties of natural numbers were developed in a logical manner for the first time by the Italian mathematician *G.* Peano, by starting from a minimum number of simple postulates. These simple properties, known as the *Peano's Postulates* (*Axioms*), may be stated as follows:

Let there exist a non-empty set N such that.

Postulate I: $1 \in N$, that is, 1 is a natural number.

Postulate II: For each $n \in N$ there exists a unique number $n^+ \in N$, called the successor of n.

Postulate III: For each $n \in N$, we have $n^+ \neq 1$, i.e., 1 is not the successor of any natural number.

Postulate IV: If $m, n \in N$, and $m^+ = n^+$ then $m = n$, i.e. each natural number, if it is a successor, is the successor of a unique natural number.

Postulate V: If K is any subset of N having the properties (i) $1 \in K$ and (ii) $m \in K \Rightarrow m^+ \in K$, then $K = N$.

The postulate V is known as the *Postulate of induction* or the *Axiom of induction*. The *Principle of mathematical induction* is just based on this axiom.

Addition Composition

In the set of natural numbers N, we define addition, which shall be denoted by the symbol '+' as follows:

(i) $m + 1 = m^+ \ \forall\ m, \in N$

(ii) $m + n^* = (m + n)^* \ \forall\ m, n \in N.$

The distinctive properties of the addition operation in N are the closure, associative, commutative and cancellation laws, i.e., if $m, n, p \in N$, then

(A_1) $m + n \in N$ (closure law)

(A_2) $(m + n) + p = m + (n + p)$ (associative law)

Notes

(A_3) $m + n = n + m$, (commutative law)

(A_4) $m + p = n + p \Rightarrow m = n$ (cancellation law)

All these properties can be established from the foregoing postulates and definitions only.

Multiplication Composition

In the set of natural numbers N, we define multiplication which shall be denoted by the symbol 'X' as follows:

(i) $m \times 1 = m \ \forall \ m \in N$

(ii) $m \times n^+ = m \times n + m, \ \forall \ m, n \in N$.

Sometimes we often find it convenient to represent $m \times n$ by $m \,.\, n$ or simply by mn.

The following properties, which can be established from Peano's postulates, hold for multiplication.

(M_1) $m, n \in N$, or $mn \in N$, (Closure law)

(M_2) $(m \,.\, n) \,.\, p = m \,.\, (n \,.\, p)$ or $(m\, n)\, p = m\, (n\, p)$, (associative law)

(M_3) $m \,.\, n = n \,.\, m$, or $m\, n = n\, m$ (Commutative law)

(M_4) $m \,.\, p = n \,.\, p \Rightarrow m = n$, or $m\, p = n\, p \Rightarrow m = n$. (Cancellation law)

Distributive Law

The distributive property of multiplication over addition is expressed in the following two forms:

If $m, n, p \in N$, we have

(i) $m \,.\, (n + p) = m \,.\, n + n \,.\, p$ [Left distributive law]

(ii) $(m + n) \,.\, p = m \,.\, p + n \,.\, p$ [Right distributive law]

The right distributive law can also be inferred from the left distributive law, since multiplication is commutative.

Order Property

We say that a natural number m is greater than another number $n (m > n)$, if there exists a number $u \in N$, such that $m = n + u$.

The number m is said to be less than the number $n (m < n)$, if there exists a number $v \in N$, such that $n = m + v$.

This *order relation* possesses the following property.

For any two natural numbers m and n, there exists one and only one of the following three possibilities:

(i) $m = n$

(ii) $m > n$,

(iii) $m < n$.

This is known as the *Trichotomy law* of natural numbers.

It is evident that any set of natural numbers has a smallest number, i.e., if A is a non-empty subset of N, there is a number $m \in A$, such that $m \leq n$ for every $n \in A$.

Notes

This is known as the *well ordering property* of natural numbers.

The relations between order and addition, and order and multiplication are given by the following results:

(i) $m > n \Rightarrow m + p > n + p$,

(ii) $m > n \Rightarrow m\,p > n\,p$, for all $m, n, p \in N$.

The operation of *subtracting* a number n from another number m is possible only when $m > n$, i.e., the subtraction operation is not defined for any two natural numbers. It is thus not a binary composition in N.

Similarly the operation of *dividing* one number is also not always possible, i.e., the division operation is also not a binary composition in N.

Integers

The set of integers is constructed from the set of natural numbers by defining a relation, denoted by "~" (read as wave), in $N \times N$ as follows:

$$(a,b) \sim (c,d) \text{ if } a + d = b + c,\ a,b,c,d \in N\ .$$

Since this relation is an equivalence relation it decomposes the set $N \times N$ into disjoint equivalence classes. We define the set of all these equivalence classes as the *set of integers* and denote it by Z.

The equivalence class of the pair (a, b) may be denoted by

$$(a, b) \text{ or } (a, b)^*$$

The addition and multiplication operations in Z are now defined as follows:

$$(a, b)^* + (c, d)^* = (a + c, b + d)^*$$

and $$(a, b)^* \,.\, (c, d)^* = (ac + bd, ad + bc)^*.$$

The *associative and commutative laws of addition and multiplication* hold as for natural numbers. The *cancellation law of addition* holds in general, but the cancellation law of multiplication holds with some restrictions. The *distributive law of multiplication over addition* is also valid.

The equivalence class $(1, 1)^*$ is defined as the integer *zero*, and is written as 0. Thus

$$0 = (1, 1)^* = (a, a)^* = (b, b)^*,\ a, b \in N.$$

This number 0 possesses the properties, that for any integer x,

(i) $x + 0 = x$ and

(ii) $x \,.\, 0 = 0$.

If $x = (\alpha, \beta)^*$ is an integer other than zero, we have $\alpha \neq \beta$, i.e., either $\alpha > \beta$ or $\alpha < \beta$. We say that the integer $(\alpha, \beta)^*$ is positive if $\alpha > \beta$ and *negative* if $\alpha < \beta$.

When $\alpha > \beta$, $\alpha, \beta \in N$, there exists a natural number u such that $\alpha = u + \beta$.

Therefore a positive integer x is given by

$$x = (\alpha,\beta)^*, \alpha > \beta, = (u + \beta, \beta)^* = (u + \alpha, \alpha)^*\ .$$

It is possible to identify the positive integer $(u + \alpha, \alpha)^*$ with the natural number u, and write it as $+ u$. Thus the set of positive integers may be written as

$$Z_N = \{+1, +2, +3, \ldots\}$$

Notes

Similarly, a negative integer can be identified with the number $-u$, and the set of negative integers written as

$$Z_{-N} = \{-1, -2, -3, \ldots\}$$

We define the *negative of an integer* x as the integer y, such that $x + y = 0$. It is easy to see that every integer has its negative. For, let

$x = (a, b)^*$. Then if $y = (b, a)^*$, we have

$$x + y = (a, b)^* + (b, a)^* = (a + b, b + a)^*$$

$$= (a + b, a + b)^* = 0$$

The negative of the integer x, also called the *additive inverse* of x, is denoted by $-x$. We therefore have, for any integer x,

$$x + (-x) = 0$$

and

$$x = (a, b)^* \Rightarrow -x = (b, a)^*.$$

We define *subtraction* of an integer if from an integer x as $x + (-y)$, written as $x - y$. Thus if $x = (a, b)^*$ and $y = (c, d)^*$, we have

$$x - y = x + (-y) = (a, b) + (d, c)^*$$

$$= (a + d, b + c)^*$$

Order Relation in Integers

If x, y be the two integers, we define $x = y$ if $x - y$ is zero, $x > y$ if $x - y$ is positive and $x < y$ if $x - y$ is negative.

The *Trichotomy Law* for integers holds as for natural numbers. Further,

$$x > y \Rightarrow x + z > y + z,$$

and

$$x > y, z > 0 \Rightarrow x z > yz, x, y, z \in Z.$$

The *cancellation law for multiplication* states that

$$xz = yz, z \neq 0 \Rightarrow x = y.$$

The addition and multiplication operations on Z satisfy the laws of natural numbers with the only modification in cancellation law of multiplication which requires $p \neq 0$. Further, the addition operation satisfies the following two properties in Z.

(i) There exists the *additive identify* 0 in the set, i.e., $0 \in Z$ such that $a + 0 = 0 + a = a$, for any $a \in Z$.

(ii) There exists the *additive inverse* of every element in Z, i.e., $a \in Z \Rightarrow -a \in Z$ such that $a + (-a) = (-a) + a = 0$.

Division

A non-zero a is said to be a *divisor* (factor) of an integer b if there exists an integer c, such that $b = ac$.

When a is divisor of b, we write "$a \mid b$". Also we say that b is an integral multiple of a. It is obvious that division is not everywhere defined in Z.

The relation of divisibility in the set of integers Z is reflexive, since $a \mid a$, $\forall\ a \in Z$. It is also transitive, since $a \mid b$ and $b \mid c \Rightarrow a \mid c$. But it is not symmetric.

Notes

The *absolute value* "$|a|$" of an integer a is defined by

$$|a| = a \text{ when } a \geq 0$$

$$= -a \text{ when } a < 0$$

Thus, except when $a = 0$, $|a| \in Z_N$.

A non-zero integer p is called a *prime* if it is neither 1 nor –1 and if its only divisors are 1, –1, p, $-p$.

When $a = bc$ with $|b| > 1$ and $|c| > 1$, we call a *composite*. Thus every integer $a \neq 0, \pm 1$ is either a prime or composite.

The operation of division of one integer by another is carried out in accordance with the *division algorithm*, which can be stated as follows.

Given two positive integers a, b there exists uniquely two non-negative integers q, r such that

$$a = bq + r, 0 \leq r < b$$

The number q is called the *quotient*, and r the *remainder* obtained on dividing a by b.

Two other forms of the theorem, which are successive generalisations, are as follows:

(i) Given two integers a, b with $b > 0$, there exist unique integers q, r, such that

$$a = bq + r, 0 \leq r < b$$

(ii) Given two integers a, b with $b \neq 0$, there exist unique integers q, r, such that

$$a = bq + r, 0 \leq r < |b|.$$

Greatest Common Divisor

A *greatest common divisor* (GCD) of two integers a and b is a positive integer d such that

(i) $d \mid a$ and $d \mid b$, and

(ii) if for an integer c, $c \mid a$ and $c \mid b$, then $c \mid d$.

We shall use the notation (a, b) for the greatest common divisor of two integers a and b. The greatest common divisor is sometimes also called *highest common factor* (HCF).

Every pair of integers a and b, not both zero, has a unique greatest common divisor (a, b) which can be expressed in the form $(a, b) = ma + nb$ for some integers m and n.

Rational Numbers

Let $(a, b) \in Z \times Z_0$, where Z_0 is the set of non-zero integers. Then the equivalence class

$$\overline{(a,b)} = \{(m,n) : (m,n) \sim (a,b); m \in Z, n \in Z_0\}$$

is called a *rational number*.

The set of all equivalence classes of $Z \times Z_0$ determined by the equivalence relation ~ defined as above is called the set of rational numbers to be denoted by Q.

The addition and multiplication operations in Q are defined as follows:

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(ad + bc, bd)}$$

and

$$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac, bd)}$$

Notes

The *associative and commutative laws of addition and multiplication* hold as for integers, and so also the distributive law of multiplication over addition. The cancellation laws hold for addition and multiplication, except as for integers.

The additive identity is the number $\overline{(0,1)}$. For

$$\overline{(a,b)}+\overline{(0,1)}=\overline{(a.1+b.1)}=\overline{(a,b)}$$

The multiplicative identity is the number $\overline{(1,1)}$. For,

$$\overline{(a.b)}+\overline{(1,1)}=\overline{(a.1,b.1)}=\overline{(a,b)}$$

The additive inverse of $\overline{(a,b)}$ is $\overline{(-a,b)}$. For,

$$\overline{(a,b)}+\overline{(-a,b)}=\overline{(a.b-ba,b^2)}=\overline{(0,b^2)}=(0,1)$$

The multiplicative inverse of $\overline{(a,b)}$ is $\overline{(b,a)}$ if a ≠ 0. For,

$$\overline{(a,b)}\cdot\overline{(b,a)}=\overline{(ab,ba)}=\overline{(1,1)}$$

The additive identity $\overline{(0,1)}$, is defined as the rational number *zero* and is written as 0.

The non-zero rational number $\overline{(a,b)}$ which is such that a ≠ 0, is said to be positive or negative according as a *a b* is positive or negative.

The negative of a rational number *z* is its additive inverse; it is written as –*x*. Thus if *x* = $\overline{(a,b)}$ then –*x* = $\overline{(-a,b)}$.

We define *subtraction* of a rational number *y* from a rational number *x* as *x* + (–*y*), written *x* – *y*. Thus, if *x* = $\overline{(a,b)}$ and *y* = $\overline{(c,d)}$, we have

$$x-y=x+(-y)=\overline{(a,b)}+\overline{(-c,d)}=\overline{(ad-bc,bd)}$$

The *reciprocal* of a non-zero rational number *x* is its multiplicative inverse, and is written as 1/x. Thus if *x* = $\overline{(a,b)}$, then

$$1/x=\overline{(b,a)},\ a\neq 0,\ b\neq 0.$$

The *division* of a rational number *x* by a non-zero rational number *y*, written as *x* ÷ *y* or *x* | *y*, is defined as *x*. (1/*y*). Thus if *x* = $\overline{(a,b)}$, then

$y=\overline{(c,d)}, c\neq 0,$ we have

$$x+y=\overline{(a,b)}\cdot\overline{(d,c)}=\overline{(ad\cdot bc)}, b\neq 0, c\neq 0\ .$$

It can be shown that subtraction is a binary composition in *Q*, and division is also a binary composition, except for division by zero.

Order Relation

Let *x*, *y* be two rational numbers. We say that *x* is greater than, less than or equal to *y*, if *x* – *y* is positive, negative or zero, and we use the usual signs to denote these relations.

Notes

if $x = \overline{(a,b)}$, $y = \overline{(c,d)}$, we have $x > y$.

if $x - y = \overline{(a,b)} + \overline{(-c,d)} = \overline{(ad-bc,bd)} > 0$,

whence we find

$(ad - bc)\, bd > 0$, i.e., $ad > bc$, $b > 0$, $d > 0$.

Similarly, $x < y$ if $ad < bc$, $b > 0$, $d > 0$.

and $x = y$ if $ad = bc$.

The *Trichotomy Law* holds for rational numbers, as usual, i.e., given two rational numbers x, y either $x > y$ or $x = y$, or $x < y$.

Also the *order relation* is compatible with addition and multiplication. For,

$$x > y \Rightarrow x + z > y + z$$

and $x > y,\ z > 0 \Rightarrow xz > yz,\ x, y, z \in Q$.

Representation of Rational Numbers

A rational number of the form $\overline{(a,1)}$ can be identified with the integer $a \in Z$, and written simply as a.

Further, since

$$\overline{(a,1)} \div \overline{(b,1)} = \overline{(a,1)} \cdot \overline{(1,b)} = \overline{(a,1,1\cdot b)} = \overline{(a,b)}$$

we obtain a method of representing the rational number (a, b) by means of two integers.

We have $\overline{(a,b)} = \overline{(a,1)} \div \overline{(b,1)}$

$= a \div b$ or $a \mid b,\ b \neq 0$.

With this notation, the sum and product of two rational numbers assume the usual meaning attached to them, viz.,

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

and $$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},\ b \neq 0,\ d \neq 0$$

Also $$\frac{a}{b} > \frac{c}{d} \Rightarrow ad > bc,\ b > 0,\ d > 0\ .$$

The system of rational numbers Q provides an extension of the system of integral Z, such that (*i*) $Q \supset Z$, (*ii*) addition and multiplication of two integers in Q have the same meanings as they have in Z and (*iii*) the subtraction and division operations are defined for any two numbers in Q, except for division by zero.

In addition to the properties described above the system of rational numbers possesses certain distinctive characteristics which distinguish it from the system of integers or natural numbers. One of these is the property of *denseness* (the density property), which is described by saying that *between any two distinct rational numbers there lies another rational number.*

Notes

Since there lies a rational number between any two rational numbers, it is clear that there lie an infinite number of rational numbers between two given rationals. This property of rational numbers make them dense every where. Evidently integral numbers or the natural numbers are not dense in this sense.

Real Numbers

We know that the equation $x^2 = 2$ has no solution in Q. Therefore if we have a square of unit length, then there exists no rational number which will give us a measure of the length of its diagonal. Thus we feel that our system of rational numbers is inadequate and we want to extend it.

The extension of rational numbers into real numbers is done by special methods two of which are due to Richard Dedekind and George Cantor. We shall not describe these methods here. We can simply say here that a real number is one which can be expressed in terms of decimals whether the decimals terminate at some state or we have a system of infinite decimals, repeating or non-repeating. We know that every repeating infinite decimals is a rational number, also every terminating decimal is a rational number.

Irrational Number

A real number which cannot be put in the form p/q where p and q are integers is called an *irrational number*. The set R of real numbers is the union of the set of rational numbers and the set of irrational numbers.

If a, b, c are real numbers, then

(i) $a + b = b + a$, $ab = ba$ (commutative of addition and multiplication)

(ii) $\left.\begin{array}{l} a+(b+c)=(a+b)+c, \\ a\,(bc)=(ab)\,c \end{array}\right\}$ Associativity of addition and multiplication

(iii) $a + 0 = 0 + a = a$, i.e., the real number 0 is the additive identity.

(iv) $a.1 = 1.a = a$, i.e., the real number 1 is the multiplicative identity.

(v) For each $a \in R$, these corresponds $-a \in R$ such that

$a + (-a) = -(a) + a = 0$

Thus every real number has an additive inverse.

(vi) Each non-zero real number has multiplicative inverse.

(vii) Multiplication composition distributes addition, i.e.,

$$a\,(b + c) = ab + ac$$

(viii) The cancellation law invariably holds good for addition. For multiplication, if $a \neq 0$, then

$$ab = ac \Rightarrow b = c$$

(ix) The order relations satisfy the *trichotomy law*.

Complex Numbers

An ordered pair (a, b) of real numbers is called a complex number. The product set $R \times R$ consisting of the ordered pairs of real numbers is called the *set of complex numbers*. We shall denote the set of complex numbers by C.

Thus

$$C = \{z : z = (a, b), a, b \in R\}.$$

Notes

Two complex numbers (a, b) and (c, d) are equal if and only if

$$a = c \text{ and } b = d.$$

The *sum* of two complex numbers (a, b) and (c, d) is defined to be the complex number $(a + c, b + d)$ and symbolically, we write

$$(a, b) + (c, d) = (a + c, b + d)$$

The addition of complex numbers is commutative, associative, admits of identity element and every complex number possesses additive inverse.

If u and v are two complex numbers, then $u - v = u + (-v)$.

The cancellation law for addition in C is

$$(a, b) + (c, d) = (a, b) + (e, f) \Rightarrow (c, d) = (e, f) \ \forall\ (a, b), (c, d), (e, f) \in C.$$

The *product* of the complex numbers (a, b) and (c, d) is defined to be the complex number $(ac - bd, ad + bc)$ and symbolically we write

$$(a, b)\ (c, d) = (ac - bd, ad + bc).$$

The multiplication of complex numbers is commutative, associative admits of identity element and every non-zero complex number possesses multiplicative inverse.

Cancellation law for multiplication in C is

$$[(a, b)\ (c, d) = (a, b)\ (e, f) \text{ and } (a, b) \neq (0, 0)] \Rightarrow (c, d) = (e, f)$$

In C multiplication distributes addition.

A complex number (a, b) is said to be divided by a complex number (c, d) if there exists a complex number (x, y) such that $(x, y)\ (c, d) = (a, b)$.

The division, except by $(0, 0)$, is always possible in the set of complex numbers.

Usual Representation of Complex Numbers

Let (a, b) be any complex number.

We have
$$(a, b) = (a, 0) + (0, b)$$
$$= (a, 0) + (0, 1)\ (b, 0)$$

Also, we have $(0, 1)\ (0, 1) = (-1, 0) = -1$. If we denote the complex number $(0, 1)$ by i, we have $i^2 = -1$. Also we have $(a, b) = a + ib$, which is the usual notation for a complex number.

In the notation $Z = a + ib$ for a complex number, a is called the real part and b is called the imaginary parts. A complex number is said to be purely real if its imaginary part is zero, and purely imaginary if its part is zero but its imaginary part is not zero.

For each complex number $z = (a, b)$, we define the complex number $z = (a, -b)$ to be the conjugate of z. In our usual notation, if

$$z = a + ib$$

then
$$\bar{z} = a - ib$$

If $z = (a, b)$ be any complex number, then the non-negative real number $\sqrt{(a^2 + b^2)}$ is called the *modulus of the complex number* z and is denoted by $|z|$.

Notes

1.2 Groups

The theory of groups, an important part in present day mathematics, started early in nineteenth century in connection with the solutions of algebraic equations. Originally a group was the set of all permutations of the roots of an algebraic equation which has the property that combination of any two of these permutations again belongs to the set. Later the idea was generalized to the concept of an abstract group. An abstract group is essentially the study of a set with an operation defined on it. Group theory has many useful applications both within and outside mathematics. Group arise in a number of apparently unconnected subjects. In fact they appear in crystallography and quantum mechanics, in geometry and topology, in analysis and algebra and even in biology. Before we start talking of a group it will be fruitful to discuss the binary operation on a set because these are sets on whose elements algebraic operations can be made. We can obtain a third element of the set by combining two elements of a set. It is not true always. That is why this concept needs attention.

Binary Operation on a Set

The concept of binary operation on a set is a generalization of the standard operations like *addition* and *multiplication* on the set of numbers. For instance we know that the operation of addition (+) gives for any two natural numbers m, n another natural number $m + n$, similarly the multiplication operation gives for the pair m, n the number $m.n$ in N again. These types of operations are found to exist in many other sets. Thus we give the following definition.

Definition

A binary operation to be denoted by 'o' on a non-empty set G is a *rule* which associates to each pair of elements a, b in G a unique element $a\ o\ b$ of G.

Alternatively a binary operation 'o' on G is a mapping from $G \times G$ to G i.e. $o : G \times G \to G$ where the image of (a, b) of $G \times G$ under 'o', i.e., $o\ (a, b)$, is denoted by $a\ o\ b$.

Thus in simple language we may say that a binary operation on a set tells us how to combine any two elements of the set to get a unique element, again of the same set.

If an operation 'o' is binary on a set G, we say that G is *closed or closure property* is satisfied in G, with respect to the operation 'o'.

Examples:

(i) Usual addition (+) is binary operation on N, because if $m, n \in N$ then $m + n \in N$ as we know that sum of two natural numbers is again a natural number. But the usual substraction (–) is not binary operation on N because if $m, n \in N$ then $m - n$ may not belongs to N. For example if $m = 5$ and $n = 6$ their $m - n = 5 - 6 = -1$ which does not belong to N.

(ii) Usual addition (+) and usual substraction (–) both are binary operations on Z because if $m, n \in Z$ then $m + n \in Z$ and $m - n \in Z$.

(iii) Union, intersection and difference are *binary operations* on $P(A)$, the power set of A.

(iv) Vector product is a binary operation on the set of all 3-dimensional Vectors but the dot product is not a binary operation as the dot product is not a vector but a scalar.

Notes

Types of Binary Operations

Binary operations have the following types:

1. ***Commutative Operation:*** A binary operation o over a set G is said to be commutative, if for every pair of elements $a, b \in G$,

$$a \, o \, b = b \, o \, a$$

Thus addition and multiplication are commutative binary operations for natural numbers whereas subtraction and division are not commutative because, for $a - b = b - a$ and $a \div b = b \div a$ cannot be true for every pair of natural numbers a and b.

For example $5 - 4 \neq 4 - 5$ and $5 \div 4 = 4 \div 5$.

2. ***Associative Operation:*** A binary operation o on a set G is called *associative* if $a \, o \, (b \, o \, c) = (a \, o \, b) \, o \, c$ for all $a, b, c \in G$.

Evidently ordinary addition and multiplication are associative binary operations on the set of natural numbers, integers, rational numbers and real numbers. However, if we define $a \, o \, b = a - 2b \; \forall \; a, b \in R$

then $(a \, o \, b) \, oc = (a \, o \, b) - 2c = (a - 2b) - 2c = a - 2b - 2c$

and $a \, o \, (b \, o \, c) = a - 2(b \, o \, c) = a - 2(b - 2c)$

$= a - 2b + 4c.$

Thus the operation defined as above is not associative.

3. ***Distributive Operation:*** Let o and o' be two binary operations defined on a set, G. Then the operation o' is said to be *left distributive* with respect to operation o if

$$a \, o' \, (b \, o \, c) = (a \, o' \, b) \, o \, (a \, o' \, c) \text{ for all } a, b, c \in G$$

and is said to be right distributive with respect to o if,

$$(b \, o \, c) \, o' \, a = (b \, o' \, a) \, o \, (c \, o' \, c) \text{ for } a, b, c, \in G.$$

Whenever the operation o is left as well as right distributive, we simply say that o is distributive with respect to o.

Identity and Inverse

Identity: A composition o in a set G is said to admit of an identity if these exists an element $e \in G$ such that

$$a \, o \, e = a = e \, o \, a \; \forall \; a \in G.$$

Moreover, the element e, if it exists is called an identity element and the algebraic structure (G, o) is said to have an identity element with respect to o.

Examples:

(i) If a $\in$ R, the set of real numbers then 0 (zero) is an additive identity of R because

$$a + 0 = a = 0 + a \; \forall \; a \in R$$

N the set of natural numbers, has no identity element with respect to addition because $0 \in N$.

Notes

(ii) 1 is the multiplicative identity of N as

$$a.1 = 1.a = a \forall\ a \in N.$$

Evidently 1 is identity of multiplication for I (set of integers), Q (set of rational numbers, R (set of real numbers).

Inverse: An element $a \in G$ is said to have its inverse with respect to certain operation o if there exists $b \in G$ such that

$$a\ o\ b = e = b\ o\ a.$$

e being the identity in G with respect to o.

Such an element b, usually denoted by a^{-1} is called the inverse of a. Thus $a^{-1}\ o\ a = e = a\ o\ a^{-1}$ for $a \in G$.

In the set of integers the inverse of an integer a with respect to ordinary addition operation is $-a$ and in the set of non-zero rational numbers, the inverse of a with respect to multiplication is $1/a$ which belongs to the set.

Algebraic Structure

A non-empty set G together with at least one binary operation defined on it is called an *algebraic structure*. Thus if G is a non-empty set and 'o' is a binary operation on G, then (G, o) is an algebraic structure.

$$(n, +), (I, +), (I, -), (R, +, .)$$

are all algebraic structures. Since addition and multiplication are both binary operations on the set R of real numbers, $(R, +, .)$ is an algebraic structure equipped with two operations.

Illustrative Examples

Example 2: If the binary operation o on Q the set of rational numbers is defined by

$$a\ o\ b = a + b - a\ b, \text{ for every } a, b \in Q$$

show that Q is commutative and associative.

Solution:

(i) 'o' is commutative in Q because if $a, b \in Q$, then

$$a\ o\ b = a + b - a\ b = b + a - b\ a = b\ o\ a.$$

(ii) 'o' is associative in Q because if $a, b, c \in Q$ then

$$\begin{aligned} a\ o\ (b\ o\ c) &= a\ o\ (b + c - b\ c) \\ &= a + (b + c - b\ c) - a\ (b + c - b\ c) \\ &= a + b - a\ b + c - (a + b - a\ b)\ c \\ &= (a\ o\ b)\ oc. \end{aligned}$$

Example 3: Given that $S = \{A, B, C, D\}$ where $A = \phi$, $B = \{a\}$, and $C = \{a, b\}$. $D = \{a, b, c\}$ show that S is closed under the binary operations $\cup$ (union of sets) and $\cap$ (intersection of sets) on S.

Notes

Solution:

(i) $A \cap B = \phi \cap \{a\} = \{a\} = B$

Similarly, $A \cap C = C$, $A \cap D$ and $A \cap A = A$.

Also, $B \cap B = B$, $B \cap C = \{a\} \cap \{a, b\} = \{a, b\} = C$,

$B \cap D = \{a\} \cap \{a, b, c\} = \{a, b, c\} = D$

$C \cap C = C$, $C \cap D = \{a, b\} \cap \{a, b, c\} = \{a, b, c\} = D$

Hence $\cap$ is a binary operation on S.

(ii) Again, $A \cup A = A$, $A \cup B = \phi \cup \{a\} = \phi = A$

$A \cup C = A$, $A \cup D = A$

and $B \cup B = B$, $B \cup C = \{a\} \cup \{a, b\} = \{a\} = B$

$B \cup D = \{a\} \cup \{a, b, c\} = \{a\} = B$

$C \cup C = C$, $C \cup D = \{a, b\} \cup \{a, b, c\}$

$= \{a, b\} = C$.

Hence $\cup$ is a binary operation on S.

Self Assessment

1. Show that multiplication is a binary operation on the set $A = \{1, -1\}$ but not on $B = \{1, 3\}$.
2. If $A = \{1, -1\}$ and $B = \{1, 2\}$, then show that multiplication is a binary operation on A but not on B.
3. If $S = \{A, B, C, D\}$ where $A = \phi$, $B = \{a, b\}$, $C = \{a, c\}$, $D = \{a, b, c\}$ show that $\cap$ is a binary operation on S but $\cup$ is not.

Group

Definition: *An algebraic structure (G, o) where G is a non-empty set with a binary operation 'o' defined on it is said to be a group, if the binary operation satisfies the following axioms (called group axioms).*

(G_1) ***Closure Axiom:*** G is closed under the operation o, i.e., $a \, o \, b \in G$, for all $a, b \in G$.

(G_2) ***Associative Axiom:*** The binary operation o is associative, i.e.,

$(a \, o \, b) \, o \, c = a \, o \, (b \, o \, c) \; \forall \, a, b, \in G$.

(G_3) ***Identity Axiom:*** There exists an element $e \in G$ such that

$e \, o \, a = a \, o \, e = a \; \forall \; a \in G$.

The element e is called the identity of 'o' in G.

(G_4) ***Inverse Axiom:*** Each element of G possesses inverse, i.e., for each element $a \in G$, there exists an element $b \in G$ such that

$$b \, o \, a = a \, o \, b = e.$$

The element b is then called the inverse of a with respect to 'o' and we write $b = a^{-1}$. Thus a^{-1} is an element of G such that

$$a^{-1} \, o \, a = a \, o \, a^{-1} = e.$$

Notes

Abelian Group of Commutative Group

A group (G, o) is said to be abelian or commutative if the composition 'o' is commutative, i.e., if

$$a \, o \, b = b \, o \, a \;\forall\; a, b \in G$$

A group which is not abelian is called non-abelian.

Examples:

(i) The structures $(N, +)$ and $(N, \times)$ are not groups i.e., the set of natural numbers considered with the addition composition or the multiplication composition, does not form a group. For, the postulate (G_3) and (G_4) in the former case, and (G_4) in the latter case, are not satisfied.

(ii) The structure $(Z, +)$ is a group, i.e., the set of integers with the addition composition is a group. This is so because addition in numbers is associative, the additive identity O belongs to Z, and the inverse of every element a, viz., $-a$ belongs to Z. This is known as *additive group of integers*.

The structure $(Z, \times)$, i.e., the set of integers with the multiplication composition does not form a group, as the axiom (G_4) is not satisfied.

(iii) The structures $(Q, +)$, $(R, +)$, $(C, +)$ are all groups i.e., the sets of rational numbers, real numbers, complex numbers, each with the additive composition, form a group.

But the same sets with the multiplication composition do not form a group, for the multiplicative inverse of the number zero does not exist in any of them.

(iv) The structure (Q_0, x) is a group, where Q_0 is the set of non-zero rational numbers. This is so because the operation is associative, the multiplicative identity 1 belongs to Q_0, and the multiplicative inverse of every element a in the set is $1/a$, which also belongs to Q_0. This is known as the *multiplicative group of non-zero rationals*.

Obviously (R_0, X) and (C_0, X) are groups, where R_0 and C_0 are respectively the sets of non-zero real numbers and non-zero complex numbers.

(v) The structure $(Q^+, \times)$ is a group, where Q^+ is the set of positive rational numbers. It can easily be seen that all the postulates of a group are satisfied.

Similarly, the structure $(R^+, \times)$ is a group, where R^+ is the set of positive real numbers.

(vi) The groups in (*ii*), (*iii*), (*iv*) and (*v*) above are all *abelian groups,* since addition and multiplication are both commutative operations in numbers.

Finite and Infinite Groups

If a group contains a finite number of distinct elements, it is called *finite group* otherwise an *infinite group*.

In other words, a group $(G, 0)$ is said to be finite or infinite according as the underlying set G is finite or infinite.

Order of a Group

The number of elements in a finite group is called the order of the group. An infinite group is said to be of infinite order.

Notes

Note: It should be noted that the smallest group for a given composition is the set $\{e\}$ consisting of the identity element e alone.

Illustrative Examples

Example 4: Show that the set of all integers ……, –4, –3, –2, –1, 0, 1, 2, 3, 4, … is an infinite abelian group with respect to the operation of addition of integers.

Solution: Let us test all the group axioms for abelian group.

(G_1) ***Closure Axiom:*** We know that the sum of any two integers is also an integer, i.e., for all $a, b \in I$, $a + b \in I$. Thus I is *closed* with respect to addition.

(G_2) ***Associativity:*** Since the addition of integers is associative, the associative—axiom is satisfied, i.e., for $a, b, c \in I$.

$$a + (b + c) = (a + b) + c$$

(G_3) ***Existence of Identity:*** We know that O is the additive identity and $O \in I$, i.e.,

$$O + a = a = a + O \forall\ a \in I$$

Hence additive identity exists.

(G_4) ***Existence of Inverse:*** If $a \in I$, then $-a \in I$. Also,

$$(-a) + a = O = a + (-a)$$

Thus every integer possesses additive inverse.

Therefore I is a group with respect to addition.

Since addition of integers is a *commutative operation*, therefore $a + b = b + a \forall\ a, b \in I$.

Hence $(I, +)$ is an *abelian group*. Also, I contains an infinite number of elements. Therefore $(I, +)$ is an abelian group of infinite order.

Example 5: Show that the set of all even integers (including zero) with additive property is an abelian group.

Solution: The set of all even integers (including zero) is

$$I = \{0, \pm 2, \pm 4, \pm 6\ldots\}$$

Now, we will discuss the group axioms one by one:

(G_1) The sum of two even integers is always an even integer, therefore *closure axiom* is satisfied.

(G_2) The addition is associative for even integers, hence *associative axiom* is satisfied.

(G_3) $O \in I$, which is an additive identity in I, hence identity axiom is satisfied.

(G_4) Inverse of an even integer a is the even integer $-a$ in the set, so *axiom of inverse* is satisfied.

(G_5) Commutative law is also satisfied for addition of even integers. Hence the set forms an abelian group.

Example 6: Show that the set of all non-zero rational numbers with respect to binary operation of multiplication is a group.

Notes

Solution: Let the given set be denoted by Q_0. Then by group axioms, we have—

(G_1) We know that the product of two non-zero rational numbers is also a non-zero rational number. Therefore Q_0 is closed with respect to multiplication. Hence, *closure axiom* is satisfied.

(G_2) We know for rational numbers.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \text{ for all } a, b, c \in Q_0$$

Hence, associative axiom is satisfied.

(G_3) Since, 1 the multiplicative identity is a rational number hence identity axiom is satisfied.

(G_4) If $a \in Q_0$, then obviously, $1/a \in Q_0$. Also

$$1/a \,.\, a = 1 = a \,.\, 1/a$$

so that $1/a$ is the multiplicative inverse of a. Thus *inverse axiom* is also satisfied.

Hence Q_0 is a group with respect to multiplication.

Example 7: Show that C, the set of all non-zero complex numbers is a multiplicative group.

Solution: Let $C = \{z : z = x + i\,y,\ x, y \in R\}$

Hence R is the set of all real numbers are $i = \sqrt{(-1)}$.

(G_1) ***Closure Axiom:*** If $a + i\,b \in C$ and $c + id \in c$, then by definition of multiplication of complex numbers

$$(a + i\,b)\{(c + i\,d) = (a\,c - b\,d) + i\,(a\,d + b\,c) \in C,$$

since $a\,c - b\,d, a\,d + b\,c \in R,$ *for* $a, b, c, d \in R$.

Therefore, C is closed under multiplication.

(G_2) ***Associative Axiom:***

$$(a + i\,b)\{(c + i\,d) \cdot (e + i\,f)\} = (a\,c\,e - a\,d\,f - b\,c\,f - b\,d\,e) + i\,(a\,c\,f + a\,d\,e + b\,c\,e - b\,d\,f)$$

$$= \{(a + i\,b) \cdot (c + i\,d)\} \cdot (e + i\,f)$$

for $a, b, c, d \in R$.

(G_3) ***Identity Axiom:*** $e = 1\ (= 1 + i_0)$ is the identity in C.

(G_4) ***Inverse Axiom:*** Let $(a + i\,b)\ (\neq 0) \in C$, then

$$(a + ib)^{-1} = \frac{1}{a + ib} = \frac{a - ib}{a^2 + b^2}$$

$$= \left(\frac{a}{a^2 + b^2}\right) + i\left(\frac{b}{a^2 + b^2}\right)$$

$$= m + i\,n \in C, \text{ Where } m = \left(\frac{a}{a^2 + b^2}\right),$$

Notes

$$n = -\frac{b}{a^2 + b^2} \in R.$$

Hence C is a multiplicative group.

Self Assessment

4. Show that the set of all odd integers with addition as operation is not a group.

5. Verify that the totality of all positive rationals form a group under the composition defined by

$$a \circ b = ab/2$$

6. Show that the set of all numbers $\cos\theta + i \sin\theta$ forms an infinite abelian group with respect to ordinary multiplication; where θ runs over all rational numbers.

Composition (Operation) Table

A binary operation in a finite set can completely be described by means of a table. This table is known as *composition table*. The composition table helps us to verify most of the properties satisfied by the binary operations.

This table can be formed as follows:

(i) Write the elements of the set (which are finite in number) in a row as well as in a column.

(ii) Write the element associated to the ordered pair (a_i, a_j) at the intersection of the row headed by a_i and the column headed by a_j. Thus (i^{th} entry on the left). (j^{th} entry on the top) = entry where the i^{th} row and j^{th} column intersect.

For example, the composition table for the group {0, 1, 2, 3, 4} for the operation of addition is given below:

	0	*1*	*2*	*3*	*4*
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

In the above example, the first element of the first row in the body of the table, 0 is obtained by adding the first element 0 of head row and the first element 0 of the head column. Similarly the third element of 4^{th} row (5) is obtained by adding the third element 2 of the head row and the fourth element of the head column and so on.

An operation represented by the composition table will be binary, if every entry of the composition table belongs to the given set. It is to be noted that composition table contains all possible combinations of two elements of the set will respect to the operation.

Notes:

(i) It should be noted that the elements of the set should be written in the same order both in top border and left border of the table, while preparing the composition table.

Notes

(ii) Generally a table which defines a binary operation '.' on a set is called *multiplication table*, when the operation is '+' the table is called an addition table.

Group Tables

The composition tables are useful in examining the following axioms in the manner explained below:

1. ***Closure Property:*** If all the elements of the table belong to the set G (say) then G is closed under the Composition o (say). If any of the elements of the table does not belong to the set, the set is not closed.
2. ***Existence of Identity:*** The element (in the vertical column) to the left of the row identical to the top row (border row) is called an identity element in the G with respect to operation 'o'.
3. ***Existence of Inverse:*** If we mark the identity elements in the table then the element at the top of the column passing through the identity element is the inverse of the element in the extreme left of the row passing through the identity element and vice versa.
4. ***Commutativity:*** If the table is such that the entries in every row coincide with the corresponding entries in the corresponding column i.e., the composition table is symmetrical about the principal or main diagonal, the composition is said to have satisfied the commutative axiom otherwise it is not commutative.

The process will be more clear with the help of following illustrative examples.

Illustrative Examples

Example 8: Prove that the set of cube roots of unity is an abelian finite group with respect to multiplication.

Solution: The set of cube roots of unity is $G = \{1, \omega, \omega^2\}$. Let us form the composition table as given below:

	I	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	$\omega^3 = 1$
ω^2	ω^2	$\omega^3 = 1$	$\omega^4 = \omega$

(G_1) ***Closure Axiom:*** Since each element obtained in the table is a unique element of the given set G, multiplication is a binary operation. Thus the closure axiom is satisfied.

(G_2) ***Associative Axiom:*** The elements of G are all complex numbers and we know that multiplication of complex number is always associative. Hence associative axiom is also satisfied.

(G_3) ***Identity Axiom:*** Since row 1 of the table is identical with the top border row of elements of the set, 1 (the element to the extreme left of this row) is the identity element in G.

(G_4) ***Inverse Axiom:*** The inverse of 1, ω, ω^2 are 1, ω^2 and ω respectively.

(G_5) ***Commutative Axiom:*** Multiplication is commutative in G because the elements equidistant with the main diagonal are equal to each other.

The number of elements in G is 3. Hence $(G,.)$ is a finite group of order 3.

Notes

Example 9: Prove that the set {1, –1, *i*, –*i*} is abelian multiplicative finite group of order 4.

Solution: Let G = {1, –1, *i*, –*i*}. The following will be the composition table for (G,.)

	1	–1	*i*	–*i*
1	1	–1	*i*	–*i*
–1	–*i*	1	–*i*	–*i*
i	*i*	–*i*	–1	1
–*i*	–*i*	*i*	1	–1

(G_1) ***Closure Axiom:*** Since all the entries in the composition table are elements of the set G, the set G is closed under the operation multiplication. Hence closure axiom is satisfied.

(G_2) ***Associative Axiom:*** Multiplication for complex numbers is always associative.

(G_3) ***Identity Axiom:*** Row 1 of the table is identical with that at the top border, hence the element 1 in the extreme left column heading row 1 is the identity element.

(G_4) ***Inverse Axiom:*** Inverse of 1 is 1. Inverse of –1 is –1. Inverse of *i* is –*i* and of –*i* is *i*. Hence inverse axiom is satisfied in G.

(G_5) ***Commutative Axiom:*** Since in the table the 1st row is identical with 1st column, 2nd row is identical with the 2nd column, 3rd row is identical with the 3rd column and 4th row is identical with the 4th column, hence the multiplication in G is commutative.

The number of elements in G is 4. Hence G is an abelian finite group of order 4 with respect to multiplication.

General Properties of Groups

Theorem 1: The identity element of a group is unique.

Proof: Let us suppose e and e' are two identity elements of group G, with respect to operation o.

Then $e \; o \; e' = e$ if e' is identity.

and $e \; o \; e' = e'$ if e is identity.

But $e \; o \; e'$ is unique element of G, therefore,

$e \; o \; e' = e$ and $e \; o \; e' = e \Rightarrow e = e'$

Hence the identity element in a group is unique.

Theorem 2: The inverse of each element of a group is unique, i.e., in a group G with operation o' for every $a \in G$, there is only one element a^{-1} such that $a^{-1} oa = a \; o \; a^{-1} = e$, e being the identity.

Proof: Let a be any element of a group G and let e be the identity element. Suppose there exist a^{-1} and a' two inverses of a in G then

$$a^{-1} \; o \; a = e = a \; o \; a^{-1}$$

and $$a' \; o \; a = e = a' \; o \; a$$

Now, we have

$$a^{-1} \; o \; (a \; o \; a') = a^{-1} \; o \; e \text{ (since } a \; o \; a' = e)$$

Notes

$= a^{-1}$ (because e is identity)

Also, $(a^{-1} \, o \, a) \, o \, a' = e \, o \, a'$ (because $a^{-1} \, o \, a = e$)

$= a'$ (because e is identity)

But $a^{-1} \, o \, (ao \, a') = (a^{-1} \, oa) \, o \, a'$ as in a group composition is associative

$\therefore \quad a^{-1} = a'$.

Theorem 3: If the inverse of a is a^{-1} then the inverse of a^{-1} is a, i.e., $(a^{-1})^{-1} = a$.

Proof: If e is the identity element, we have

$a^{-1} \, o \, a = e$ (by definition of inverse)

$\Rightarrow (a^{-1})^1 \, o \, (a^{-1} \, o \, a) = (a^{-1})^{-1} \, o \, e$

[because $a^{-1} \in G \Rightarrow (a^{-1})^{-1} \in G$]

$\Rightarrow [(a^{-1})^{-1} \, o \, a^{-1}] \, o \, a = (a^{-1})^{-1}$

[because Composition in G is associative and e is identity element]

$\Rightarrow e \, o \, a = (a^{-1})^{-1}$

$\Rightarrow a = (a^{-1})^{-1}$

$\Rightarrow (a^{-1})^{-1} = a$.

Theorem 4: The inverse of the product of two elements of a group G is the product of the inverse taken in the reverse order i.e.,

$(a \, o \, b)^{-1} = b^{-1} \, o \, a^{-1} \; \forall \, a, b \in G$.

Proof: Let us suppose a and b are any two elements of G. If a^{-1} and b^{-1} are inverses of a and b respectively, then

$a^{-1} \, o \, a = e = a \, o \, b^{-1}$ (e being the identity element)

and $b^{-1} \, o \, b = e = b \, o \, b^{-1}$

Now, $(a \, o \, b) \, o \, b^{-1} \, o \, a^{-1} = [(a \, o \, b) \, ob^{-1}] \, o \, a^{-1}$ (by associativity)

$= [a \, o \, (b \, o \, b^{-1})] \, o \, a^{-1}$ (by associativity)

$= (a \, o \, e) \, o \, a^{-1}$ [because $b \, o \, b^{-1} = e$]

$= a \, o \, a^{-1}$ [because $a \, o \, e = a$]

$= e$ [because $a \, o \, a^{-1} =$]

Also $(b^{-1} \, o \, a^{-1}) \, o \, (aob) = b^{-1} \, o \, [a^{-1} \, o \, (a \, o \, b)]$ (by associativity)

$= b^{-1} \, o \, [(a^{-1} \, o \, a) \, ob]$

$= b^{-1} \, o \, (e \, o \, b)$ [because $a^{-1} \, o \, a = e$]

$= b^{-1} \, o \, b$ [because $e \, o \, b = b$]

$= e$.

Hence, we have

$(b^{-1} \, o \, a^{-1} \, o \, (a \, o \, b) = e = (a \, o \, b) \, o \, (b^{-1} \, o \, a^{-1})$

Therefore, by definition of inverse, we have

$(a \, o \, b)^{-1} = b^{-1} \, o \, a^{-1}$

Notes

This theorem can be generalised as:

if $a, b, c, \ldots k, l, m \in G$, then

$$(a \circ b \circ c \circ \ldots k \circ l \circ m)^{-1} = m^{-1} \circ l^{-1} \circ k^{-1} \circ .\ldots c^{-1} \circ b^{-1} \circ a^{-1}.$$

Theorem 5: Cancellation laws hold good in a group, i.e., if a, b, c, are any elements of G, then

$$a \circ b = a \circ c \Rightarrow b = c \qquad \text{(left cancellation law)}$$

and

$$b \circ a = c \circ a \Rightarrow b = c \qquad \text{(right cancellation law)}$$

Proof: Let $a \in G$. Then

$a \in G \Rightarrow a^{-1} \in G$ such that $a^{-1} \circ a = e$

$= a \circ a^{-1}$, where e is the identity element

Now, let us assume that

$a \circ b = a \circ c$

then $a \circ b = a \circ c \Rightarrow a^{-1} \circ (a \circ b) = a^{-1} \circ aoc$

$\Rightarrow (a^{-1} oa)\, ob = (a^{-1} oa)\, oc$ (by associative law)

$\Rightarrow eob = eoc$ (because $a^{-1} oa = e$)

$\Rightarrow b = c$.

Similarly, $b \circ a = c \circ a$

$\Rightarrow (boa) \circ a^{-1} = (coa) \circ a^{-1}$

$\Rightarrow bo\,(ao\, a^{-1}) = co\,(ao\, a^{-1})$

$\Rightarrow boe = coe$

$\Rightarrow b = c$.

Theorem 6: If G is a group with binary operation o and if a and b are any elements of G, then the linear equations

$$aox = b \text{ and } yoa = b$$

have unique solutions in G.

Proof: Now $a \in G \Rightarrow a^{-1} \in G$,

and $a^{-1} \in G, b \in G \Rightarrow a^{-1} ob \in G$.

Substituting $a^{-1} ob$ for x in the equation $aox = b$, we obtain

$a \circ (a^{-1} \circ b) = b$

$\Rightarrow (a \circ a^{-1}) \circ b = b$

$\Rightarrow e \circ b = b$

$\Rightarrow b = b$ [because e is identity]

Thus $x = a^{-1} ob$ is a solution of the equation $aox = b$.

To show that the solution is unique let us suppose that the equation $aox = b$ has two solutions given by

$$x = x_1 \text{ and } x = x_2$$

Notes

Then $aox_1 = b$ and aox_2

$\Rightarrow aox_1 = aox_2 = b$

$\Rightarrow x_1 = x_2$ (by left cancellation law)

In a similar manner, we can prove that the equation

$$y \, o \, a = b$$

has the unique solution

$$y = b \, o \, a^{-1}.$$

Theorem 7: If corresponding to any element $a \in G$; there is an element O_a which satisfies one of the conditions

$$a + O_a = a \text{ or } O_a + a = a$$

then it is necessary that $O_a = o$, where O_a is the identity element of the group.

Proof: Since o is the identity element,

We have

$$a + o = a \quad \ldots \text{(i)}$$

also, it is given that

$$a + O_a = a \quad \ldots \text{(ii)}$$

Hence, from (i) and (ii)

$$a + O_a = a + O$$

or $O_a = o$ (by left cancellation law)

Again, we have

$$o + a = a \quad \ldots \text{(iii)}$$

and $O_a + a = a$ (given) … (iv)

Hence, from (iii) and (iv), we get

$$O_a + a = o + a$$

so that $O_a = o$ (by right cancellation law.)

Modulo System

It is of common experience that railway time-table is fixed with the provision of 24 hours in a day and night. When we say that a particular train is arriving at 15 hours, it implies that the train will arrive at 3 p.m. according to our watch.

Thus all the timing starting from 12 to 23 hours correspond to one of 0, 1, 3… 11 o'clock as indicated in watches. In other words all integers from 12 to 23 one equivalent to one or the other of integers 0, 1, 2, 3, …, 11 with modulo 12. In saying like this the integers in question are divided into 12 classes.

In the manner described above the integer could be divided into 2 classes, or 5 classes or m (m being a positive integer) classes and then we would have written mod 2 or mod 5 or mod m. This system of representing integers is called modulo system.

Notes

Addition Modulo m

We shall now define a new type of addition known as "addition modulo m" and written as $a +_m b$ where a and b are any integers and m is a fixed positive integer.

By definition, we have

$$a +_m b = r, \quad 0 \le r \le m$$

where r is the least non-negative remainder when $a + b$, i.e., the ordinary sum of the a and b, is divided by m.

For example $5 +_6 3 = 2$, since $5 + 3 = 8 = 1\,(6) + 2$, i.e., 2 is the least non-negative remainder when $5 + 3$ is divided by 6.

Similarly, $5 +_7 2 = 0$, $4 +_3 2 = 0$; $3 +_3 1 = 1$, $15 +_5 7 = 2$.

Thus to find $a +_m b$, we add a and b in the ordinary way and then from the sum, we remove integral multiples of m in such a way that the remainder r is either 0 or a positive integer less than m.

When a and b are two integers such that $a - b$ is divisible by a fixed positive integer m, then we write

$$a = b \pmod m$$

which is read as "a is concurrent to b modulo m".

Thus $a = b \pmod m$ if $a - b$ is divisible by m. For example $13 = 3 \pmod 5$ since $13 - 3 = 10$ is divisible by 5, $5 = 5 \pmod 5$, $16 = 4 \pmod 6$; $-20 = 4 \pmod 6$

Multiplication Modulo p

We shall now define a new type of multiplication known as "multiplication modulo p" and written as $a \times_p b$ where a and b are any integers and p is a fixed positive integer.

$$a \times_p b = r,\ 0 \le r \le p,$$

where r is the least non-negative remainder when ab, i.e., the ordinary product of a and b, is divided by p. For example $4 \times_7 2 = 1$, since $4 \times 2 = 8 = 1(7) + 1$.

It can be easily shown that if $a = b \pmod p$ then $a \times_p C = b \times_p C$.

Additive Group of Integers Modulo m

The set $G = \{0, 1, 2, \ldots m - 1\}$ of first m non-negative integers is a group, the composition being addition reduced modulo m.

Closure Property: We have by definition of addition modulo m,

$$a +_m b = r$$

where r is the least non-negative remainder when the ordinary sum $a + b$ is divided by m. Obviously $0 \le r \le m - 1$. Therefore for all $a, b \in G$, we have $a +_m b \in G$ and thus G is closed with respect to the composition addition modulo m.

Associative Property: Let a, b, c be any arbitrary elements in G.

Then $\quad (a + b) +_m c = (a +_m b) +_m c$

$\therefore \quad b +_m c = b + c \pmod m$

Notes

= least non-negative remainder when $a + (b + c)$ is divisible by m

= least non-negative remainder when $(a + b) + c$ divided by m.

since $a + (b + c) = (a + b) + c$

$= (a + b) +_m c$ [by definition of $+m$]

$= (a +_m b) +_m c$ [$\therefore a + b = a +_m b \pmod m$]

'$+_m$' is an associative composition.

Existence of Identity Element: We have $0 \in G$. Also, if a is any element of G, then $0 +_m a = a + m^0$. Therefore 0 is the identity element.

Existence of Inverse: The inverse of 0 is 0 itself. If $r \in G$ and $r \neq 0$, then $m - r \in G$. Also $(m - r) +_m r = 0 = r + \widehat{m}\ (m - r)$. Therefore $(m - r)$ is the inverse of r.

Commutative Property: The composition '$+m$' is commutative also.

Since

$a +_m b$ = least non-negative remainder when $a + b$ is divided by m

= least non-negative remainder when $b + a$ is divided by m

$= b +_m a$.

The set G contains m elements.

Hence $(G, +m)$ is a finite abelian group of order m.

Multiplicative Group of Integers Modulo p where p is Prime

The set G of $(p - 1)$ integers 1, 2, 3, …, $p - 1$, p being prime, is a finite abelian group of order $p - 1$, the composition being multiplication modulo p.

Let $G = \{1, 2, 3, \ldots p - 1\}$ where p is prime.

Closure Property: Let a and b be any elements of G. Then $1 < a < p - 1$, $1 < b < p - 1$. Now by definition $a \times_p b = r$ where r is the least non-negative remainder when the ordinary product $a\,b$ is divided by p. Since p is prime, therefore $a\,b$ is not exactly divisible by p. Therefore r cannot be zero and w shall have $1 \leq r \leq p - 1$. Thus $a \times_p b \in G \forall\ a, b \in G$. Hence the closure axiom is satisfied.

Associative Law: a, b, c, be any arbitrary elements of G.

Then $a \times p^b \times p^c = a \times p^{(bc)}$ [$\therefore b \times_p C = bc \pmod p$]

= least non-negative remainder when $a\ (bc)$ is divided by p

= least non-negative remainder when $ab\ (c)$ is divided by p

$= (ab) \times_p C$

$= (a \times_p b) \times_p C$ [$\therefore ab = a \times pb \pmod p$]

$\therefore$ 'X'_p is an associative composition.

Existence of left identity: We have $1 \in G$. Also if a is any element of G, then $1 \times_p a = a$. Therefore 1 is the left identity.

Existence of left inverse: Let s be any member of G. Then $1 < s < p - 1$.

Notes

Let us consider the following $(p-1)$ products:

$$1 \times_p s,\ 2 \times_p s,\ 3 \times_p s,\ \ldots\ (p-1) \times_p s.$$

All these are elements of G. Also no two of these can be equal as shown below:

Let i and j be two unequal integers such that

$$1 \le i \le p-1, 1 \le j \le p-1 \text{ and } i > j$$

Then $i \times_p s = j \times_p s$

$\Rightarrow$ $i\,s$ and $j\,s$ leave the same least non-negative remainder when divided by p

$\Rightarrow$ $i\,s - j\,s$ is divisible by p

$\Rightarrow$ $(i-j)\,s$ is divisible by p.

Since $1 \le (i-j) < p-1$; $1 \le s \le p-1$ and p is prime, therefore $(i-j)\,s$ cannot be divided by p.

$\therefore$ $i \times_p s \times j \times_p s$.

Thus $1 \times_p s,\ 2 \times_p s,\ \ldots\ (p-1) \times_p S$ are $(p-1)$ distinct elements of the set G. Therefore one of these elements must be equal to 1.

Let $s' \times_p s = 1$. The s' is the left inverse of s.

Commutative Law: The composition 'Xp' is commutative, since

$$\begin{aligned} a \times_p b &= \text{least non-negative remainder when } ab \text{ is divisible by } p \\ &= \text{least non-negative remainder when } ba \text{ is divided by } p \\ &= b \times_p a \end{aligned}$$

$\therefore$ (G, X^p) is a finite abelian group of order $p-1$.

Theorem 8: The residue classes modulo form a finite group with respect to addition of residue classes

Proof: Let G be the set of residue classes (mod m), then

$$G = \{ \{0\}, \{1\}, \{2\}, \ldots \{r_1\}, \ldots \{r_2\}, \ldots \{m-1\} \}$$

or $$G = \{0, 1, 2, \ldots \{r_1\} \ldots \{r_2\} \ldots m-1 \pmod m\}$$

Closure axiom: $(r_1) + \{r_2\} = \{r_1 + r_2\}$

$= \{r\} \in G$ where r is the least positive integer obtained as remainder when $r_1 + r_2$ is divided by m $(0 \le r \le m)$.

Thus the closure axiom is satisfied.

Associative axiom: The addition is associative.

Identity axiom: $\{0\} \in G$) and $\{0\} + \{r\} = \{r\}$. Hence the identity for addition is $\{0\}$.

Inverse axiom: Since $\{m-r\} + \{r\} = \{m\} = \{0\}$, the additive inverse of the element $\{r\}$ is $\{m-r\}$.

Hence G is a finite group with respect to addition modulo m.

Theorem 9: The set of non-zero residue classes modulo p, where p is a prime, forms a group with respect to multiplication of residue classes.

Proof: Let I = {…, –3, –2, –1, 0, 1, 2, 3, …} be the set of integers. Let $a \in$ then $\{a\}$ is residue class modulo p of I,

Notes

if $\{a\} = x : x \in I$ and $x - a$ is divisible by $p\}$.

If $p \mid a$ then $\{a\} = \{0\}$ which is called the zero residue class. Let G be the set of non-zero residue classes mod p (p being prime) then

$$G = \{1, 2, 3, \ldots (p - 1)\}$$

Closure axiom: Let $r_1, r_2 \in G$ then $r_1 \cdot r_2 = r \pmod{p}$

where r is the least non-negative integer such that $0 < r < p - 1$ obtained after dividing r_1, r_2 by p.

Also, since p is prime, r_1, r_2 is not divisible by p. Hence r cannot be zero.

Hence, $r_1 \cdot r_2 = r \in G$.

Thus closure axiom is satisfied.

Associative axiom: Multiplication of residue classes is associative.

Existence of Identity: $1 \in G$ and $a.\ 1 = 1\ a = a\ \forall\ a \in G$.

Therefore 1 is the identity element in G with respect to multiplication.

Existence of Inverse: Let $s \in G$ then $1 \le s \le p - 1$. Let us consider following $(p - 1)$ elements.

$$1 \cdot s, 2 \cdot s, 3 \cdot s, \ldots, (p-1) \cdot s .$$

All these elements are elements of G because the closure law is true. All these elements are distinct as otherwise if

$$i \cdot s = j \cdot s \text{ for } i \neq j \text{ and } i, j \in G$$

the $i \cdot s = j \cdot s \Rightarrow i \cdot s - j \cdot s$ is divisible by p

$\Rightarrow (i - j) \cdot s$ is divisible by p

$\Rightarrow (i - j)$ is divisible by p [because $1 \le s < (p-1)$]

$\Rightarrow i - j$ which is contrary to our assumption that $i \neq j$.

Therefore above $(p - 1)$ elements are the same as the elements of G. Hence some one of them should be 1 also, let $s' \cdot s = 1$ where $1 \le s' \le p - 1$. Hence s' is inverse of s. Hence inverse axiom is also satisfied.

$\therefore$ G is a group under multiplication mod p.

Note: Since $r \cdot s = s \cdot r\ \forall\ r, s \in G$.

G is finite abelian group of order $(p - 1)$.

Illustrative Examples

Example 10: Prove that the set $G = \{0, 1, 2, 3, 4\}$ is a finite abelian group of order 5 with respect to addition modulo 5.

Notes

Solution: Let us prepare a composition table as given below:

+ *(mod 5)*	*0*	*1*	*2*	*3*	*4*
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Closure Property: All the entries in the composition table are elements of the set *G*. Hence G is closed under addition modulo 5.

Associative Property: Addition modulo 5 is associative always.

Identity: $0 \in G$ is the identity element.

Inverse: It is clear from composition table.

Element	–	0	1	2	3	4
Inverse	–	0	4	3	2	1

$\therefore$ Inverse exists for every element of *G*.

Commutative Law: The composition is commutative as the corresponding rows and columns is *G* are 5.

Hence {*G*, + (mod 5)} is a finite abelian group of order 5.

Example 11: Prove that the set $G = \{1, 2, 3, 4, 5, 6\}$ is a finite abelian group of order 5 with respect to multiplication modulo 7.

Solution: Let us prepare the following composition table:

X_7	*1*	*2*	*3*	*4*	*5*	*6*
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Closure Property: All the entries in the table are elements of *G*. Therefore *G* is closed with respect to multiplication modulo 7.

Associative Property: Multiplication modulo 7 is associative always.

Identity: Since first row of the table is identical to the row of elements of *G* in the horizontal border, the element to the left of first row in vertical border is identity element, i.e., 1 is identity element in *G* with respect to multiplication modulo 7.

Inverse: From the table it is obvious that inverses of 1, 2, 3, 4, 5, 6 are 1, 4, 5, 2, 3 and 6 respectively. Hence inverse of each element in *G* exists.

Notes

Commutative Property: The composition is commutative because the elements equidistant from principal diagonal are equal each to each.

The set G has 6 elements. Hence (G, X_7) is a finite abelian group of order 6.

Self Assessment

7. Show that the set {1, 2, 3, 4} does not form a group under 'addition modulo 5', but it forms a group under 'multiplication modulo 5'.
8. Prove that the set {0, 1, 2, 3} is a finite abelian group of order 4 under addition modulo 4 as composition.

1.3 Rings

The concept of a group has its origin in the set of mappings or permutations, of a set onto itself. So far we have considered sets with one binary operation only. But rings are the outcome of the motivation which arises from the fact that integers follow a definite pattern with respect to the addition and multiplication. Thus we now aim at studying *rings which are algebraic systems with two suitably restricted and related binary operations*.

Definition: An algebraic structure $(R, +, .)$ where R is a non-empty set and + and . are two defined operations in R, is called a ring if for all a, b, c in R, the following axioms are satisfied:

R_1 . $(R, +)$ is an abelian group, i.e.,

(R_{11}) $a + b \in R$ (closure law for addition)

(R_{12}) $(a + b) + c = a + (b + c)$ (associative law for addition)

(R_{13}) R has an identity, to be denoted by O, with respect to addition,

i.e., $a + 0 = a \ \forall \ a \in R$ (Existence of additive identity)

(R_{14}) There exists an additive inverse for every element in R, i.e., there exists an element $-a$ in R such that

$a + (-a) = 0 \ \forall \ a \in R$ (Existence of additive inverse)

(R_{15}) $a + b = b + a$ (Commutative law for addition)

R_2 $(R, .)$ is a semigroup, i.e.,

(R_{21}) $a \,.\, b \in R$ (Closure law for multiplication)

(R_{22}) $(a \,.\, b) \,.\, c = a \,.\, (b \,.\, c)$ (associative law for multiplication)

R_3 Multiplication is left as well as right distributive over addition, i.e.,

$$a \,.\, (b + c) = a \,.\, b + a \,.\, c$$

and $$(b + c) \,.\, a = b \,.\, a + c \,.\, a$$

Elementary Properties of a Ring

Theorem 10: If R is a ring, then for all $a, b \in R$.

(a) $a \,.\, 0 = 0 \,.\, a = 0$

(b) $a\,(-b) = (-a)\,b = -\,(ab)$

(c) $(-a)\,(-b) = ab$

Notes

Proof: (*a*) We know that

$$a0 = a(0 + 0) = a0 + a0 \vee a \in R \quad \text{(using distributive law)}$$

Since R is a group under addition, applying right cancellation law,

$$a0 = a0 + a0 \Rightarrow 0 + a0 = a0 + a0 \Rightarrow a0 = 0$$

Similarly, $0a = (0 + 0)a = 0a + 0a$ (using distributive law)

$\therefore$ $0 + 0a = 0a + 0a$ (because $0 + 0a = 0a$)

Applying right cancellation law for addition, we get

$$0 = 0a \text{ i.e., } 0a = 0$$

Thus $a0 = 0a = 0$.

(b) To prove that $a(-b) = -ab$ we would show that

$$ab + a(-b) = 0$$

We know that $a[b + (-b)] = a0$ [because $b + (-b) = 0$]

$= 0$ (with the virtue of result (*a*) above)

or $ab + a(-b) = 0$ (by distributive law)

$\therefore$ $a(-b) = -(ab)$.

Similarly, to show $(-a)b = -ab$, we must show that

$$ab + (-a)b = 0$$

But $ab + (-a)b = [a + (-a)]b = 0b = 0$

$\therefore$ $-(a)b = -(ab)$

Hence the result.

(c) Actually to prove $(-a)(-b) = ab$ is a special case of foregoing article. However its proof is given as under:

$(-a)(-b) = -[a(-b)]$ [by result *b*]

$= [-(ab)]$ [because $a(-b) = -ab$]

$= ab$

because $-(-x) = x$ is a consequence of the fact that in a group inverse of the inverse of an element is element itself.

Illustrative Examples

Example 12: Prove that the set of all rational numbers is a ring with respect to ordinary addition and multiplication.

Let Q be the set of all rational numbers.

R_1 $(Q, +)$ is abelian.

(R_{11}) Let $a, b \in Q$ then $a + b \in Q$ because sum of two rational numbers is a rational number.

Notes

(R_{12}) Let $a, b, c \in Q$ then

$$(a + b) + c = a + (b + c)$$

because associative law for addition holds.

(R_{13}) $0 \in Q$ and $0 + a = a + 0 = a \ \forall \ a \in Q$, i.e., 0 is the additive identity in Q.

(R_{14}) $\forall \ a \in Q, -a \in Q$ and $a + (-a) = 0$. Hence additive inverse in Q exists for each element in Q.

(R_{15}) Let $a, b \in Q$ then $a + b = b + a$ because addition is commutative for rationals.

R_2 $(Q, .)$ is a semi group.

(R_{21}) Since the product of two rational numbers is a rational number, $a, b \in Q \Rightarrow a \cdot b \in Q$.

(R_{22}) Multiplication in Q is associative.

R_3 Multiplication is left as well as right distributive over addition in the set of rational numbers, i.e.,

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(b + c) \cdot a = b \cdot a + c \cdot a,$$

for $a, b, c, \in Q$.

Hence $(Q, +, .)$ is a ring.

Example 13: A Gaussian integer is a complex number $a + ib$, where a and b are integers. Show that the set $J(i)$ of Gaussian integers forms a ring under ordinary addition and multiplication of complex numbers.

Solution: Let $a_1 + ib_1$ and $a_2 + ib_2$ be any two elements of $J(i)$ then

$$(a_1 + ib_1) + (a_2 + ib_2) = (a_1 + a_2) + i\,(b_1 + b_2)$$

$$= A + iB \text{ (say)}$$

and

$$(a_1 + ib_1) \,.\, (a_2 + ib_2) = (a_1a_2 - b_1b_2) + i\,(a_1b_2 + b_1a_2)$$

$$= C + i\,D \text{ (say)}$$

These are Gaussian integers and therefore $J(i)$ is closed under addition as well as multiplication of complex numbers.

Addition and multiplication are both associative and commutative compositions for complex numbers.

Also, multiplication distributes with respect to addition.

$0 (= 0 + 0i) \in J(i)$ is the additive identity.

The additive inverse of $a + ib \in, J(i)$ is

$(-a) + (-b)\, i \in J(i)$ is

$(a + ib) + (-a) + (-b)\, i$

$= (a - a) + (b - b)\, i$

$= 0 + 0i = 0.$

The Gaussian integer $1 + 0.i$ is multiplicative identity.

Notes

Therefore, the set of Gaussian integers is a commutative ring with unity as multiplicative identity.

Example 14: Prove that the set of all real numbers of the form $m+n\sqrt{2}$ where *m, n* are rational numbers is a ring under the usual addition and multiplication.

Solution: Let $R = \{ m+n\sqrt{2} : m, n \text{ are real numbers}\}$.

R_1 $(R, +)$ is abelian group.

(R_{11}) Let , $m_1+n_1\sqrt{2}, m_2+n_2\sqrt{2} \in R$ then

$$(m_1+n_1\sqrt{2})+(m_2+n_2\sqrt{2}) = (m_1+m_2)+(n_1+n_2)\sqrt{2} \in R$$

because sum of two real numbers is a real number.

$$(R_{12})\,(m_1+n_1\sqrt{2})+(m_2+n_2\sqrt{2}) = (m_1+n_2\sqrt{2})\,(m_1+n_2\sqrt{2})\,(m_1+n_2\sqrt{2})$$

because addition of real numbers is a real number

(R_{13}) Associative law for addition of real numbers holds, i.e.,

$$(m_1+n_1\sqrt{2})+\{(m_2+n_2\sqrt{2})+(m_3+m_3\sqrt{2})\}$$

$$= \{(m_1+n_1\sqrt{2}+(m_2+n_2\sqrt{2})\}+(m_3+m_3\sqrt{2})$$

for $m_n, n_1, m_2, n_2, m_3, n_3$ to be rational numbers.

(R_{14}) 0 $(=0+0.\sqrt{2})$ Î R is the identity of addition in R.

(R_{15}) Let $m+n\sqrt{2} \in R$, then – $(m+n\sqrt{2})$

$= -m-n\sqrt{2} \in R$ and also

$$(m+n\sqrt{2})+(-m-n\sqrt{2}) = (m-n)+(n-n)\sqrt{2} = 0$$

Hence additive inverse for each element in R exists in R.

R_2 $(R, .)$ is a semi-group.

(R_{21}) $(m_1+n_1\sqrt{2})\cdot(m_2+n_2\sqrt{2})$

$= (m_1m_2+2n_1n_2)+(m_1n_2+m_2n_1)\sqrt{2}$

$= a+b\sqrt{2} \in R$

as a and b being the sums of products of rational numbers are rational.

(R_{22}) Multiplication is associative in R, i.e.,

$$\{(m_1+n_1\sqrt{2})\,(m_2+n_2\sqrt{2})\}\cdot(m_3+n_3\sqrt{2})$$

$$= (m_1+n_1\sqrt{2})\,(m_2+n_2\sqrt{2})\cdot(m_3+n_3\sqrt{2})$$

R_3 Multiplication is left as well as right distributive over addition in R. Hence R is a ring under usual addition and multiplication.

Notes

Example 15: Prove that the set of residues {0, 1, 2, 3, 4} modulo 5 is using with respect to addition and multiplication of residue classes (mod 5).

Solution: Let $R = \{0, 1, 2, 3, 4\}$.

Addition and multiplication tables for the given set R, are as under

+ *mod 5*	*0*	*1*	*2*	*3*	*4*	*mod 5*	*0*	*1*	*2*	*3*	*4*
0	0	1	2	3	4	0	0	0	0	0	0
1	1	2	3	4	0	1	0	1	2	3	4
2	2	3	4	0	1	2	0	2	4	1	3
3	3	4	0	1	2	3	0				
4	4	0	1	2	3	4					

From the addition composition table following is clear:

(i) Since all the elements of the table belong to the set, it is closed under addition (mod 5).

(ii) Addition (mod 5) is always associative.

(iii) $0 \in R$ is the identity of addition.

(iv) The additive inverse of the elements 0, 1, 2, 3, 4 are 0, 4, 3, 2, 1 respectively.

(v) Since the elements equidistant from the principal diagonal are equal to each other, the addition (mod 5) is commutative.

Hence $(R, +)$ is an abelian group.

From the multiplication composition table, we see that $(R, .)$ is semi group, i.e., following axioms hold good.

(vi) Since all the elements of the table are in R, the set R is closed under multiplication (mod 5).

(vii) Multiplication (mod 5) is always associative.

(viii) The multiplication (mod 5) is left as well as right distributive over addition (mod 5).

Hence $(R, +, .)$ is a ring.

Example 16: Prove that the set of residue classes modulo the positive integer m is a ring with respect to addition and multiplication of residue classes (mod m).

Solution: Let $R = \{0, 1, 2, \ldots, r_1, \ldots, r_2, \ldots (m - 1) \text{ (mod } m)\}$

R_1 $(R, +)$ is an abelian group.

(i) Let $r_1, r_2 \in R$ then

where r is the remainder obtained after dividing $r_1 + r_2$ by m.

$\therefore$ R is closed under addition (mod m).

(ii) Addition is associative.

(iii) $O \in R$ is the identity element for addition in R.

(iv) Since $(m - r) + r = m = 0$, the additive inverse of $r \in R$ is $(m - r) \in R$.

Notes

(v) Addition is commutative.

R_2 $(R, .)$ is a semigroup, *i.e.,*

(vi) $r_1\ r_2 = r'\ (\text{mod}\ m) \in R$

r being the remainder obtained after dividing $r_1\ r_2$ by m if $r_1\ r_2 \geq m$.

(vii) $(r_1 \cdot r_2) \cdot r_3 = r_1 \cdot (r_2 \cdot r_3)\ \forall\ r_1, r_2, r_3, \in R$ i.e., multiplication is associative. R_3 Distributive axiom is satisfied, *i.e.,*

(viii) $r_1\ (r_2 + r_3) = r_1\ r_2 + r_1\ r_3$ and $(r_2 + r_3)\ r_1 = r_2\ r_1 + r_3\ r_1$ for $r_1\ r_2, r_3 \in R$.

Hence $(R, +, .)$ is a ring.

Special Types of Rings

Some special types of rings are discussed below:

1. ***Commutative Rings:*** A ring R is said to be a commutative, if the multiplication composition in R is commutative, i.e.,

$$ab = ba\ \forall\ a, b \in R.$$

2. ***Rings with Unit Element:*** A ring R is said to be a ring with unit element if R has a multiplicative identity, i.e., if there exists an element R denoted by 1, such that

$$1 \cdot a = a \cdot 1 = a\ \forall\ a \in R.$$

The ring of all $n \times n$ matrices with elements as integers (rational, real or complex numbers) is a ring with unity. The unity matrix

$$I_n = \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & 1 \end{bmatrix}$$

is the unity element of the ring.

3. ***Rings with or without Zero Divisors:*** While dealing with an arbitrary ring R, we may find elements a and b in R neither of which is zero, and their product may be zero. We call such elements *divisors of zero* or *zero divisors*.

Definition: A *ring elemen*t a $(\neq 0)$ is called a divisor of zero if there exists an element b $(\neq 0)$ in the ring such that either

$$ab = 0 \text{ or } ba = 0$$

We also say that a ring R is without zero divisors if the product of no. two non-zero elements of same is zero, i.e., if

$$ab = 0 \Rightarrow \text{either } a = 0 \text{ or } b = 0 \text{ or both } a = 0 \text{ and } b = 0.$$

Cancellation Laws in a Ring

We say that cancellation laws hold in a ring R if

$$ab = ac\ (a \neq 0) \Rightarrow b = c$$

and $ba = ca\ (a \neq 0) \Rightarrow b = c$ where *a, b, c,* are in R.

Thus in a ring with zero divisors, it is impossible to define a cancellation law.

Notes

Theorem 11: A ring has no divisor of zero if and only if the cancellation law s holds in R.

Proof: Suppose that R has no zero divisors. Let $a, b, c,$ be any three elements of R such that $a \neq 0$, $ab = ac$.

Now, $ab = ac \Rightarrow ab - ac = 0$

$\Rightarrow a(b - c) = 0$

$\Rightarrow b - c = 0$ (because R is without zero divisors and $a \neq 0$)

$\Rightarrow b = c$.

Thus the left cancellation law holds in R. Similarly, it can be shown that right cancellation law also holds in R.

Conversely, suppose that the cancellation laws hold in R.

Let $a, b \in R$ and if possible let $ab = 0$ with $a \neq 0$, $b \neq 0$ then $ab = a \cdot 0$ (because $a \cdot 0 = 0$)

Since $a \neq 0$, $ab = a \cdot 0 \Rightarrow b = 0$ (by left cancellation law)

Hence we get a contradiction to our assumption that $b \neq 0$ and therefore the theorem is established.

Division Ring

A ring is called a division ring if its non-zero elements form a group under multiplication.

Pseudo ring: A non-empty set R with binary operations '+' and '.' satisfying all the postulates of a ring except right and left distributive laws, is called a pseudo ring if

$$(a+b)\cdot(c+d) = a\cdot c + a\cdot d + b\cdot c + b\cdot d \text{ for all } a,b,c,d \in R$$

Subrings

Definition: *Let R be a ring. A non-empty subset S of the set R is said to be a subring of R if S is closed under addition and multiplication in R and S itself is a ring, for those operations.*

If R is any ring, then {0} and R are always subrings of R. These are said to be improper subrings. The subrings of R other than these two, if any, are said to be proper subrings of R.

Evidently, if S is a subring of a ring R, it is a sub group of the additive group R.

Theorem 12: The necessary and sufficient condition for a non-empty subset S of a ring R to be a subring of R are

(i) $a, b \in S \Rightarrow a - b \in S$,

(ii) $a, b \in S \Rightarrow ab \in S$.

Proof: To prove that the conditions are necessary let us suppose that S is a subring of R.

Obviously S is a group with respect to addition, therefore,

$$b \in S \Rightarrow -b \in S$$

Since S is closed under addition

$$a \in S, b \in S \Rightarrow a \in S, -b \in S \Rightarrow a + (-b) \in S$$

$$\Rightarrow a - b \in S.$$

Notes

Also S is closed with respect to multiplication,

$$a \in S, b \in S \Rightarrow ab \in S.$$

Now to prove that the conditions are sufficient suppose S is a non-empty subset of R for which the conditions (i) and (ii) are satisfied.

From condition (i)

$$a \in S \Rightarrow a - a \in S \Rightarrow 0 \in S.$$

Hence additive identity is in S.

Now $0 \in S, a \in S \Rightarrow -a \in S$

i.e., each element of S possesses additive inverse.

Let $a, b \in S$ then $-b \in S$ and then from condition (i)

$$a \in S, -b \in S \Rightarrow a - (-b) \in S \Rightarrow (a + b) \in S$$

Thus S is closed under addition. S being subset of R, associative and commutative laws hold in S. Therefore, $(S, +)$ is an abelian group.

From condition (ii) S is closed under multiplication.

Since S is a subset of R, the associative law for multiplication and distributive laws of multiplication over addition hold in S. Thus S is a subring of R.

Intersection of Subrings

Theorem 13: The intersection of two subrings is a subring.

Proof: Let S_1 and S_2 be two subrings of ring R.

Since $0 \in S_1$ and $0 \in S_2$ at least $0 \in S_1 \cap S_2$. Therefore $S_1 \cap S_2$ is non-empty.

Let $a, b \in S_1 \cap S_2$, then

$$a \in S_1 \cap S_2 \Rightarrow a \in S_1 \text{ and } a \in S_2$$

and $b \in S_1 \cap S_2 \Rightarrow b \in S_1$ and $b \in S_2$.

But S_1 and S_2 are subrings of R, therefore

$$a, b \in S_1 \Rightarrow a - b \in S_1 \text{ and } a\,b \in S_1.$$

and $$a, b \in S_2 \Rightarrow a - b \in S_2 \text{ and } a\,b \in S_2.$$

Consequently, $a, b \in S_1 \cap S_2 \Rightarrow a - b \in S_1 \cap S_2$ and $a\,b \in S_1 \cap S_2$.

Hence $S_1 \cap S_2$ is a subring of R.

Illustrative Examples

Example 17: If R is a ring with additive identity 0, then for all $a, b \in R$, prove that

$$a(b - c) = ab - ac$$

and $$(b - c)\,a = ba - ca.$$

Solution: We have, $a(b - c) = a[b + (-c)]$

$= ab + a(-c)$ [left distributive law]

Notes

$$= ab + [-(ac)]$$

$$= ab - ac.$$

Also, $(b - c)\, a = [b + (-c)]\, a$

$$= ba + (-c)\, a \qquad \text{(right distributive law)}$$

$$= ba + [-(ca)] = ba - ca.$$

Example 18: Suppose M is a ring of all 2×2 matrices with their elements as integers, the addition and multiplication of matrices being the two ring compositions. Then M is a ring with left zero-divisor.

Solution: The null matrix $O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the zero element of ring M.

$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ are two non-zero elements of M.

Now $AB = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0.$

Hence M is a ring with left zero divisor.

Example 19: Prove that the ring of integers is a ring without zero divisors.

Solution: Since the product of two non-zero integers is never zero, it is the ring without zero divisors.

Example 20: Prove that the ring of residue classes modulo a composite integer m possess proper zero divisors.

Solution: Let $m = ab$ i.e., a and b are two factors of m.

Then $ab \not\equiv 0 \pmod{m}$

But $a \not\equiv \pmod{m}$ and $b \not\equiv 0 \pmod{m}$.

Hence the residue classes $\{a\}$ and $\{b\}$ are proper zero-divisors.

Example 21: Prove that the totality R of all ordered pairs (a, b) of real numbers is a ring with zero divisors under the addition and multiplication defined as

$$(a, b) + (c, d) = (a + c, b + d),$$

$$(a, b)\,(c, d) = (ac, bd), \ \forall\ (a, b), (c, d) \in R.$$

Solution: First of all, we prove that R is ring. We have

$$(R_1) : [(a, b) + (c, d)] = (a + c, b + d) \in R$$

Hence R is closed for addition.

$$(R_1) : [(a, b) + (c, d)] + (e, f) = (a + c, b + d) + (e, f)$$

$$= ((a + c) + e, (b + d) + f)$$

Notes

$$= [a+(c+e), b+(d+f)]$$

[addition is associative in real numbers]

$$= (a,b)+(c+e, d+f)$$

$$= (a,b)+[(c+d)+(e,f)]$$

So the addition is associative in R

(R_3) : (0, 0) + (*a*, *b*) = (0 + *a*, 0 + *b*) = (*a*, *b*) $\forall$ (*a*, *b*) $\in$ *R*, so that (0, 0) is the additive identity in *R*.

(R_4) : $(-a,-b)+(a,b)=(-a+a,-b+b)=(0,0)$ so the additive inverse of (*a*, *b*), is (–*a*, –*b*) $\forall$ (*a*, *b*) $\in$ *R*.

(R_5) : (*a*, *b*) + (*c*, *d*) = (*a* + *c*, *b* + *d*)

$$= (c+a, d+b)$$

[because addition is commutative in real numbers]

$$= (c,d)+(a,b) \quad \forall \ (a, b), (c, d) \in R.$$

(R_6): [(*a*, *b*), (*c*, *d*)] [*e*, *f*]

$$= (ac, bd)(e,f)$$

$$= \{(ac)e,(bd)f\}$$

$$= \{a(c,e,b(d\ f)\}$$

[because ordinary multiplication is associative]

$$= (a,b)(c,e,d\ f)$$

$$= (a,b)[(c,d)(e,f)] \quad \forall \ (a,b)(c,d)(e,f) \in R\ .$$

(R_7) : $(a,b)[(c,d)+(e,f)]$

$$= (a,b)(c+e, d+f)$$

$$= (a\,c + a\,e, b\,d + b\,f) \qquad \text{(by distributive law of reals)}$$

$$= (a\,c\,b\,d),(a\,e, b\,f)$$

$$= (a\,b),(c,d)+(a,b)(e,f)\ .$$

Similarly

$$[(c\,d)+(e,f)](a,b)$$

$$= (c\,d)+(a,b)+(e,\ f)(a,b)\ .$$

Hence R is a ring.

Now, in order to show that *R* is a ring with zero divisors we must produce at least two non-zero elements whose product is zero. Clearly neither (*a*, 0) with $a \neq 0$ nor (0, *b*) with $b \neq 0$ is the zero element (additive identity) or *R* yet their product

$$(a,0)(0,b)=(a.0,0.b)=(0,0)$$

Notes

which is zero element in R.

Thus R is a ring with zero divisors.

It can also be verified that R is also a commutative ring with unity element (1, 1).

Example 22: Prove that M the set of all 2 × 2 matrices of the form

$$\begin{bmatrix} a+bi\ c\ +di \\ -c+di\ a-bi \end{bmatrix}, i=\sqrt{-1}$$

where *a, b, c, d* are real numbers, form a division ring.

Solution: Since I = $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in M$ is a ring with unity under matrix addition and multiplication.

Let A be a non-zero matrix in M, and let

$$A=\begin{bmatrix} a+bi\ c\ +di \\ -c+di\ a-bi \end{bmatrix}$$

where *a, b, c, d* are not all zero. Consider

$$B=\begin{bmatrix} \dfrac{a-bi}{a^2+b^2+c^2+d^2} & -\dfrac{c+di}{a^2+^2+c^2+d^2} \\ \dfrac{c-di}{a^2+b^2+c^2+d^2} & \dfrac{a+bi}{a^2+b^2+c^2+d^2} \end{bmatrix}$$

Evidently $B \in M$. Also $A\ B = B\ A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Thus every non-zero matrix of M is invertible. Hence M is a division ring.

Example 23: Prove that the set of integers is a subring of the ring of rational numbers.

Solution: Let I be the set of integers and Q the set of rational numbers.

Clearly $I \subset Q$ and $a,b \in I \Rightarrow a-b \in I$ and $a\,b \in I$

Therefore, I is a subring of Q.

Example 24: Show that the set of matrices $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ is a subring of the ring of 2 × 2 matrices with integral elements.

Solution: Let M be the set of matrices of the type $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$

Clearly $M \subset R$

Let $A=\begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}, B=\begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} \in M$ then

$A-B=\begin{bmatrix} a_1-a_2 & b_1-b_2 \\ 0 & c_1-c_2 \end{bmatrix} \in M$ and

Notes

also

$$A\,B=\begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}=\begin{bmatrix} a_1a_2 & a_1b_2\ b_2c_1 \\ 0 & c_1\ c_2 \end{bmatrix}\in M$$

$\therefore$ M is subring of R.

Self Assessment

9. Show that the set of even integers including zero is a commutative ring with zero-divisors under the usual addition and multiplication.

10. Prove that the ring R = {0, 1, 2, 3, 4, 5, 6, 7} under the addition and multiplication modulo 8 is a commutative ring without zero divisors.

11. Prove that set I of integers is a subring of R, the set of real numbers.

12. If a, b belong to a ring R and $(a + b)^2 = a^2 + 2ab + b^2$, then show that R is a commutative ring.

Ideals

Definition: Let $(R, +,.)$ be any ring and S a subring of R, then S is said to be right ideal of R if $a \in S, b \in R \Rightarrow a\,b \in S$ and left ideal of R if $a \in S, b \in R \Rightarrow b\,a \in S$.

Thus a non-empty subset S or R is said to be a ideal of R if:

(i) S is a subgroup of R under addition.

(ii) $\forall\ a \in S$ and $b \in R$, both $a\,b$ and $ba \in S$.

Principal Ideals: If R is a commutative ring with unity and $a \in R$, the ideal $\{ax : x \in R\}$ is called the principal ideal generated by a and is denoted by (a), thus (a) stands for the ideal generated by a.

Principal Ideal Ring: A commutative ring with unity for which every ideal is a principal ideal is said to be a principal ideal ring.

Prime Ideal: Let R be a commutative ring. An ideal P of ring R is said to be a prime ideal of R if

$$ab \in P, a, b \in R \Rightarrow a \in P \text{ or } b \in P\ .$$

Example 25: In the commutative ring of integers I, the ideal $P = \{5r : r \in I\}$ is a prime ideal since if $ab \in P$, then $5 \mid ab$ and consequently $5 \mid a$ or $5 \mid b$ as 5 is prime.

Integral Domain

Definition: A commutative ring with unity is said to be an integral domain if it has no zero-divisors. Alternatively a commutative ring R with unity is called an integral domain if for all $a, b \in R, a\,b = 0 \Rightarrow a = 0 \text{ or } b = 0$.

Examples:

(i) The set I of integers under usual addition and multiplication is an integral domain as for any two integers $a, b; ab = 0 \Rightarrow a = 0$ or $b = 0$.

(ii) Consider a ring R = {0, 1, 2, 3, 4, 5, 6, 7} under the addition and multiplication modulo 8. This ring is commutative but it is not integral domain because $2 \in R, 4 \in R$ are two non-zero elements such that 2.4 = 0 (mod 8).

Notes

Euclidean Rings

An integral domain R is said to be a Euclidean ring if for every $a \neq 0$ in R there is defined a non-negative integer, to be denoted by $d(a)$, such that:

(i) for all $a, b \in R$, both non-zero, $d(a) \leq d(ab)$,

(ii) for any $a, b \in R$, both non-zero, there exists $q, r \in R$ such that $a = qb + r$ when either $r = 0$ or $d(r) < d(b)$.

Illustrative Examples

Example 26: Prove that the ring of complex numbers C is an integral domain.

Solution: Let $J(i) = \{a + bi : a, b \in I\}$.

It is easy to prove that $J(i)$ is a commutative ring with unity.

The zero element $0 + 0.i$ and unit element $1 + 0.i$.

Also this ring is free from zero-divisors because the product of two non-zero complex numbers cannot be zero. Hence $J(i)$ is an integral domain.

Example 27: Prove that set of numbers of the form $a + b\sqrt{2}$ with a and b as integers is an integral domain with respect to ordinary addition and multiplication.

Solution: Let $D = \{a + b\sqrt{2} : a, b \in I\}$

(I_1) $(D, +)$ is an abelian group.

(I_{11}) Let $a_1 + b_1\sqrt{2} \in D$ and $a_2 + b_2\sqrt{2} \in D$, then $a_1, b_1, a_2, b_2 \in I$

Now, $(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in D$

as $a_1 + a_2, b_1 + b_2 \in I$.

Hence D is closed under addition.

(I_{12}) Addition is associative in the set of real numbers.

(I_{13}) $0 = (0 + 0\sqrt{2}) \in D$ is the additive identity in D because $0 \in I$.

(I_{14}) If $(a + b\sqrt{2}) \in D$

Then $(-a) + (-b)\sqrt{2} \in D$ and $(a + b\sqrt{2}) + [(-a) + (-b)\sqrt{2}] = 0 + 0\sqrt{2} = 0$ the additive identity. Hence each element in D possesses additive inverse.

(I_{15}) Addition is commutative in the set of real numbers.

I_2 $(D, .)$ is semi-abelian group with unity.

$(I_{21})(a_1 + b_2\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \in D$ as $a_1 + b_2 + 2b_1b_2, a_1b_1 \in I$ for $a_1, b_1, a_2, b_2 \in I$.

Notes

Hence D is closed under multiplication.

(I_{12}) Multiplication is commutative in the set of real numbers.

(I_{23}) Multiplication is associative in the set of real numbers.

(I_{24}) $1+0\sqrt{2}=1\in D$ and for $a+b\sqrt{2}\in D$, we have

$$(1+0\sqrt{2}(a+b\sqrt{2})=(a+b\sqrt{2})(I+0\sqrt{2})+a+b\sqrt{2}$$

$\therefore$ 1 is the multiplicative identity in D.

I_3. In the set of real numbers multiplication is distributive over addition.

I_4. Now, to prove that this ring is without zero divisors let $a+b\sqrt{2}$ and $c+d\sqrt{2}$ be two arbitrary elements of D. Then

$$(a+b\sqrt{2})(c+d\sqrt{2})=0 \Rightarrow ac+2bd=0 \text{ and } bc+ad=0$$

= either $a = 0$ and $b = 0$ or $c = 0$ and $d = 0$

= either $a+b\sqrt{2}$ or $c+d\sqrt{2} = 0$.

Thus the given set is a commutative ring with unity and without zero-divisors, i.e., it is an integral domain.

1.4 Fields

Definition: A commutative ring with unity is called a field if its every non-zero element possesses a multiplicative inverse.

Thus a ring R in which the elements of R different from 0 form an abelian group under multiplication is a field.

Hence, a set F, having at least two distinct elements together with two operations '+' and '.' is said to form a field if the following axioms are satisfied:

(F_1) $(F, +)$ is an abelian group.

(F_{11}) F is closed under addition, i.e., $\forall\ a,b\in F\Rightarrow a+b\in F$.

(F_{12}) Addition is commutative in F i.e., $(a+b)+c=a+(b+c)$

for all $a,b,c\in F$.

(F_{14}) Identity element with respect to addition exists in F, i.e., $\exists$, $0 \in$ F such that $a + 0 = 0 + a = a$ $\forall\ a \in F$.

(F_{15}) There exists inverse of every element of F, i.e., $\forall\ a \in F$, there exists an element $-a$ in F such that

$$a+(-a)=(-a)+a=0.$$

(F_{20}) Properties of $(F,.)$

(F_{21}) F is closed under multiplication, i.e., $\forall\ a,b\in F\Rightarrow a,b\in F$.

(F_{22}) Multiplication is commutative in F, i.e., $a\cdot b=b\cdot a$ for all $a, b, \in F$.

(F_{23}) Multiplication is associative in F, i.e., $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c, \in F$.

Notes

(F_{24}) There exists an identity element 1 for multiplication F such that

$$a \cdot 1 = 1 \cdot a = a \quad \forall \ a \in F.$$

(F_{25}) For all $a \in F$, $a \neq 0$, there exists an element a^{-1} (multiplicative inverse) in F such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

F_3. Distributive laws of multiplication over addition for all $a, b, c \in F$,

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

and

$$(b + c) \cdot a = b \cdot a + c \cdot a$$

The above properties can be summarised as:

(1) $(F, +)$ is an abelian group.

(2) $(F, .)$ is a semi-abelian group and $(F - \{0\}, .)$ is an abelian group.

(3) Multiplication is distributive over addition.

Examples:

(i) The set of real numbers is a field under usual addition and multiplication compositions.

(ii) The set of rational numbers is a field under usual addition and multiplication operations.

(iii) The set of integers is not a field.

Some Theorems

Theorem 14: The multiplicative inverse of a non-zero element of a field is unique.

Proof: Let there be two multiplicative inverse a^{-1} and a' for a non-zero element $a \in F$.

Let (1) be the unity of the field F.

$\therefore$ $aa^{-1} = 1$ and $a \cdot a' = 1$ so that $a \cdot a^{-1} = a \cdot a'$.

Since $F - \{0\}$ is a multiplicative group, applying left cancellation, we get $a^{-1} = a'$.

Theorem 15: A field is necessarily an integral domain.

Proof: Since a field is a commutative ring with unity, therefore, in order to show that every field is an integral domain we only need proving that a field is without zero divisors.

Let F be any field let $a, b \in F$ with $a \neq 0$ such that $ab = 0$. Let 1 be the unity of F. Since $a \neq 0$, a^{-1} exists in F and therefore,

$$ab = 0 \Rightarrow a^{-1}(ab) = a^{-1} 0$$

$$\Rightarrow (a^{-1} a)\, b = 0 \qquad \text{(because } a^{-1} a = 1\text{)}$$

$$\Rightarrow 1 \,.\, b = 0$$

$$\Rightarrow b = 0 \qquad \text{(because 1. } b = b\text{)}$$

Similarly if $b \neq 0$ then it can be shown that

$$ab = 0 \Rightarrow a = 0$$

Thus $ab = 0 \Rightarrow a = 0$ or $b = 0$.

Hence, a field is necessarily an integral domain.

Notes

Corollary: Since integral domain has no zero divisors and field is necessarily an integral domain, therefore, field has no zero-divisor.

Theorem 16: If a, b are any two elements of a field F and $a \neq 0$, there exists a unique element x such that $a \,.\, x = b$.

Proof: Let 1 be the unity of F and a^{-1}, the inverse of a in F then

$$a \,.\, (a^{-1}\, b) = (aa^{-1}) \,.\, b = 1 \,.\, b = b$$

$\therefore$ $$ax = b \Rightarrow a \,.\, x = a \,.\, (a^{-1}\, b)$$

$$\Rightarrow x = a^{-1}\, b \qquad \text{(by left cancellation)}$$

Thus $$x = a^{-1}\, b \in F.$$

Now, suppose there are two such elements x_1, x_2 (say) then

$$a \,.\, x_1 = b \text{ and } a \,.\, x_2 = b$$

Hence $a \,.\, x_1 = a \,.x_2$

On applying left cancellation, we get

$$x_1 = x_2$$

Hence the uniqueness is established.

Theorem 17: Every finite integral domain is a field.

or

A finite commutative ring with no zero divisor is a field.

Proof: Let D be an integral domain with a finite number of distinct elements $a_1, a_2, ..., a_n$. In order to prove that D is a field, we have to prove that there exists $1 \in D$ such that $1 \,.\, a = a \;\forall\; a \in D$ and for every $a\ (\neq 0) \in D$ there exists an element $a^{-1} \in D$ such that $a^{-1}\, a = 1$.

Let $a \neq 0$ and $a \in D$. Now the elements $aa_1 = aa_2, ..., aa_n$ are the elements of D.

All of them are distinct because otherwise if $aa_i = aa_j$, for $i \neq j$ then

$$aa_i = aa_j \Rightarrow a(a_i - a_j) = 0$$

$$\Rightarrow a_i - a_j = 0$$

(because $a \neq 0$ and D is without zero divisors)

$$\Rightarrow a_i = a_j \text{ contradicting } i \neq j.$$

Let one of these elements be a. Thus there exists an element, say $1 \in D$ such that

$a \,.\, 1 = a = 1 \,.\, a$ (because multiplication is commutative)

Let y be any element of D then for some $x \in D$ we should have

$$ax = y = xa$$

Therefore, $$1y = 1\,(ax) \qquad \text{(because } ax = y\text{)}$$

$$= (1a)\, x = ax \qquad \text{(because } 1a = a\text{)}$$

Notes

Thus $1y = y = y1 \forall\ y \in D = y1$. (because multiplication is commutative) Therefore 1 is the unit element of D.

Now $1 \in D$ and as such one of the elements $aa_1, aa_2, ..., aa_n$ is equal to 1, i.e.,

$$aa_s = 1 = a_s\ a \text{ for some } s \text{ such that } 1 \le s \le n.$$

Thus $a_s \in D$ is the multiplicative inverse of the non-zero element a in D. Since a is arbitrary element in D, we conclude that each non-zero element of D possesses multiplicative inverse.

Hence D is a field.

Illustrative Examples

Example 28: Prove that the set of complex numbers is a field with respect to addition and multiplication operation.

or

Let C be the set of ordered pairs (a, b) of real numbers. Define addition and multiplication in C by the equations

$$(a, b) + (c, d) = (a + c, b + d)$$

$$(a, b)\ (c, d) = (ac - bd, bc + ad)$$

Prove that C is a field.

Solution: C is closed under addition and multiplication since $a + c$, $b + d$, $ac - bd$, $bc + ad$ are all real numbers.

Let $(a, b), (c, d), (e, f) \in C$

then

$$\begin{aligned}[(a, b) + (c, d)] + (e, f) &= (a + c, b + d) + (e, f) \\ &= [(a + c) + e, (b + d) + f] \\ &= [a + (c + e), b + (d + f)] \\ &= (a, b) + (c + e, d + f) \\ &= (a, b) + [(c, d) + (e, f)]\end{aligned}$$

Hence addition is associative

Since
$$\begin{aligned}(a, b) + (c, d) &= (a + c, b + d) \\ &= (c + a, d + b) = (c, d) + (a, b)\end{aligned}$$

addition is commutative in C.

$(0, 0) \in C$ is additive identity in C as

$$(0, 0) + (a, b) = (0 + a, 0 + b) = (a, b) \forall\ (a, b) \in C.$$

Notes

If $(a, b) \in C$ then $(-a, -b) \in C$

and also $(-a, -b) + (a, b) = (-a + a, b + b) = (0, 0)$

Hence [(–*a*, –*b*) is the additive inverse, of (*a*, *b*)]

Also $[(a, b)(c, d)](e, f) = [(ac - bd, bc + ad)(e, f)]$

$= [(ac - bd)e - (bc + ad)f, (bc + ad)e + (ac - bd)f]$

$= [a(ce - df) - b(de + cf), b(ce - df) + a(de + cf)]$

$= (a, b)(ce - df, de + cf)$

$= (a, b)[(c, d)(e, f)]$

Hence multiplication is associative in *C*.

Distributive laws also hold in *C* because,

$(a, b)[(c, d) + (e, f)] = (a, b)(c + e, d + f)$

$= [a(c + e) - b(d + f), b(c + e) + a(d + f)]$

$= [(ac - bd) + (ac - bf), (bf + ad) + (be + af)]$

$= (ac - bd, bc + ad) + (ae - bf, be + af)$

$= (a, b)(c, d) + (a, b)(e, f)$

Similarly, it can be proved that multiplication is distributive over addition in *C* from right too.

Multiplication is commutative in *C* because

$(a, b)(c, d) = (ac - bd, bc + ad)$

$= (ca - db\ cb + da)$

$= (c, d)(a, b)$

Since (1, 0) ∈ *C* and also (1, 0) (*a*, *b*)

= (*a*, *b*) (1, 0) is multiplicative identity in *C*.

Multiplicative inverse for non-zero elements in *C* exists because if (*a*, *b*) is non-zero elements in *C* then *a* and *b* are not zero at a time.

Let (*c*, *d*) be the multiplicative inverse of (*a*, *b*) then

$(a, b)(c, d) = (1, 0)$

i.e. $[(ac - bd), (bc + ad)] = (1, 0)$

so that $ac - bd = 1, bc + ad = 0$

i.e., $c = \frac{a}{a^2 + b^2}, d = \frac{-b}{a^2 + b^2}$

Notes

Since $a \neq 0$ or $b \neq 0$, $a^2 + b^2 \neq 0$, i.e., C or d or both are non-zero real numbers.

Hence C is a field.

Note: The question could have been done by assuming the elements of C as $a + ib$ etc. also.

Example 29: Show that the set of numbers of the form $a+b\sqrt{2}$ with a and b as rational numbers is a field.

Solution: Let $R = \{a+b\sqrt{2} : a,\ b \in Q\}$

$F_1(R, +)$ is a abelian group.

(F_{11}) Let $a_1+b_1\sqrt{2} \in R$ and $a_2+b_2\sqrt{2} \in R,$ then a_1, b_1, a_2, b_2 are the elements of Q, the set of rational numbers.

Now $(a_1+b_1\sqrt{2})+(a_2+b_2\sqrt{2}) = (a_1+a_2)+(b_1+b_2)\sqrt{2} \in R$ since $a_1+a_2, b_1+b_2 \in Q.$

Hence closure axiom for addition is satisfied.

(F_{12}) Addition is commutative for real numbers.

(F_{13}) Addition is associative for real numbers.

$(F_{14})\ 0+0\sqrt{2} = 0 \in R$ as $0 \in Q$, hence 0 is the identity of addition in R because

$$(0+0\sqrt{2})+(a+b\sqrt{2}) = (0+a)+(0+b\sqrt{2})$$

$$= a+b\sqrt{2} \forall\ a, b \in Q.$$

(F_{15}) If $a+b\sqrt{2} \in R$ then $(-a)+(-b)\sqrt{2} \in R$ and also

$$[(-a)+(-b)\sqrt{2}]+(a+b\sqrt{2})$$

$$= (-a+a)+(-b+b)\sqrt{2} = 0+0\sqrt{2}$$

$$= 0$$

$\therefore$ each element of R possesses additive inverse .

(F_2) Properties of field for $(F,)$

$(F_{21})\ (a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2})$

$$(a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1\sqrt{2}) \in R$$

Since $a_1a_2+2b_1b_2,\ a_1b_2+a_2b_1 \in Q$ for $a_1, a_2, b_1, b_2 \in Q.$

Thus R is closed under multiplication

(F_{22}) Multiplication in R is commutative

(F_{23}) Multiplication in R is associative

$(F_{24})\ 1+0\sqrt{2} = 1 \in R$ and $1\ (a+b\sqrt{2})$

$$= a+b\sqrt{2} \forall\ a, b \in Q.$$

Notes

$\therefore$ 1 is multiplicative identity in R.

(F_{22}) Let $a+b\sqrt{2} \neq 0,$ i.e., at least one of a and b is non-zero then

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2}$$

$$= A+B\sqrt{2} \in R, \text{ Where } A, B \in \text{Q}$$

and

$$A = \frac{a}{a^2-2b^2}, B = \frac{-b}{a^2-2b^2}$$

$a^2-2b^2 \neq 0$ as otherwise if $a = 0$, $b = 0$ which is impossible due to our assumption for non-zero element $a+b\sqrt{2}.$

Thus at least one of A and B is non-zero. Hence inverse of $a+b\sqrt{2}$ is a non-zero element $A+B\sqrt{2}$ in $R,$ because

$$\left(A+B\sqrt{2}\right)\left(a+b\sqrt{2}\right) = \frac{1}{(a+b\sqrt{2})}(a+b\sqrt{2}) = 1.$$

Thus every non-zero element in R possesses multiplicative inverse.

Hence R is a field.

Example 30: If the operations be addition and multiplication (mod p), prove that the set {0, 1, 2, ..., p – 1}, (mod p) where p is prime, is a field.

Solution: Let this set be denoted by $I \mid (p)$ which has already be shown a commutative ring with unity. To prove that $I \mid (p)$ is a field we will have to show that every non-zero element of $I \mid (p)$ is invertible. Let $r \in I(p)$ and $r \neq 0$.

Now $r \neq 0 \Rightarrow \cong 0 \pmod{p}$

$\Rightarrow r$ is not divisible by p

$\Rightarrow r$ and p are relatively prime.

i.e., there exist integers x, y such that $rx + py = 1$ implying that

$$rx \in 1 \pmod{p} \text{ as } py \equiv 0 \pmod{p}.$$

Thus x is inverse of r in $I \mid (p)$.

Hence $I \mid (p)$is a field.

Self Assessment

13. With addition and multiplication as operation prove that
    (i) The set {0, 1} (mod 2) is a field.
    (ii) The set {0, 1, 2} (mod 3) is a field.

Notes

14. Prove that the set of all real numbers of the form $u + \nu\sqrt{3}$ where u and ν are of the form $a + b\sqrt{2}$ in which a and b are rational numbers, is a field.
15. Prove that the set E of all even integers is a commutative ring but not a field.
16. Show that a finite commutative ring without zero divisors is a field.

1.5 Vector Spaces

Before giving a formal definition of an abstract vector space we define what is known as an external composition in one set over another. We have already defined a binary composition in a set A as a mapping of $A \times A$ to A. This may be referred to as an *internal composition* in A. Let now A and B be two non-empty sets. Then a mapping

$$f : A \times B \to B$$

is called an external composition in B over A.

Definition: Let $(F, +, .)$ be a field. Then a set V is called a vector space over the field F, if V is an abelian group under an operation which is denoted by $+$, and if for every $a \in F$, $u \in V$ there is defined an element $a\,u$ in V such that:

(i) $a(u + \nu) = au + a\nu$, for all $a \in F, u, \nu \in V$.

(ii) $(a + b)u = au + bu$, for all $a, b \in F, u \in V$.

(iii) $a(bu) = (ab)u$, for all $a, b \in F, u \in V$.

(iv) $1 . u = u . 1$ represents the unity element of F under multiplication.

The following notations will be constantly used in the forthcoming discussions.

(i) Generally F will be field whose elements shall often be referred to as *scalars*.

(ii) V will denote vector space over F whose elements shall be called as *vectors*.

Thus to test that V is a vector space over F, the following axioms should be satisfied.

V_1 $(V, +)$ is an abelian group.

(V_{11}) ***Closure law:*** $u, \nu \in V \Rightarrow u + \nu \in V$.

(V_{12}) ***Associative law:*** For all $u, \nu, w \in V \Rightarrow (u + \nu) + w = u + (\nu + w)$

(V_{13}) ***Existence of identity:*** There exists an element of zero vector.

(V_{14}) ***Existence of Inverse:*** For all $u \in V$, there exists a unique vector $-u \in V$ such that

$$u + (-u) = 0$$

(V_{15}) ***Commutative Law:***

$$u + \nu = \nu + u \text{ for } u, \nu \in V$$

V_2 scalar multiplication is distributive over addition in V, i.e.,

$$a(u + \nu) = au + a\nu, a \in F, \nu \in V$$

V_3 distributivity of scalar multiplication over addition in F, i.e.,

$$(a + b)u = au + bu, a, b \in F, u \in V.$$

Notes

V_4 Scalar multiplication is associative i.e.,

$$a(bu) = (ab)u \;\forall\; a, b \in F \text{ and } u \in V$$

V_5 ***Property of Unity:*** Let $1 \in F$ be the unity of F, then

$$1u = u = u \;|\; \forall\; u \in V$$

A vector space V over a field F is expressed by writing $V(F)$. Sometimes writing only V is sufficient provided the context makes it clear that which field has been considered.

If the field is R, the set of real numbers, then V is said to be real vector space. If the field is Q, the set of rational numbers, then V is said to be a rational vector space and if the field is C, the set of complex numbers V is called a complex vector space.

Illustrative Examples

Example 31: Show that the set of all vectors in a plane over the field of real numbers is a vector space.

Solution: Let V be the set of all Vectors in a plane and R be the field of real numbers.

(V_1) $(V, +)$ is an abelian group.

(V_{11}) $u, \nu \in V \Rightarrow u + \nu \in V$ (Closure axiom)

(V_{12}) $(u + \nu) + w = u + (\nu + w)$, for $u, \nu, w \in V$ (associative axiom)

(V_{13}) There is a null vector $O \in V$ such that

$u + 0 = u \;\forall\; u \in V$ (additive identity)

(V_{14}) If $u \in V, -u \in V$ and also $u + (-u) = 0$

Hence $-u$ is inverse of u in V, i.e., inverse axiom is satisfied for each element in V.

(V_{15}) $u + \nu = \nu + u$ for all $u, \nu, \in V$.

V_2 $a(u + \nu) = au + a\nu,\ a \in R, u, \nu \in V$

$V_3 (a + b)u = au + bu, a, b \in R, u \in V.$

$V_4 a(bu) = (ab)u,\ a,\ b \in R, u \in V.$

V_5 $1\ u = u, \;\forall\; u \in V,$ where 1 is unity of R.

Hence V is a vector space over R.

Example 32: Let C be the field of complex numbers and R be the field of real numbers, then prove that

(i) R is a vector space over R.

(ii) C is a vector space over C.

Notes

Solution:

(i) $V_1(R, +)$ is an abelian group as $(R, +)$ is a field.

$V_2\ \alpha(a+b) = \alpha\, a + \alpha\, b \ \forall\ \alpha \in R$ and $\forall\ a, b \in R$.

$V_3(\alpha+\beta)\, a = \alpha\, a + \beta\, a \ \forall\ \alpha, \beta \in R$ and $\forall\ a \in R$.

$V_4\alpha(\beta\, a) = (\alpha\, \beta)a, \forall\ \alpha, \beta \in R$ and $\forall\ a \in R$.

$V_5 1\ .\ a = a\ .\ 1 = a, 1 \in R$ and $\forall\ a \in R$.

Hence R is a vector space over R.

(ii) $V_1(C, +)$ is an abelian group because C is a field

$V_2\ \alpha(u+\nu) = \alpha\, u + \alpha\, \nu \ \forall\ \alpha \in C$ and $\forall\ u, \nu \in C$

(using left distributive law of multiplication over addition in C.)

$V_3.\ (\alpha+\beta)u = \alpha\, u + \beta\, u, \forall\ \alpha, \beta \in C$ and $\forall\ u \in C$.

(using right distributive law in C)

$V_4\alpha(\beta u) = (\alpha\, \beta)u, \forall\ \alpha, \beta \in C$ and $\forall\ u \in C$

(associative law of multiplication in C)

$V_5 1\ .\ u = u$ for $1 \in C$ for $\forall\ u \in C$.

Hence C is a vector space over the field C.

Example 33: A field K can be regarded as a vector space over any subfield H or K.

Solution: We consider K as a set of vectors. Let us regard the elements of the satisfied H as scalars.

Let addition of vectors be the composition in the field K. Let us define the scalar multiplication as follows:

If $a \in H$ and $\alpha \in K$, $a\ \alpha$ is the product of these two elements in the field K.

V_1 Since K is a field, therefore $(K, +)$ is an abelian group.

$$V_2 a(\alpha+\beta) = a\ \alpha + a\ \beta \ \forall\ a \in H \text{ and } \forall, \alpha, \beta \in K.$$

This is a consequence of the left distributive law in K because

$$a, \alpha, \beta \in K \qquad \text{(because } H < K \text{ and } a \in H\text{)}$$

$V_3(a+b)\alpha = a\ \alpha + b\ \alpha \ \forall\ a, b \in H$ and $\forall\ \alpha \in K$. This is due to the right distributive law in K.

$V_4(ab)\alpha = a(b\alpha) \ \forall\ a, b \in H$ and $\forall\ \alpha \in K$. This result is due to associativity of multiplication in K.

$V_5.\ 1\ .\ \alpha = \alpha \ \forall\ \alpha \in K$ where 1 is the unity of the subfield H. But $H \subset K$ and as such 1 is also the unity of the field K.

Hence K is a vector space over H.

General Properties of Vector Spaces

Notes

Let V be a vector space over a field F then

1. $a\,O = O$ for $a \in F, O \in V$
2. $O\nu = O$ for $O \in F, \nu \in V$
3. $a(-\nu) = (-\nu)a = -(a\nu)$ for $a \in F, \nu \in V$
4. $a(u - \nu) = au - a\nu$ for $a \in F, u$ and $\nu \in V$
5. If $a\nu = 0$ then either $a = 0$ or $V = 0$ for $a \in F, \nu \in V$.

Proof:

1. L.H.S $= a\,O$

   $= a\,(O + O)$ (because $O = O + O$)

   $= a\,O + a\,O$ (distributive law)

   Thus $aO = aO + aO$ or $aO + O = aO + aO$

   Hence by cancellation law we get

   $aO = O$.

2. L.H.S. $= O\nu = (O + O)\nu$ (because $O = 0 + 0$)

   $= 0\nu + 0\nu$ (distributive law)

   Thus $0\nu = 0\nu + 0\nu$

   or $0 + 0\nu = 0\nu + 0\nu$

   Hence by cancellation law

   $= 0\nu = 0.$

3. $a\nu + a(-\nu) = a(\nu - \nu) = a\,0 = 0$

   Therefore $a\,\nu$ is additive inverse of $a(-\nu)$.

   Again $a\,\nu + (-a)\nu = (\nu - \nu)a = Oa = 0.$

   Therefore $a\,\nu$ is additive inverse of $(-\nu)\,a$.

   i.e. $(-v)\,a = -av$

4. L.H.S. $= a(u - \nu)$

   $= a\,[u + (-\nu)]$

   $= au + a(-\nu)$ [by property (3)]

   $= a\,u - a\nu$

   $=$ R.H.S.

5. If $a = 0$ then the proposition is true.

   But if $a \neq 0$ then a^{-1} exists in F.

   $a\nu = 0 \Rightarrow a^{-1}(a\nu) = a^{-1}0 \Rightarrow (a^{-1}\,a)\nu$

   $= 0 \Rightarrow 1\,.\,\nu = 0 \Rightarrow \nu = 0.$

Notes

Cancellation

Let V be a vector space over a field F, then

(i) $a\nu = b\nu \Rightarrow a = b$ for $a, b \in F$ and $\nu \in V$, $\nu \neq 0$.

(ii) $au = a\nu \Rightarrow \nu = u$ for $a \in F\ a \neq 0$, and $u, \nu \in V$.

Proof:

(i) L.H.S. = $a\nu = b\nu$ or $a\nu - b\nu = 0$

or $(a-b)\,\nu = 0.$

Since $\nu \neq 0$, therefore, we must have

$a - b = 0$ or $a = b$

(ii) L.H.S. $au = a\nu$

or $a(u - \nu) = 0$

Since $a \neq 0$, we must have

$\nu - u = 0 \Rightarrow u = \nu$

Example 34: Let F be a field and let V be the totality of all ordered n-tuples $(\alpha_1, \alpha_2, ...\alpha_n)$ where $\alpha_1 \Sigma F$. Two elements $(\alpha_1, \alpha_2, ...\alpha_n)$ and $(\beta_1, \beta_2, ...\beta_n)$ of V are declared to be equal if and only if $\alpha_i = \beta_i$ for each i = 1, 2, ..., n. We now introduce the requisite operations in V to make of it a vector space by defining:

1. $(\alpha_1, \alpha_2, ...\alpha_n) + (\beta_1, \beta_2, ...\beta_n) = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, ..., \alpha_n + \beta_n)$

2. $a\ (\alpha_1, \alpha_2, ...\alpha_n) = (a\alpha_1, a\alpha_2, ...a\alpha_n)$ for $a \in F$

It is easy to verify that with these operations, V is a vector space over F.

Example 35: Let F be any field and let $V = F(x)$, the set of polynomials in x over F. We merely choose the fact that two polynomials can be added to get again a polynomial and that a polynomial can always be multiplied by an element of F. With these natural operations $F(x)$ is a vector space over F.

Example 36: The set of continuous real-valued functions on the real line is a real vector space with addition of functions $f + g$ and multiplication by real numbers as its laws of composition.

Example 37: The set of solution of the differential equation $\frac{d^2y}{dx^2} = -y$ is a real vector space.

Self Assessment

17. Show that the set W of ordered tried $(a_1, a_2, 0)$ where $a_1, a_2 \in F$ is a vector space.

18. Prove that the set $W = \{(x, 2y, 4z) : x, y, z \in R\}$ is a vector space.

Notes

19. In $F(x)$ let V_n be the set of all polynomials of degree less than n. Using the natural operations for polynomials of addition and multiplication by $a \in F$, show that V_n is a vector space over $F(x)$.

1.6 Summary

- The concept of set is fundamental in all branches of mathematics. A set according to the German mathematician George Cantor, is a *collection of definite well-defined objects of perception or thought*. By a well defined collection we mean that there exists a rule with the help of which it is possible to tell whether a given object belongs or does not belong to the given collection.
- Let A and B be two sets. The union of A and B is the set of all elements which are in set A or in set B. We denote the union of A and B by $A \cup B$, which is usually read as "A union B". On the other hand, the intersection of A and B is the set of all elements which are both in A and B. We denote the intersection of A and B by $A \cap B$, which is usually read as "A intersection B".
- The properties of natural numbers were developed in a logical manner for the first time by the Italian mathematician G. Peano, by starting from a minimum number of simple postulates. These simple properties, are known as the *Peano's Postulates* (*Axioms*).
- The system of rational numbers Q provides an extension of the system of integral Z, such that (*i*) $Q \supset Z$, (*ii*) addition and multiplication of two integers in Q have the same meanings as they have in Z and (*iii*) the subtraction and division operations are defined for any two numbers in Q, except for division by zero.

1.7 Keywords

Complex Number: The product set $R \times R$ consisting of the ordered pairs of real numbers.

Fields: A commutative ring with unity is called a field if its every non-zero element possesses a multiplicative inverse.

Irrational Number: A real number which cannot be put in the form p/q where p and q are integers.

Modulus of the Complex Number z: If $z = (a, b)$ be any complex number, then the non-negative real number $\sqrt{(a^2 + b^2)}$.

Operator or Transformation of A: If the domain and co-domain of a function f are both the same set say $f : A \to A$, then f is often called the operator.

Tabular form of the Set: Here the elements are separated by commas and are enclosed in brackets { }

1.8 Review Questions

1. Let S be a set of all real numbers of the form $(m + \sqrt{2}n)$ where $m, n \in Q$, a set of rational number, prove that S is a multiplication or additive group, m, n not vanishing simultaneously.

Notes

2. Prove that the four matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

form a multiplicative group.

3. If addition and multiplication modulo 10 is defined on the set of integers $R = \{0, 2, 4, 6, 8\}$.

Prove that the resulting system is a ring, Is it an integral domain?

4. Prove that the field has no proper ideals.
5. Show that the complex field C is a vector space over the real field R.

1.9 Further Readings

Books

I.N. Herstein *Topics in Algebra*.

Kenneth Hoffman and Ray Kunze, *Linear Algebra*

Michael Artin, *Algebra*

Notes

Unit 2: Vector Subspaces

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand the concept of a vector subspace
- Know more about subspaces by worked out examples
- See that a subspace has all the properties of a vector space.

Introduction

The unit one is the basis of the next five units. This unit is also based on the ideas of a vector space.

The subspace idea will help us in understanding the concepts of basis and dimension as well as how to set up the co-ordinates of a vector.

2.1 Vector Subspace

Let V be a vector space over a field F. Then a non-empty subset W of V is called a vector subspace of V if under the operations of V, W itself, is a vector space of F. In other words, W is a subspace of V whenever $w_1, w_2 \in W, \alpha, \beta \in F \Rightarrow \alpha w_1 + \beta w_2 \in W$.

Algebra of Subspaces

Theorem 1: The intersection of any two subspaces w_1 and w_2 of a vector space $V(F)$ is also a subspace of $V(F)$.

Proof: $w_1 \cap w_2$ is non-empty because at least $o \in w_1$ and w_2 both.

Let $u, v \in w_1 w_2$ and $\alpha, \beta \in F$

Then $u \in w_1 \cap w_2 \Rightarrow u \in w_1$ and $u \in w_2$

Notes

and $v \in w_1 \cap w_2 \Rightarrow v \in w_1$ and $v \in w_2$ since w_1 is subspace, hence

$\alpha, \beta \in F$ and $u, v \in w_1 \Rightarrow \alpha u + \beta v \in w_1$ and with the same argument

$\alpha, \beta \in F$ and $u, v \in w_2 \Rightarrow \alpha u + \beta v \in w_2$.

Therefore $\alpha u + \beta v \in w_1$ and $\alpha u + \beta v \in w_2$.

$\Rightarrow \alpha u + \beta v \in w_1 \cap w_2$.

Thus $w_1 \cap w_2$ is a subspace of $V(F)$.

Theorem 2: The union of two subspaces is a subspace if one is contained in the other.

Proof: Let W_1 and W_2 be two subspaces of a vector space V.

Let $W_1 \subset W_2$ or $W_2 \subset W_1$. Then $W_1 \cup W_2$ or W_1 (whichever is the case). Since W_1, W_2 are subspaces of $V, W_1 \cap W_2$ is also a subspace of V.

Conversely, suppose $W_1 \cup W_2$ is a subspace of V then we have to prove $W_1 < W_2$ or $W_2 < W_1$. Suppose it is not so, i.e., let us assume that W_1 is not a subset of W_2 and W_2 is also not a subset of W_1.

If W_1 is not a subset of W_2 then it implies that there exists

$$\alpha \in W_1 \text{ and } \alpha \notin W_2 \qquad \text{...(i)}$$

Similarly if W_2 is not a subset of W_1 then there exists

$$\beta \in W_2 \text{ and } \beta \notin W_1 \qquad \text{...(ii)}$$

From (i) and (ii) we see that

$\alpha \in W_1 \cup W_2$ and $\beta \in W_1 \cup W_2$ since $W_1 \cup W_2$ is a subspace of $V, \alpha + \beta \in W_1 \cup W_2$

But $\alpha + \beta \in W_1 \cup W_2 \Rightarrow (\alpha + \beta) \in W_1$ or W_2.

Suppose it belongs to W_1 then since $\alpha \in W_1$ and W_1 is a subspace of $V, (\alpha + \beta) - \alpha = \beta \in W_1$ which is contradiction. Similar contradiction is arrived by assuming $\alpha + \beta \in W_2$.

Therefore, either $W_1 \subset W_2$ or $W_2 \subset W_1$.

2.2 Illustrative Examples

Example 1: Prove that the set W of ordered tried $(a_1, a_2, 0)$ where $a_1, a_2 \in F$ is a subspace of $V_3(F)$,

Solution: Let $a = (a_1, a_2, 0)$ and $b = (b_1, b_2, 0)$ be two elements of W.

Therefore $a_1, a_2, b_1, b_2 \in F$. Let $a, b \in F$ then

Notes

$$a\alpha + b\beta = a(a_1, a_2, 0) + b(b_1, b_2, 0)$$

$$= (aa_1, aa_2, 0) + (bb_1, bb_2, 0)$$

$$= (aa_1 + bb_1, aa_2 + bb_2, 0) \in W$$

because $aa_1 + bb_1, aa_2 + bb_2 \in F$.

Therefore, W is a subspace of $V_3(F)$.

Example 2: Let R be the field of real numbers. Show that

$\{(x, 2y, 3z) : x, y, z \in R\}$ is a subspace of $V_3(R)$.

Solution: Let $W = \{(x, 2y, 3z) : x, y, z \in R\}$.

Let $\alpha = (x_1, 2y_1, 3z_1), \beta = (x_2, 2y_2, 3z_2)$ be any two elements of W then $x_1, y_1, z_1, x_2, y_2, z_2$ are obviously real numbers. If a, b are two real numbers, then

$$a\alpha + b\beta = a(x_1 + 2y_1 + 3z_1) + b(x_2 + 2y_2 + 3z_2)$$

$$= (ax_1 + bx_2, 2ay_1 + 2ay_2, 3az_1 + 3az_2)$$

which belongs of $W, ax_1 + bx_2, ay_1 + by_2$ and $az_1 + bz_2$ being real numbers.

Thus $\alpha, \beta \in R$ and $b \in W$

$$a\alpha + b\beta \in W.$$

i.e., W is subspace of $V_3(R)$.

Example 3: If V is any vector space, V is a subspace of V; the subset consisting of the zero vector alone is a space of V, and is called the zero subspace.

Example 4: An $n \times n$ matrix A over the field F is symmetric if $A_{ij} = A_{ji}$, for each i and j. The symmetric matrices form a subspace of the square of all $n \times n$ matrices over the field F.

Example 5: The space of polynomial functions over the field F is a subspace of the space of all functions from F into F.

Example 6: Let F be a subfield of the field C of complex numbers, and let V be the vector space of all 2 × 2 matrices over F. Let W_1 be the subset of V consisting of all matrices of the form

$$\begin{pmatrix} a & b \\ c & 0 \end{pmatrix}$$

Notes

where a, b, c are arbitrary scalars in F. Finally let W_2 be the subset of V consisting of all matrices of the form

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

where a, b are arbitrary scalars in F. Then W_1, W_2 are subspaces of V.

Example 7: The solution space of a system of homogeneous linear equations. Let us consider the simultaneous equations involving n unknown $x_i's$.

$$a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0$$

$$a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = 0$$

$$\begin{array}{ccc} . & . & . \\ . & . & . \\ . & . & . \\ . & . & . \\ . & . & . \end{array}$$

$$a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = 0$$

In matrix form we write the equation as

$$AX = 0$$

where A is a $m \times n$ matrix over the field F as all $a_{ij} \in A$ for i = 1 to m and j = 1 to n. Then the set of all $n \times 1$ matrices X over the field such that

$$AX = 0$$

is a subspace of the space of all $n \times 1$ matrices over F. To prove this we must show that

$$A(ax + y) = 0$$

when $AX = 0$ and $AY = 0$.

and C is an arbitrary scalar in F.

Consider a matrix A an $m \times n$ matrix over F and B and C are $n \times p$ matrices over F, then

$$A(a\,B + C) = a\,(AB) + AC$$

for each scalar a in F. Now

$$\left[A(aB+C)\right]_{ij} = \sum_k A_{ik}(aB+C)_{kj}$$

$$= \sum_k \left(aA_{ik}B_{kj} + A_{ik}C_{kj}\right)$$

$$= a\sum_k A_{ik}B_{kj} + \sum_k A_{ik}C_{kj}$$

$$= a(AB)_{ij} + (AC)_{ij}$$

$$= (aAB + AC)_{ij}$$

Similarly one can show that

Notes

$(aB+C)A = a(BA)+CA$, if the matrix sums and products are defined.

Thus $A(aX+Y) = a(AX)+AY = a(0)+0 = 0$

Theorem 3: Let V be a vector space over the field F. The intersection of any collection of subspaces of V is a subspace of V.

Proof: As shown in theorem 1, here let $\{W_a\}$ be a collection of subspaces of V, and let $W = \cap_a W_a$ be their intersection. Remember that W is defined as the set of all elements belonging to every W_a. Also since each W_a is a subspace, each contains the zero vector. Thus W is a non-empty set. Let u, v be vectors in W and $\alpha, \beta \in F$. Then

$u \in W, v \in W$

So $u, v \in W$ and $\alpha, \beta \in F$

Therefore $\alpha u + \beta v \in W$ since $\alpha u + \beta v$ is in all W_i's. Thus $W = \cap_a W_a$ is a subspace of $V(F)$.

Definition: Let S_1, S_2, ..., S_n are subsets of a vector space V, the set of all sums

$\alpha_1 + \alpha_2 + ... + \alpha_k$

of vectors $\alpha_i \in S_i$ is called the sum of the subsets $S_1, S_2, ...S_k$ and is denoted by

$S_1 + S_2 + ... + S_k$ or by $\sum_{i=1}^{k} S_i$.

If $W_1, W_2, W_3 ... W_k$ are subspaces of V, then the sum

$W = W_1 + W_2 + ... + W_k$

is easily seen to be a subspace of V which contains each of the subspaces W_i. From this it follows, that W is a subspace spanned by the union of $W_1, W_2, W_3 ... W_k$.

Example 8: Let F be a subfield of the field c of complex numbers. Suppose

$\alpha_1 = (1,2,0,3,0)$

$\alpha_2 = (0,0,1,4,0)$

$\alpha_3 = (0,0,0,0,1)$

Now a vector α is in the subspace W of F^5 spanned by $\alpha_1, \alpha_2, \alpha_3$ if and only if there exist scalars c_1, c_2, c_3 in F such that

$\alpha = c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3$

Thus W consists of all vectors of the form

$\alpha = (c_1, 2c_1, c_2, 3c_1 + 4c_2, c_3)$

Notes

Where c_1, c_2, c_3 are arbitrary scalars in F. Writing α the set of all 5-tuples

$$\alpha = (x_1, x_2, x_3, x_4, x_5)$$

with $x_i \in F$ such that

$$x_2 = 2x_1$$

$$x_4 = 3x_1 + 4x_2$$

It is clear that the vector $(-3,-6,1,-5,2)$ is in W, whereas $(2,4,6,7,8)$ is not in W.

Self Assessment

1. Let $V = R^3 = (x, y, z : x, y, z \in R)$ and let W be the set of all triples (x, y, z) such that $x - 3y + 4z = 0$

   Show that W is a subspace of V.

2. Prove that the set W of n-tuples $(x_1, x_2, ...x_{n-1}, 0)$ where all x's belong to F, is a subspace of the vector space $V_n(F)$.

3. Show that the set W of the elements of the vector space $V_3(R)$, of the form $(x + 2y, y, 3y - x), x, y \in R$, is a subspace of $V_3(R)$.

4. Let V be the space of all polynomial functions over F. Let S be the subset of V consisting of the polynomial functions $f_0, f_1, f_2, ...$ defined by

   $$f_n(x) = x^n, n = 0, 1, 2, ...$$

   Show that W is the subspace spanned by the set S.

5. Show that the vector $(3,-1,0,-1)$ is not in the subspace of R^4 spanned by the vectors $(2,-1,3,2), (-1,1,1,-3)$ and $(1,1,9,-5)$.

2.3 Summary

- If V is any vector space, V is a subspace of V; the subset consisting of the zero vector alone is a space of V, and is called the zero subspace.
- Let F be a subfield of the field C of complex numbers, and let V be the vector space of all 2 × 2 matrices over F. Let W_1 be the subset of V consisting of all matrices of the form

  $$\begin{pmatrix} a & b \\ c & 0 \end{pmatrix}$$

- Consider a matrix A an $m \times n$ matrix over F and B and C are $n \times p$ matrices over F, then

  $A(a\,B + C) = a\,(AB) + AC$

  for each scalar a in F.

Notes

- Let $S_1, S_2, ..., S_n$ are subsets of a vector space V, the set of all sums

  $\alpha_1 + \alpha_2 + ... + \alpha_k$

  of vectors $\alpha_i \in S_i$ is called the sum of the subsets $S_1, S_2, ...S_k$ and is denoted by

  $S_1 + S_2 + ... + S_k$ or by $\sum_{i=1}^{k} S_i$.

2.4 Keywords

Symmetric Matrix: An $n \times n$ matrix A over the field F is symmetric if $A_{ij} = A_{ji}$, for each i and j. The symmetric matrices form a subspace of the square of all $n \times n$ matrices over the field F.

Vector Subspace: Let V be a vector space over a field F. Then a non-empty subset W of V is called a vector subspace of V if under the operations of V, W itself, is a vector space of F.

2.5 Review Questions

1. Consider the three sets A,B,C such that

   $A = \{x_1, x_2; x_1 \le x_2\}$

   $B = \{x_1, x_2; x_1 x_2 \ge 0\}$

   $C = \{x_1, x_2; x_1 = x_2\}$

   which of these sets are subspace of $V(2)$? Give reasons.

2. Let $V = R^3 = [(x, y, z); x, y, z \in R]$ and Let W be the set of all triples (x, y, z) such that

   $2x - 3y + 4z = 0$

   Show that W is a subspace of V.

3. Let V be the vector space of functions from R into R let V_s be the subset of even functions $f(-x) = f(x)$; let V_0 be the subset of odd functions $f(-x) = -f(x)$. Then

   (a) Prove that V_s and V_0 are subspaces of V.

   (b) Prove that $V_s + V_0 = V$

   (c) Prove that $V_s \cap V_0 = \{0\}$ = null vector.

4. Let W_1 and W_2 be subspaces of a vector space V such that $W_1 + W_2 = V$ and $W_1 \cap W_2 = (0)$. Prove that for each α in V there are unique vectors α_1 in W_1 and α_2 in W_2 such that $\alpha = \alpha_1 + \alpha_2$.

Notes

2.6 Further Readings

Books

Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I. N. Herstein, *Topics in Algebra*

Michael Artin, *Algebra*

Notes

Unit 3: Bases and Dimensions of Vector Spaces

CONTENTS

Objectives

After studying this unit, you will be able to:

- See that in dealing with a finite dimensional vector space V over the F, we sometime enquire whether a set of vectors is dependent or independent set.
- Understand that if you find a set of vectors as independent set in a vector space V then this set of vectors forms the basis of the space V and the number of vectors in the sets defines the dimension of the space V.

Introduction

In this unit we explain the concept of linear dependence and linear independence of the set of vectors.

The number of independent set of vectors determines the dimension of the vector space and the set of independent vectors forms the basis of the vector space.

3.1 Linear Dependence and Linear Independence of Vectors

Linear Dependence: Let $V(F)$ be a vector space and let $S = \{u_1, u_2, ...u_n\}$ be a finite subset of V.

Then S is said to be linearly dependent if there exists scalars $\alpha_1, \alpha_2 ... \alpha_n \in F$, not all zero, such that

$$\alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_n u_n = 0.$$

Linear Independence: Let $V(F)$ be a vector space and let $S = \{u_1, u_2, ...u_n\}$ be finite subset of V. Then S is said to be linearly independent if

$$\sum_{i=1}^{n} a_u u_i = 0, \alpha_1 \in F.$$

holds only when $\alpha_i = 0, \qquad i = 1, 2, ...n.$

Notes

The following are easy consequences of the definition:

1. Any set which contains a linearly dependent set is linearly dependent.
2. Any subset of linearly independent set is linearly independent.
3. Any set which contains 0 vector is linearly dependent.
4. A set S of vectors is linearly independent if and only if each finite subset of S is linearly independent.

An infinite subset S of V is said to be linearly independent if every finite subset S is linearly independent, otherwise it is linearly dependent.

Illustrative Examples

Example 1: Show that the system of three vectors (1, 3, 2)(1, –7, –8), (2, 1, –1) of $V_3(R)$ is linearly dependent.

Solution: For $\alpha_1, \alpha_2, \alpha_3 \in R$ such that

$$\alpha_1(1,3,2) + \alpha_2(1,-7,-8) + \alpha_3(2,1,-1) = 0$$

$$\Leftrightarrow \quad (\alpha_1 + \alpha_2 + 2\alpha_3, 3\alpha_1 - 7\alpha_2 + \alpha_3, 2\alpha_1 - 8\alpha_2 - \alpha_3) = 0$$

$$\Leftrightarrow \quad \alpha_1 + \alpha_2 + 2\alpha_3 = 0, 3\alpha_1 - 7\alpha_2 + \alpha_3 = 0, 2\alpha_1 - 8\alpha_2 - \alpha_3 = 0$$

$$\Leftrightarrow \quad \alpha_1 = 3, \alpha_2 = 1, \alpha_3 = -2.$$

Therefore, the given system of vectors is linearly dependent.

Example 2: Consider the vector space $R^3(R)$ and the subset $S = \{(1,0,0),(0,1,0),(0,0,1)\}$ of R^3. Prove that S is linearly independent.

Solution: For $\alpha_1, \alpha_2, \alpha_3 \in R$,

$$\alpha_1(1,0,0) + \alpha_2(0,1,0) + \alpha_3(0,0,1) = (0,0,0)$$

$$\Leftrightarrow \quad (\alpha_1, \alpha_2, \alpha_3) = (0,0,0)$$

$$\Leftrightarrow \quad \alpha_1 = 0, \alpha_2 = 0, \alpha_3 = 0.$$

This shows that if any linear combination of elements of S is zero then the coefficients must be zero. S is linearly independent.

Example 3: Show that $\{1, x, 1 + x + x^2\}$ is a linearly independent set of vectors in the vector space of all polynomials over the real number field.

Solution: Let α, β, γ be scalar (real numbers) such that

$$\alpha(1) + \beta(x) + \gamma(1 + x + x^2) = 0 \text{ then}$$

$$\alpha + \beta x + \gamma(1 + x + x^2) = 0$$

$$\Rightarrow \quad \alpha + \gamma + (\beta + \gamma)x + \gamma x^2 = 0$$

$$\Rightarrow \quad \alpha + \gamma = 0, \beta + \gamma = 0, \gamma = 0,$$

Notes

$\Rightarrow \quad \alpha = 0, \beta = 0, \gamma = 0.$

Hence the vectors $1, x, 1+x+x^2$ are linear independent over the field of real numbers.

Example 4: If the set $S = \{\alpha_1, \alpha_2, ...\alpha_n\}$ of vectors of $V(F)$ is linearly independent, then none of the vectors $\alpha_1, \alpha_2, ...\alpha_n$ can be zero vector.

Solution: Let α_r be zero vector where $1 \le r \le n$ then

$$0\alpha_1 + 0\alpha_2 + ... + a\alpha_r + 0\alpha r + ... + 1 + 0\alpha_n = 0$$

for any $a \neq 0$ in F.

Since $a \neq 0$ we notice that S is linearly dependent. This is contrary to what is given.

Hence none of the vectors $\alpha_1, \alpha_2, ...\alpha_n$ can be a zero vector.

3.2 Basis and Dimension of a Vector Space

A subset S of a vector space $V(F)$ is said to be a basis of $V(F)$, if

(i) S consists of linearly independent vectors, and

(ii) S generates $V(F)$ i.e. $\xi(S) \in V$ i.e. each vector in V is a linear combination of the finite number of elements of S.

For example the set (1, 0, 0), (0, 1, 0), (0, 0, 1) is a basis of the vector space $V_3(R)$ over the field of real numbers.

The set $\beta = (v_1, v_2, v_3, \ldots, v_n)$ is a basis of V if every vector w in V can be written in a unique way as a combination $w = x_1v_1 + x_2v_2 + \ldots\ldots\ldots\ldots + x_nv_n$.

If every vector can be uniquely written as a combination, of the vectors $v_1, v_2, \ldots v_x$ of β, then β is independent and spans V, so β is a basis.

If V is a finite dimensional vector space, then it contains a finite set $v_1, v_2, \ldots, v_n$ of linearly independent elements that spans V.

If $v_1, v_2, \ldots v_n$ is a basis of V over F and if $w_1, w_2, \ldots w_m$ in V are linearly independent over F, then $m \le n$.

We also see that if V is finite-dimensional over F then any two basis of V has the same number of elements.

Thus for a finite dimensional space V, the basis has a unique number of elements say n. This unique integer, n; in fact, is the number of elements in any basis of V over F.

Definition: The integer n is called the dimension of the vector space over F.

The ***Dimension*** of a finite space V over F is thus the number of elements in any basis of V over F.

A vector space V is finite-dimensional if some finite set of vectors spans V. Otherwise V is infinite dimensional.

The dimension of V will be denoted by dim V.

If W is the subspace of a finite dimensional vector space V, then W is finite dimensional, and dim $W \le$ dim V. Moreover, dim W = dim V if and only if $W = V$.

Notes

Illustrative Examples

Example 5: Show that the set

$S = \{(1,2,1)(2,1,0),(1,-1,2)\}$ forms a basis for $V_3(F)$.

Solution: Let $a_1, a_2, a_3 \in F$.

then $a_1(1,2,1) + a_2(2,1,0) + a_3(1,-1,2) = 0$

$\Rightarrow \quad (a_1 + 2a_2 + a_3, 2a_1 + a_2 - a_3, a_1 + 2a_3) = (0,0,0)$

$\Rightarrow \quad a_1 + 2a_2 + a_3 = 0, 2a_1 + a_2 - a_3 = 0, a_1 + 2a_3 = 0$

$\Rightarrow \quad a_1 = a_2 = a_3 = 0.$

Hence the given set is linearly independent.

Now let $(1,0,0) \quad = x(1,2,1) + y(2,1,0) + z(1,-1,2)$

$$= (x + 2y + z, 2x + y - z, x + 2z)$$

so that $x + 2y + z = 1, 2x + y - z = 0, x + 2z = 0$

$\therefore \; x = -2/9, y = 5/9, z = 1/9$

Thus, the unit vector (1,0,0) is a linear combination of the vectors of the given set, i.e.

(1, 0, 0) = –2/9 (1, 2, 1) + 5/9(2, 1, 0) + 1/9 (1, –1, 2)

Similarly,

(0, 1, 0) = 4/9 (1, 2, 1) – 1/9(2, 1, 0) – 2/9 (1, –1, 2) and

(0, 0, 1) = 1/3 (1, 2, 1) – 1/3(2, 1, 0) + 1/3 (1, –1, 2)

Since $V_3(F)$ is generated by the unit vectors (1,0,0), (0,1,0),(0,0,1) we see therefore that ever elements of $V_3(F)$ is a linear combination of the given set S. Hence the vectors of this set form a basis of $V_3(F)$.

Example 6: Prove that system S consisting n vectors

$e_1 = \{1,0,...0\}, e_2 = \{0,1,...,0\} ... e_n = \{0,0,...1\}$ is a basis of $V_n(F)$.

Solution: First we shall prove that the given system S is linearly independent.

Let $a_1, a_2, \ldots a_n$ be any scalars, then

$a_1e_1 + a_2e_2 + \ldots a_ne_n = 0$

$\Rightarrow \quad a_1(1,0,...,0) + a_2(0,1,...0) + ... + a_n(0,0,...,1) = 0$

$\Rightarrow \quad (a_1, a_2, ...a_n) = 0$

$\Rightarrow \quad a_1 = 0, a_2 = 0, ...a_n = 0$

Notes

Therefore, S is linearly independent set.

Further, we must show that $L(S) = V_n(F)$.

Let $v = (v_1, v_2, ...v_n)$ be any vector in $V_n(F)$. We can write

$(v_1, v_2, ...v_n) = v_1(1,0,...,0) + v_2(0,1,...,0) + ... + v_n(0,0,...,1)$

i.e., $v = v_1e_1 + v_2e_2 + ... + v_ne_n$.

Hence S is a basis of $V_n(F)$.

Example 7: Prove that the vector space $F(x)$ of polynomials over the field F has a basis S, such that $S = \{1, x, x^2, ...\}$.

Solution: Let $a, b, c, ...$ be scalars such that

$a(1) + b(x) + c(x^2) + ... + = 0$

$\Rightarrow \quad a = 0, b = 0, c = 0, ...$

$\therefore$ the vectors $1, x, x^2, ...$ are linearly independent.

Let $f(x) = a_0 + a_1x + a_2x^2 + ... + a_ix^i$ be a polynomial in the given vector space then

$$f(x) = a_0(1) + a_1(x) + a_2(x^2) + ...a_i(x^i)$$

$\Rightarrow f(x)$ can be expressed as a linear combination of a finite number of elements of $\{1, x, x^2, ...\}$.

Thus $\{1, x, x^2, ...\}$ is a basis.

Self Assessment

1. Find the condition that the vectors (a_1, a_2) and (b_1, b_2) in $V_2(F)$ are linearly dependent.

   [***Ans:*** $a_1b_2 - a_2b_1 = 0$]

2. Test the linear dependence or independence of the vectors:

   (i) $\alpha_1 = (0,1,-2), \alpha_2 = (1,-1,1), \alpha_3 = (1,2,1)$ in $V_3(R)$

   (ii) $(1,2,3), (3,-2,1)(2,-6,5)$ in R^3

   (iii) $(1,0,-1), (2,1,3)(-1,0,0)(1,0,1)$ in $V_3(R)$.

   (iv) The set $\{(1,2,1), (3,1,5)(3,4,7)\}$

3. Is the vector $\alpha = (2,-5,-3)$ in $V_3(R)$, a linear combination of vectors.

   $\alpha_1 = (1,-3,2)$, $\alpha_2 = (2,-4,-1)$, $\alpha_3 = (1,-5,-7)$?

4. Prove that the number of elements in a basis of a finite dimensional vector space is unique.

Notes

5. If $\{e_1, e_2, e_3\}$ is a basis for R^3, then show that

   $\{e_2, e_3 + e_1, e_1 + e_2\}$ is also a basis.

6. Show that the set $S = \{(1,0,0)(1,1,0)(0,1,1),(0,1,0)\}$ spans $V_3(R)$, but does not form a basis.

7. Show that the set $\{(2,-1,0)(3,5,1)(1,1,2)\}$ forms a basis of $V_3(R)$.

3.3 Summary

- Let $V(F)$ be a vector space and let $S = \{u_1, u_2, ...u_n\}$ be a finite subset of V. Then S is said to be linearly dependent if there exists scalars $\alpha_1, \alpha_2 ... \alpha_n \in F$, not all zero, such that

  $\alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_n u_n = 0.$

- Let $V(F)$ be a vector space and let $S = \{u_1, u_2, ...u_n\}$ be finite subset of V. Then S is said to be linearly independent if

  $$\sum_{i=1}^{n} a_u u_i = 0, \alpha_1 \in F.$$

  holds only when $\alpha_i = 0,\ i = 1,2,...n.$

3.4 Keywords

Dimension: The Dimension of a finite space V over F is thus the number of elements in any basis of V over F.

Linear Combination: $V_3(F)$ is generated by the unit vectors (1,0,0), (0,1,0), (0,0,1) therefore that elements of $V_3(F)$ is a linear combination of the given set S.

3.5 Review Questions

1. Prove that a set of vectors containing null vector is a linearly dependent set.
2. Prove that the three functions $t^2, \cos x$ and e^x are linearly independent.
3. Prove that the set (1,2,0)(2,1,2)(3,1,1) is a basis for R^3.
4. Prove that if two vectors are linearly dependent, one of them is a scalar multiple of the other.

3.6 Further Readings

Books

Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I N Herstein, *Topics in Algebra*

Michael Artin, *Algebra*

Notes

Unit 4: Co-ordinates

CONTENTS

Objectives

After studying this unit, you will be able to:

- See that the dimension and basis of a vector space V over the field F help us in introducing the co-ordinates of a vector.
- Understand how to go from one basis to another basis with the help of an invertible matrix.
- See that the solved examples help you to find the invertible matrix and hence the co-ordinates of the vector in the new basis can be found out.

Introduction

For an abstract vector space V over the field F can be spanned by a set of independent vectors which form the basis of the vector space V.

There are more than one way of finding the basis and so it is important to know the relation between one basis over the other.

4.1 Co-ordinates

So far we have dealt with basis and dimension in the unit 3. We also showed the linear independence and dependence of vectors. The dimension of a vector space is the number of basis vectors of the vector space V over the field. The standard basis for a three dimensional vector space is taken as

$$l_1 = (1,0,0)$$

$$l_2 = (0,1,0)$$

$$l_3 = (0,0,1)$$

and they form an independent set of vectors and span the whole V_3 over the field R.

Notes

Now we want to introduce co-ordinates in the vector space V analogous to the natural co-ordinates x_i of the vector

$$\alpha = (x_1, x_2 ... x_n)$$

in the space F^n. The co-ordinates in the three dimensional space F^3 are x, y, z co-ordinates. So the co-ordinates of a vector α in V relative to the basis β will be the scalars which serve to express α as a linear combination of the vectors in the basis. If the vectors in the basis are $(\varepsilon_1, \varepsilon_2, \varepsilon_3, ... \varepsilon_n)$ then the vector α is expressible in terms of its co-ordinates as well as in terms of the vectors of basis as follows

$$\alpha = (x_1, x_2, x_3, ... x_n) = \sum_{i=1}^{n} x_i \varepsilon_i \qquad ...(1)$$

For another vector β having co-ordinates $y_1, y_2, ... y_n$ we have

$$\beta = (y_1, y_2, y_3, ... y_n) = \sum_{i=1}^{n} y_i \varepsilon_i .$$

writing

$$\alpha = (x_1, x_2, x_3, ... x_n)$$

the vector α has a unique expression as a linear combination of the standard basis vectors (1), and the i^{th} co-ordinates x_i of α is the coefficient of ε_i in the expression (1). By this way of 'natural' ordering of the vectors in the standard basis i.e. by writing ε_1 as the first vector, ε_2 as the second vector etc. we define the order of the co-ordinates of the vector α also. So we have the definition:

Definition: If V is a finite-dimensional space, the ordered basis for V is a finite sequence of basis vectors $(\varepsilon_1, \varepsilon_2, \varepsilon_3, ... \varepsilon_n)$ which is a linearly independent set and spans V. So we just say that

$$\beta = (\varepsilon_1, \varepsilon_2, \varepsilon_3, ... \varepsilon_n) \qquad ...(2)$$

is an ordered basis for V. Now suppose V is a finite dimensional vector space over the field F and (2) is an ordered basis for V, there is a unique n-tuple $\alpha = (x_1, x_2, ... x_n)$ of scalars such that:

$$\alpha = \sum_{i=1}^{n} x_i \varepsilon_i .$$

The n-tuple is unique, because if we also have

$$\alpha = \sum_{i=1}^{n} z_i \varepsilon_i$$

then $$\sum_{i=1}^{n} (x_i - z_i) \varepsilon_i = 0$$

Since ε_i for each i, is an independent set, so

$$x_i - z_i \equiv 0$$

or $$x_i = z_i$$

Notes

We shall call x_i, the i[th] co-ordinate of α relative to the basis

$$\beta = (\varepsilon_1, \varepsilon_2, \varepsilon_3, ...\varepsilon_n)$$

If γ is an other vector having ordered co-ordinates $(y_1, y_2, ...y_n)$, then

$$\gamma = (y_1, y_2, ...y_n) = \sum_{i=1}^{n} y_i \varepsilon_i,$$

then $$\alpha + \gamma = \sum_{i=1}^{n} x_i \varepsilon_i + \sum_{i=1}^{n} y_i \varepsilon_i$$

$$= \sum_{i=1}^{n} (x_i + y_i) \varepsilon_i \qquad ...(3)$$

So that the i^{th} co-ordinate of $(\alpha + \gamma)$ in this ordered basis is $(x_i + y_i)$. Similarly the i^{th} co-ordinate of $(c\alpha)$ is cx_i. It is clear that every n-tuple $(z_1, z_2, ...z_n)$ is V_n is the n-tuple of co-ordinates of some vector z in V_n namely the vector

$$z = \sum_{i=1}^{n} z_i \varepsilon_i \qquad ...(4)$$

4.2 Change of Basis from One Ordered Basis to Another

In a three dimensional space V_3, we have $\varepsilon_1 = (1,0,0), \varepsilon_2 = (0,1,0), \varepsilon_3 = (0,0,1)$ as three independent set of basis vectors. We also know that by taking a certain combination of these ε_i's we find another set like

$$\varepsilon_1' = (1,1,0), \varepsilon_2' = (1,1,1) \text{ and } \varepsilon_3' = (0,1,1) \qquad ...(4A)$$

which is again independent. The set $\varepsilon_1', \varepsilon_2', \varepsilon_3'$ is related to the set $\varepsilon_1, \varepsilon_2, \varepsilon_3$ by the relations

and
$$\left.\begin{aligned} \varepsilon_1' &= \varepsilon_1 + \varepsilon_2 \\ \varepsilon_2' &= \varepsilon_1 + \varepsilon_2 + \varepsilon_3 \\ \varepsilon_3' &= \varepsilon_2 + \varepsilon_3 \end{aligned}\right] \qquad ...(4B)$$

So by taking $\beta' = (\varepsilon_1', \varepsilon_2', \varepsilon_3')$ as a new basis of V_3 the vector α will have new co-ordinate system $\alpha = (x_1', x_2', x_3')$ given by

$$\alpha = \sum_{i=1}^{3} x_i' \varepsilon_i', \qquad ...(5)$$

We can now find a relation between the new co-ordinates (x_1', x_2', x_3') and old co-ordinates $(x_1, x_2, ..., x_n)$ of α in n dimensional space.

Notes

To find the relation, it is more convenient to use the matrix of α relative to the order basis

$$X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \qquad ...(6)$$

rather than the n-tuple $(x_1, x_2, ...x_n)$ of co-ordinates.

This notation will be particularly useful as we now proceed to describe what happens to the co-ordinates of a vector α as we change from one ordered basis to another.

Suppose that we are dealing with a space V which is n dimensional and that the basis β is changed to a new basis β' i.e.

$$\beta = (\varepsilon_1, \varepsilon_2, \varepsilon_3, ...\varepsilon_n), \beta' = (\varepsilon'_1, \varepsilon'_2, \varepsilon'_3, ...\varepsilon'_n) \qquad ...(7)$$

Let there be unique scalars P_{ij} such that

$$\varepsilon'_{ij} = \sum_{i=1}^{n} P_{ij}\varepsilon_i \qquad j = 1, 2, ...n \qquad ...(8)$$

Let $x'_1, x'_2, x'_3, ...x'_n$ be the co-ordinates of a given vector α in the basis β', then

$$\alpha = x'_1\varepsilon'_1 + x'_2\varepsilon'_2 + ...x'_n\varepsilon'_n$$

$$= \sum_{j=1}^{n} x'_j\varepsilon'_j$$

$$= \sum_{j=1}^{n} x'_j \sum_{i=1}^{n} P_{ij}\varepsilon_i$$

$$\text{or } \alpha = \sum_{j=1}^{n} \varepsilon_i \left(\sum_{j=1}^{n} P_{ij}x'_j \right) \qquad ...(8A)$$

Putting

$$x_i = \sum_{j=1}^{n} P_{ij}x'_j \qquad ...(9)$$

We have

$$\alpha = \sum_{i=1}^{n} x_i\varepsilon_i \qquad ...(10)$$

where now x_i denotes the i^{th} co-ordinate of the vector α in the old β.

In matrix form equation (9) becomes

$$X = PX' \qquad ...(11)$$

Notes

where $X = \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_n \end{bmatrix}, X' = \begin{bmatrix} \varepsilon_1' \\ \varepsilon_2' \\ \vdots \\ \varepsilon_n' \end{bmatrix}$

$$P = \left(P_{ij}\right) \qquad ...(12)$$

where P is an $n \times n$ matrix whose i,j entry is P_{ij} since β and β' basis are independent sets, $X = 0$ is only possible if $X' = 0$ also. Now the transformation matrix P is such that its inverse exists. Hence multiplying (6) by P^{-1} we obtain

$$X' = P^{-1}X \qquad ...(13)$$

So the new set of co-ordinates $\left(x_1', x_2', x_3', ...x_n'\right)$ are related to the old set of co-ordinates $\left(x_1, x_2, ...x_n\right)$ of the vector α by the relation (13).

Example 1: From equation (4), P matrix is given by

$$P = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

let $P = \begin{vmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{vmatrix} = -1$

Thus the new basis $\beta' = \left(\varepsilon_1', \varepsilon_2', \varepsilon_3'\right)$ is given in terms of old basis $\beta = \left(\varepsilon_1, \varepsilon_2, \varepsilon_3\right)$ by the matrix relation

$$\begin{pmatrix} \varepsilon_1' \\ \varepsilon_2' \\ \varepsilon_3' \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \varepsilon_3 \end{pmatrix} \qquad ...(14)$$

Now $$P^{-1} = \begin{pmatrix} 0 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 0 \end{pmatrix} \qquad ...(15)$$

If the co-ordinates of $\alpha = \left(x_1, x_2, x_3\right)$ in old basis β then in the new basis β' they are given by

$$\begin{pmatrix} x_1' \\ x_2' \\ x_3' \end{pmatrix} = \begin{pmatrix} 0 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \qquad ...(16)$$

Example 2: Show that the vectors $\varepsilon_1' = (1,1,0,0), \varepsilon_2' = (0,0,1,1), \varepsilon_3' = (1,0,0,4), \varepsilon_4' = (0,0,0,2)$ form a basis for R^4. Find the co-ordinates of each of the standard basis vectors in the ordered basis $\left(\varepsilon_1', \varepsilon_2', \varepsilon_3', \varepsilon_4'\right)$.

Solution: To prove that the set $\varepsilon_1', \varepsilon_2', \varepsilon_3', \varepsilon_4'$ form a basis, we have to show that they are independent. So let c_1, c_2, c_3, c_4 are scalars not all of them zero such that $\varepsilon_i' s$ are dependent, then

$$c_1\varepsilon_1' + c_2\varepsilon_2' + c_3\varepsilon_3' + c_4\varepsilon_4' = 0$$

Notes

or $c_1 + c_3 = 0$

$c_1 = 0$

$c_2 = 0$

$c_2 + 4c_3 + 2c_4 = 0$

So we get $c_1 = 0$

$c_2 = 0$

$c_3 = 0$

$c_4 = 0$

Thus the four set of vectors $\varepsilon_1', \varepsilon_2', \varepsilon_3', \varepsilon_4'$ are independent. Let P be a matrix such that

$$\begin{pmatrix} \varepsilon_1' \\ \varepsilon_2' \\ \varepsilon_3' \\ \varepsilon_4' \end{pmatrix} = P \begin{pmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \varepsilon_3 \\ \varepsilon_4 \end{pmatrix}$$

where
$$\varepsilon_1 = (1,0,0,0)$$
$$\varepsilon_2 = (0,1,0,0)$$
$$\varepsilon_3 = (0,0,1,0)$$
$$\varepsilon_4 = (0,0,0,1)$$

So $$P = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 4 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

Let $P = -2$, so, P is non-singular and invertible.

$$P^{-1} = \begin{pmatrix} 0 & 0 & 1 & -2 \\ 1 & 0 & -1 & 2 \\ 0 & 1 & 0 & -1/2 \\ 0 & 0 & 0 & 1/2 \end{pmatrix}$$

Thus $\varepsilon_1 = \varepsilon_3' - 2\varepsilon_4', \varepsilon_2 = \varepsilon_1' - \varepsilon_3' + 2\varepsilon_4'$

$\varepsilon_3 = \varepsilon_2' - \varepsilon_{4/2}', \varepsilon_4 = \varepsilon_{4/2}'$ is the answer.

Example 3: Let V be the vector space over the complex numbers of all functions from R into C i.e. the space of all complex-valued functions on the real line. Let $f_1(x) = 1, f_2(x) = e^{ix}, f^3(x) = e^{-1x}$.

(a) Prove that f_1, f_2, f_3 are linearly independent.

Notes

(b) Let $g_1(x)=1, g_2(x)=\cos x, g_3(x)=\sin x$. Find an invertible 3×3 matrix P such that

$$g_j=\sum_{i=1}^{3} P_{ij} f_i \qquad \text{for } j=1,2,3$$

Solution: Let $f_1(x), f_2(x), f_3(x)$ be a dependent set then we can find real c_1, c_2, c_3 not all of them zero so that

$$c_1 f_1(x)+c_2 f_2(x)+c_3 f_3(x)=0$$

or $$c_1.1+c_2 e^{ix}+c_3 e^{-ix}=0 \qquad ...(1)$$

Taking real part we have

$$c_1+c_2\cos x+c_3\cos x=0 \qquad ...(2)$$

Taking imaginary part we have

$$c_2-c_3=0 \qquad ...(3)$$

From (2) we have $c_1=0, c_2+c_3=0$ for arbitrary x,

From (3) we have $c_2=c_3$

So we get $c_1=c_2=c_3$.

which contradicts the statement that all *c*'s are not zero. So the set f_1, f_2, f_3 is an independent set.

So find g_1, g_2, g_3 in terms of $f_1(x), f_2(x), f_3(x)$ we see that

$$g_1(x)=f_1(x)=1$$

$$g_2(x)=\cos x=\frac{f_2(x)+f_3(x)}{2}$$

$$g_3(x)=\sin x=\frac{f_2(x)-f_3(x)}{2i}$$

Thus $$\begin{pmatrix} g_1(x) \\ g_2(x) \\ g_3(x) \end{pmatrix}=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1/2 & 1/2 \\ 0 & 1/2i & -1/2i \end{pmatrix}\begin{pmatrix} f_1(x) \\ f_2(x) \\ f_3(x) \end{pmatrix} \qquad ...(4)$$

Thus $$P=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1/2 & 1/2 \\ 0 & -i/2 & i/2 \end{pmatrix} \qquad ...(5)$$

Also Let $$P=\frac{2i}{4}=\frac{i}{2}\neq 0 \qquad ...(6)$$

So *P* is invertible 3 × 3 matrix given by (5).

Notes

Self Assessment

1. Find the co-ordinate matrix for the vector $\alpha = (1,0,1)$ in the basis of C^3 consisting of the vectors $(2i,1,0),(2,-1,1),(0,1+i,1-i)$ in that order.

2. Let $\beta' = (\varepsilon_1', \varepsilon_2', \varepsilon_3')$ be the ordered basis for R^3. Consisting of $\varepsilon_1' = (1,0,-1)$, $\varepsilon_2' = (1,1,1)$, $\varepsilon_3' = (1,0,0)$

   What are the co-ordinates of the vector $\alpha = (a,b,c)$ in the above ordered basis β'.

3. Let R be the field of the real numbers and let θ be a fixed real number. Let the new basis $\beta' = (\varepsilon_1', \varepsilon_2')$ be given in terms of the matrix P by the relation

   $$\begin{pmatrix} \varepsilon_1' \\ \varepsilon_2' \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \varepsilon_1 \\ \varepsilon_2 \end{pmatrix}$$

   Here $\varepsilon_1 = (1,0)$ and $\varepsilon_2 = (0,1)$

   $$P = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

   Find the co-ordinates of the vector $\alpha(x_1, x_2)$ in terms of the new basis β'.

4. Show that the set of vectors $\beta' = (\varepsilon_1', \varepsilon_2', \varepsilon_3')$ given by

   $\varepsilon_1' = (-1,0,0)$

   $\varepsilon_2' = (4,2,0)$

   $\varepsilon_3' = (5,-3,8)$

   form a basis of F^3. Find the co-ordinates of the vector $\alpha = (x_1, x_2, x_3)$ in the basis β'.

4.3 Summary

- The dimension of a vector space is the number of basis vectors of the vector space V over the field. The standard basis for a three dimensional vector space is taken as

  $l_1 = (1,0,0)$

  $l_2 = (0,1,0)$

  $l_3 = (0,0,1)$

  and they form an independent set of vectors and span the whole V_3 over the field R.

- The co-ordinates in the three dimensional space F^3 are x, y, z co-ordinates. So the co-ordinates of a vector α in V relative to the basis β will be the scalars which serve to express α as a linear combination of the vectors in the basis.

Notes

- If V is a finite-dimensional space, the ordered basis for V is a finite sequence of basis vectors $(\varepsilon_1, \varepsilon_2, \varepsilon_3, ...\varepsilon_n)$ which is a linearly independent set and spans V. So we just say that

  $$\beta = (\varepsilon_1, \varepsilon_2, \varepsilon_3, ...\varepsilon_n)$$

  is an ordered basis for V.

4.4 Keywords

n-tuple $(z_1, z_2, ...z_n)$**:** V_n is the n-tuple of co-ordinates of some vector z in V_n namely the vector

$$z = \sum_{i=1}^{n} z_i \varepsilon_i$$

Unique Scalars: P_{ij} are such that

$$\varepsilon_{ij}^{'} = \sum_{i=1}^{n} P_{ij} \varepsilon_i \qquad j = 1, 2, ...n$$

4.5 Review Questions

1. Show that the vectors

   $$\alpha_1 = (1,1,0,0), \alpha_2 = (1,0,0,4),$$
   $$\alpha_3 = (0,0,1,1), \alpha_4 = (0,0,0,2)$$

   form a basis for R^4. Find the co-ordinates of the standard basis vectors in the ordered basis $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$.

2. Let W be the subspace of C^2 spanned by $\alpha_1 = (1,0,i)$ and $\alpha_2 = (1+i,1,-1)$

   (a) Show that α_1 and α_2 form basis for W.

   (b) Show that the vectors $\beta_1 = (1,1,0)$ and $\beta_2 = (1,i,1+i)$ are in W and form an other basis for W.

   (c) What are the co-ordinates of α_1 and α_2 in the ordered basis (β_1, β_2) for W?

Answers: Self Assessment

1. $\left(-1, \frac{1+2i}{2}, \frac{3+i}{4}\right)$

2. $(b-c, b, a-2b+c)$

3. $x_1^{'} = \cos\theta x_1 + \sin\theta x_2$
   $x_2^{'} = -\sin\theta x_1 + \cos\theta x_2$

4. $\left(-x_1 + 2x_2 + \frac{11x_3}{8}, \frac{x_2}{2} + \frac{3x_3}{8}, \frac{x_3}{8}\right)$

Notes

4.6 Further Readings

Books

Kenneth Hoffman, Ray Kunze, *Linear Algebra*

Michael Artin, *Algebra*

Unit 5: Summary of Row-Equivalence

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand the technique of row operations on matrices of $m \times n$ type.
- Know that if B is a matrix obtained from row operations of A then B and A are called row equivalent.
- Understand how to obtain a row reduced echelon matrix.

Introduction

In solving a system of simultaneous equations the method of row operations on $m \times n$ matrix helps in finding the solution.

The idea of row space of a matrix helps in finding the subspace of the row space.

5.1 Matrices and Elementary Row Operations

Suppose F is a field. We consider the problem of finding x-scalars, $x_1, x_2, \ldots x_n$ which satisfy the conditions

$$\left.\begin{array}{ccccccccc} A_{11}x_1 & + & A_{12}x_2 & + & A_{13}x_3 & + \cdots + & A_{1n}x_n & = & y_1 \\ A_{21}x_1 & + & A_{22}x_2 & + & A_{23}x_3 & + \cdots + & A_{2n}x_n & = & y_2 \\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots \\ A_{m1}x_1 & + & A_{m2}x_2 & + & A_{m3}x_3 & + \cdots + & A_{mn}x_n & = & y_n \end{array}\right\} \quad \ldots (1)$$

where $y_1, \ldots y_m$ and A_{ij}, $l < i < m$, $i \leq j \leq n$ are given elements of F. We shall now abbreviate the system of equations (1) by

Notes

$$\left.\begin{aligned} &AX = Y \\ &A = \begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1} & A_{m2} & \cdots & A_{mn} \end{bmatrix} \\ \text{Where} \quad &X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}, Y = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} \end{aligned}\right\} \quad ...(2)$$

In solving the linear system of equations (1) we sometimes use the technique of elimination. We can illustrate this method on the following homogeneous equations:

$2x_1 - x_2 + x_3 = 0$

$x_1 + 3x_2 + 4x_3 = 0$

If we add (–2) times the second equation to the first equation,

we obtain

$-7x_2 - 7x_3 = 0$

or $x_2 = -x_3$

If we add (3) times the first equation to the second equation

we obtain

$7x_1 + 7x_3 = 0$

or $x_1 = -x_3$

So we conclude that if (x_1, x_2, x_3) is the solution then $x_1 = x_2 = -x_3$. Thus the set of solutions consists of all triples $(a, a, -a)$.

For the general system (1), suppose we select m, scalars $c_1, c_2, ...c_m$, multiply the jth equation by c_j and then add, we obtain the equations

$$(C_1A_{11} + ... + C_mA_{m1})x_1 + ... + (C_1A_{1n} + C_2A_{2n} + ... + C_mA_{mn})x_n = \sum_{j=1}^{m} C_j y_j$$

Such an equation is called a linear combination of the equations in (1). Evidently any solution of the entire system of equations (1) will also be the solution of this new equation. This is the fundamental idea of the elimination process. Thus if we have another system of linear equations

$$\left.\begin{array}{ccccccccc} B_{11}x_1 & + & B_{12}x_2 & + & \cdots & + & B_{1n}x_n & = & Z_1 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ B_{K1}x_1 & + & B_{K2}x_2 & & \cdots & & B_{Kn}x_n & = & Z_K \end{array}\right\} \quad ...(3)$$

in which each of the K equations is a linear combination of the equations (1), then every solution of (1) is a solution of the new system (2).

Notes

Let us say that two systems of linear equations are **equivalent** if each equation in each system is a linear combination of the equations in the other system. We then formally state the following theorem:

Theorem 1: Equivalent systems of linear equations have exactly the same solutions.

Consider now the system (1) as given by the system (2). We call A the matrix of coefficients of the system. We wish now to consider operations on the rows of the matrix A which correspond to forming linear combinations of the equations in the system $AX = Y$. We restrict ourselves to three **elementary row operations** on $m \times n$ matrix A over the field F:

1. Multiplication of one row of A by a non-zero scalar c;
2. Replacement of the r^{th} row of A by row r plus c times row s, c is any scalar and $r \neq s$;
3. interchange of two rows of A.

An elementary row operation is thus a special type of function (rule) e which is associated with each $m \times n$ matrix (A). One can precisely describe e in the three cases as follows:

1. $e(A)_{ij} = A_{ij}$ if $i \neq r$, $e(A)_{rj} = cA_{rj}$
2. $e(A)_{ij} = A_{ij}$ if $i \neq r$, $e(A)_{rj} + cA_{rj}$
3. $e(A)_{ij} = A_{ij}$ if i is different from r and s, $e(A)_{rj} = A_{si}$,

$$e(A)_{sj} = A_{rj}$$

A particular e is defined on the class of all m rowed matrices over F. One reason that we restrict ourselves to these simple types of row operations is that having performed such an operation e on a matrix A, we can recapture A by performing a similar operation on $e(A)$.

Definition: If A and B are $m \times n$ matrices over the field F, we say that B is **row-equivalent** to A if B is obtained from A by a finite sequence of elementary row operations. Consider the two systems of equations

$$AX = 0,$$

and $$BX = 0.$$

If matrix B is obtained from A by a finite sequence of elementary row operations we say that B matrix is row equivalent to A. Hence the above two system of equations are equivalent and so they have the same solutions.

Example 1: Consider

$$AX = 0$$

where $$A = \begin{pmatrix} -1 & i \\ -i & 3 \\ 1 & 2 \end{pmatrix}$$

so the system of equations is

$$-x_1 + ix_2 = 0$$

$$-ix_1 + 3x_2 = 0$$

$$x_1 + 2x_2 = 0$$

Notes

Let us perform row operations on A

$$A=\begin{pmatrix}-1 & i\\ -i & 3\\ 1 & 2\end{pmatrix}\xrightarrow{(2)}\begin{pmatrix}0 & 2+i\\ -i & 3\\ 1 & 2\end{pmatrix}\xrightarrow{(2)}\begin{pmatrix}0 & 2+i\\ 0 & 3+2i\\ 1 & 2\end{pmatrix}\xrightarrow{(2)}\begin{pmatrix}0 & 1\\ 0 & 3+2i\\ 1 & 0\end{pmatrix}\xrightarrow{(2)}\begin{pmatrix}0 & 1\\ 0 & 0\\ 1 & 0\end{pmatrix}=B$$

Now $BX = 0$

gives us

$$B=\begin{pmatrix}0 & 1\\ 0 & 0\\ 1 & 0\end{pmatrix}$$

has only the trivial solution;

$$x_1 = 0$$

$$x_2 = 0$$

Definition: An $m \times n$ matrix B is called **row-reduced** if:

(a) the first non-zero entry in each non-zero row of B is equal to 1;

(b) each column of B which contains the leading non-zero entry of some row has all its other entries 0.

Example 2: One example of a row-reduced matrix is the $n \times n$ **identity matrix** I. This is the $n \times n$ matrix defined by

$$I_{ij}=\delta_{ij}=\begin{cases}1 & \text{if } i=j\\ 0 & \text{if } i\neq j\end{cases}$$

Here we have introduced **Kronecker delta** [redacted].

Example 3: Find a row reduced matrix which is equivalent to

$$A=\begin{bmatrix}2 & -1 & 3 & 2\\ 1 & 4 & 0 & -1\\ 2 & 6 & -1 & 5\end{bmatrix}$$

Now

$$A=\begin{bmatrix}2 & -1 & 3 & 2\\ 1 & 4 & 0 & -1\\ 2 & 6 & -1 & 5\end{bmatrix}\xrightarrow{(2)}\begin{bmatrix}0 & -9 & 3 & 4\\ 1 & 4 & 0 & -1\\ 2 & 6 & -1 & 5\end{bmatrix}\xrightarrow{(2)}\begin{bmatrix}0 & -9 & 3 & 4\\ 1 & 4 & 0 & -1\\ 0 & -2 & -1 & 7\end{bmatrix}\xrightarrow{(1)}\begin{bmatrix}0 & -9 & 3 & 4\\ 1 & 4 & 0 & -1\\ 0 & 1 & \frac{1}{2} & -\frac{7}{2}\end{bmatrix}$$

$$\xrightarrow{(2)}\begin{bmatrix}0 & -9 & 3 & 4\\ 1 & 0 & -2 & 13\\ 0 & 1 & \frac{1}{2} & -\frac{7}{2}\end{bmatrix}\xrightarrow{(2)}\begin{bmatrix}0 & 0 & \frac{15}{2} & -\frac{55}{2}\\ 1 & 0 & -2 & 13\\ 0 & 1 & \frac{1}{2} & -\frac{7}{2}\end{bmatrix}\xrightarrow{(1)}\begin{bmatrix}0 & 0 & 1 & -\frac{11}{3}\\ 1 & 0 & -2 & 13\\ 0 & 1 & \frac{1}{2} & -\frac{7}{2}\end{bmatrix}$$

Notes

$$\xrightarrow{(2)}\begin{bmatrix}0 & 0 & 1 & -\frac{11}{3}\\ 1 & 0 & 0 & \frac{17}{3}\\ 0 & 1 & \frac{1}{2} & -\frac{7}{2}\end{bmatrix}\xrightarrow{(2)}\begin{bmatrix}0 & 0 & 1 & -\frac{11}{3}\\ 1 & 0 & 0 & \frac{17}{3}\\ 0 & 1 & 0 & \frac{-5}{3}\end{bmatrix}$$

The row-equivalence of A with the final matrix in the above sequence tells us in particular that the solutions of

$$AX = 0$$

i.e.,
$$2x_1 - x_2 + 3x_3 + 2x_4 = 0$$
$$x_1 + 4x_2 - x_4 = 0$$
$$2x_1 + 6x_2 - x_3 + 5x_4 = 0$$

and

$$x_3 - \frac{11}{3}x_4 = 0$$

$$x_1 + \frac{17}{3}x_4 = 0$$

$$x_2 - \frac{5}{3}x_4 = 0$$

are exactly the same. In the second system it is apparent that

$$x_3 = \frac{11}{3}x_4$$

$$x_1 = -\frac{17}{3}x_4$$

$$x_2 = \frac{5}{3}x_4$$

Thus if $x_4 = C$ then we obtain a solution $\left(-\frac{17}{3}C, \frac{5}{3}C, \frac{11}{3}C, C\right)$ and also that every solution is of this form.

Self Assessment

1. If $A = \begin{bmatrix}3 & -1 & 2\\ 2 & 1 & 1\\ 1 & -3 & 0\end{bmatrix}$, find all solutions of $AX = 0$ by row-reducing A.

2. Find a row-reduced matrix which is row-equivalent to $A = \begin{bmatrix}i & -(1+i) & 0\\ 1 & -2 & 1\\ 1 & 2i & -1\end{bmatrix}$

Notes

5.2 Row-reduced Echelon Matrices

Definition: An $m \times n$ matrix R is called a row-reduced echelon matrix if:

(a) R is row-reduced;

(b) every row of R which has all its entries 0 occurs below every row which has a non-zero entry;

(c) if rows 1,..., r are the non-zero rows of R, and if the leading non-zero entry of row i occurs is column k_i, $i = 1,..., r$, then $k_1 < k_2 < ... < k_r$.

One can also describe an $m \times n$ row-reduced echelon matrix R as follows. Either every entry in R is 0, or there exists a positive integer r, $1 \le r \le m$, and r positive integers $k_1 ,..., k_r$ with $1 \le k_i \le n$ and

(a) $R_{ij} = 0$ for $i > r$, and $R_{ij} = 0$ if $j < k_i$.

(b) $R_{iki} = \delta_{ij}$, $1 \le i \le r$, $1 \le j \le r$.

(c) $k_1 < ... < k_r$.

Example 4: Two examples of row-reduced echelon matrices are the $n \times n$ identity matrix, and the $m \times n$ zero matrix $0^{m, n}$, in which all entries are 0. The reader should have no difficulty in making other examples, but we should like to give one non-trivial one:

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

Theorem 2: Every $m \times n$ matrix A is row-equivalent to a row-reduced echelon matrix.

Proof: We know that A is row-equivalent to a row-reduced matrix. All that we need observe is that by performing a finite number of row interchanges on a row-reduced matrix we can bring it to row-reduced echelon form.

In Examples 1 and 3, we saw the significance of row-reduced matrices in solving homogeneous systems of linear equations. Let us now discuss briefly the system $RX = 0$, when R is a row-reduced echelon matrix. Let rows 1,..., r be the non-zero rows of R, and suppose that the leading non-zero entry of row i occurs in column k_i. The system $RX = 0$ then consists of r non-trivial equations. Also the unknown x_k, will occur (with non-zero coefficient) only in the i^{th} equation. If we let $u_1,...,u_{n-r}$ denote the $(n - r)$ unknowns which are different from $x_{k1},...,x_{kr}$, then the r non-trivial equations in $RX = 0$ are of the form

$$\left.\begin{aligned} x_{k1} + \sum_{j=1}^{n-r} C_{1j} u_j &= 0 \\ \vdots \qquad\qquad &\vdots \\ x_{kr} + \sum_{j=1}^{n-r} C_{rj} u_j &= 0 \end{aligned}\right\} \quad ...(1)$$

All the solutions to the system of equations $RX = 0$ are obtained by assigning any values whatsoever to $u_1,...,u_{n-r}$ and then computing the corresponding values of $x_{k1},...,x_{kr}$ from (1). For example, if R is the matrix displayed in Example 4, then $r = 2$, $k_1 = 2$, $k_2 = 4$, and the two non-trivial equations in the system $RX = 0$ are

$$x_2 - 3x_3 + \frac{1}{2}x_5 = 0 \text{ or } x_2 = 3x_3 - \frac{1}{2}x_5$$

Notes

$$x_4 + 2x_5 = 0 \text{ or } x_4 = -2x_5$$

So we may assign any values to x_1, x_3, and x_5, say $x_1 = a$, $x_3 = b$, $x_5 = c$, and obtain the solution $(a, 3b - \frac{1}{2}c, b, -2c, c)$.

Let us observe one thing more in connection with the system of equations $RX = 0$. If the number r of non-zero rows in R is less than n, then the system $RX = 0$ has a non-trivial solution, that is, a solution $(x_1,...,x_n)$ in which not every x_j in 0. For, since $r < n$, we can choose some x_j which is not among the r unknowns $x_{k1},...,x_{kr}$, and we can then construct a solution as above in which this x_j is 1. This observation leads us to one of the most fundamental facts concerning systems of homogeneous linear equations.

Theorem 3: If A is an $m \times n$ matrix and $m < n$, then the homogeneous system of linear equations $AX = 0$ has a non-trivial solution.

Proof: Let R be a row-reduced echelon matrix which is row-equivalent to A. Then the systems $AX = 0$ and $RX = 0$ have the same solutions by Theorem 3. If r is the number of non-zero rows in R, then certainly $r \leq m$, and since $m < n$, we have $r < n$. It follows immediately from our remarks above that $AX = 0$ has a non-trivial solution.

Theorem 4: If A is an $n \times n$ (square) matrix, then A is row-equivalent to the $n \times n$ identity matrix if and only if the system of equations $AX = 0$ has only the trivial solution.

Proof: If A is row-equivalent to I, then $AX = 0$ and $IX = 0$ have the same solutions. Conversely, suppose $AX = 0$ has only the trivial solution $X = 0$. Let R be an $n \times n$ row-reduced echelon matrix which is row-equivalent to A, and let r be the number of non-zero rows of R. Then $RX = 0$ has no non-trivial solution. Thus $r \geq n$. But since R has n rows, certainly $r \leq n$, and we have $r = n$. Since this means that R actually has a leading non-zero entry of 1 in each of its n rows, and since these 1's occur each in a different one of the n columns, R must be the $n \times n$ identity matrix.

Let us now ask what elementary row operations do toward solving a system of linear equations $AX = Y$ which is not homogeneous. At the outset, one must observe one basic difference between this and the homogeneous case, namely, that while the homogeneous system always has the trivial solution $x_1 = \cdots = x_n = 0$, an inhomogeneous system need have no solution at all.

We form the augmented matrix A' of the system $AX = Y$. This is the $m \times (n + 1)$ matrix whose first n columns are the columns of A and whose last column is Y. More precisely,

$$A'_{ij} = A_{ij}, \text{ if } j \leq n$$
$$A'_{i(n+1)} = y_i$$

Suppose we perform a sequence of elementary row operations on A arriving at a row-reduced echelon matrix R. If we perform this same sequence of row operations on the augmented matrix A', we will arrive at a matrix R' whose first n columns are the columns of R and whose last column contains certain scalars $z_1,...,z_m$. The scalars z_i are the entries of the $m \times 1$ matrix

$$Z = \begin{bmatrix} z_1 \\ \vdots \\ z_m \end{bmatrix}$$

which results from applying the sequence of row operations to the matrix Y. It should be clear to the reader that, just as in the proof of Theorem 3 the systems $AX = Y$ and $RX = Z$ are equivalent and hence have the same solutions. It is very easy to determine whether the system $RX = Z$ has any solutions and to determine all the solutions if any exist. For, if R has r non-zero rows, with the leading non-zero entry of row i occurring in column k_i, $i = 1,...,r$, then the first r equations of

Notes

$RX = Z$ effectively express $x_{k1},...,x_{kr}$ in terms of the $(n - r)$ remaining x_j and the scalars $z_1,...,z_r$. The last $(m - r)$ equations are

$$\begin{aligned} 0 &= z_{r+1} \\ \vdots & \quad \vdots \\ 0 &= z_m \end{aligned}$$

and accordingly the condition for the system to have a solution is $z_i = 0$ for $i > r$. If this condition is satisfied, all solutions to the system are found just as in the homogeneous case, by assigning arbitrary values the $(n - r)$ of the x_j and then computing x_{ki} from the ith equation.

Example 5: Let F be the field of rational numbers and

$$A = \begin{bmatrix} 1 & -2 & 1 \\ 2 & 1 & 1 \\ 0 & 5 & -1 \end{bmatrix}$$

and suppose that we wish to solve the system $AX = Y$ for some y_1, y_2 and y_3. Let us perform a sequence of row operations on the augmented matrix A' which row-reduces A:

$$\begin{bmatrix} 1 & -2 & 1 & y_1 \\ 2 & 1 & 1 & y_2 \\ 0 & 5 & -1 & y_3 \end{bmatrix} \xrightarrow{(2)} \begin{bmatrix} 1 & -2 & 1 & y_1 \\ 0 & 5 & -1 & (y_2 - 2y_1) \\ 0 & 5 & -1 & y_3 \end{bmatrix} \xrightarrow{(2)}$$

$$\begin{bmatrix} 1 & -2 & 1 & y_1 \\ 0 & 5 & -1 & (y_2 - 2y_1) \\ 0 & 0 & 0 & (y_3 - y_2 + 2y_1) \end{bmatrix} \xrightarrow{(1)} \begin{bmatrix} 1 & -2 & 1 & y_1 \\ 0 & 1 & -\frac{1}{5} & \frac{1}{5}(y_2 - 2y_1) \\ 0 & 0 & 0 & (y_3 - y_2 + 2y_1) \end{bmatrix} \xrightarrow{(2)}$$

$$\begin{bmatrix} 1 & 0 & \frac{3}{5} & \frac{1}{5}(y_1 + 2y_2) \\ 0 & 1 & -\frac{1}{5} & \frac{1}{5}(y_2 - 2y_1) \\ 0 & 0 & 0 & (y_3 - y_2 + 2y_1) \end{bmatrix}$$

The condition that the system $AX = Y$ have a solution is thus

$$2y_1 - y_2 + y_3 = 0$$

and if the given scalars y_i satisfy this condition, all solutions are obtained by assigning a value c to x_3 and then computing

$$x_1 = -\frac{3}{5}c + \frac{1}{5}(y_1 + 2y_2)$$

$$x_2 = \frac{1}{5}c + \frac{1}{5}(y_2 - 2y_1)$$

Let us observe one final thing about the system $AX = Y$. Suppose the entries of the matrix A and the scalars $y_1,...y_m$ happen to lie in a subfield F_1 of the field F. If the system of equations $AX = Y$ has a solution with $x_1,...,x_n$ in F, it has a solution with $x_1,...,x_n$ in F_1. For, over either field, the condition for the system to have a solution is that certain relations hold between $y_1,...,y_m$ in F_1

Notes

(the relations $z_i = 0$ for $i > r$, above). For example, if $AX = Y$ is a system of linear equations in which the scalars y_k and A_{ij} are real numbers, and if there is a solution in which $x_1,...,x_n$ are complex numbers, then there is a solution with $x_1,...,x_n$ real numbers.

Self Assessment

3. Find all solutions to the following system of equations by row-reducing the coefficient matrix:

$$\begin{aligned} \frac{3}{3}x_1 + 2x_2 - 6x_3 &= 0 \\ -4x_1 \quad\quad + 5x_3 &= 0 \\ -3x_1 + 6x_2 - 13x_3 &= 0 \\ -\frac{7}{3}x_1 + 2x_2 - \frac{8}{3}x_3 &= 0 \end{aligned}$$

4. Find a row-reduced echelon matrix which is row-equivalent to

$$A = \begin{bmatrix} 1 & -i \\ 2 & 2 \\ i & 1+i \end{bmatrix}$$

What are the solutions of $AX = 0$?

5.3 Summary of Row-Equivalence

In this section we shall utilize some elementary facts on bases and dimension in finite-dimensional vector spaces to complete our discussion of row-equivalence of matrices. We recall that if A is an $m \times n$ matrix over the field F the row vectors of A are the vectors $\alpha_1,...,\alpha_m$ in F^n defined by

$$\alpha_i = (A_{ij},..., A_{in})$$

and that the row space of A is the subspace of F^n spanned by these vectors. The row rank of A is the dimension of the row space of A.

If P is a $k \times m$ matrix over F, then the product $B = PA$ is a $k \times n$ matrix whose row vectors $\beta_1,...,\beta_k$ are linear combinations

$$\beta_i = P_{i1}\alpha_1 + ... + P_{im}\alpha_m$$

of the row vectors of A. Thus the row space of B is a subspace of the row space of A. If P is an $m \times m$ invertible matrix, then B is row-equivalent to A so that the symmetry of row-equivalence, or the equation $A = P^{-1}B$, implies that the row space of A is also a subspace of the row space of B.

Theorem 5: Row-equivalent matrices have the same row space.

Thus we see that to study the row space of A we may as well study the row space of a row-reduced echelon matrix which is row-equivalent to A. This we proceed to do.

Theorem 6: Let R be a non-zero row-reduced echelon matrix. Then the non-zero row vectors of R form a basis for the row space of R.

Proof: Let $\rho_1,...,\rho_r$ be the non-zero row vectors of R:

$$\rho_i = (R_{i1},...,R_{in})$$

Certainly these vectors span the row space of R; we need only prove they are linearly independent. Since R is a row-reduced echelon matrix, there are positive integers $k_1,...,k_r$ such that, for $i \leq r$

Notes

$$\left.\begin{array}{lll} \text{(a)} & R(i,j)=0 & \text{if } j<k_i \\ \text{(b)} & R(i,k_j)=\delta_{ij} & \\ \text{(c)} & k_1<\ldots<k_r & \end{array}\right\} \quad \ldots(1)$$

Suppose $\beta = (b_1,\ldots,b_n)$ is a vector in the row space of R:

$$\beta = c_1\rho_1 + \ldots + c_r\rho_r \quad \ldots(2)$$

Then we claim that $c_j = b_{ki}$. For, by

$$b_{kj} = \sum_{i=1}^{r} c_i R(i,k_j)$$

$$= \sum_{i=1}^{r} c_i \delta_{ij} \quad \ldots(3)$$

$$= c_j$$

In particular, if $\beta = 0$, i.e., if $c_1\rho_1 + \ldots + c_r\rho_r = 0$, then c_j must be the k_jth coordinate of the zero vector so that $c_j = 0$, $j = 1,\ldots, r$. Thus $\rho_1,\ldots,\rho_r$ are linearly independent.

Theorem 7: Let m and n be positive integers and let F be a field. Suppose W is a subspace of F^n and dim $W \leq m$. Then there is precisely one $m \times n$ row-reduced echelon matrix over F which has W as its row space.

Proof: There is at least one $m \times n$ row-reduced echelon matrix with row space W. Since dim $W \leq m$, we can select some m vectors $\alpha_1,\ldots,\alpha_m$ in W which span W. Let A be the $m \times n$ matrix with row vectors $\alpha_1,\ldots,\alpha_m$ and let R be a row-reduced echelon matrix which is row-equivalent to A. Then the row space of R is W.

Now let R be any row-reduced echelon matrix which has W as its row space. Let $\rho_1,\ldots,\rho_r$ be the non-zero row vectors of R and suppose that the leading non-zero entry of ρ_i occurs in column k_i, $i = 1,\ldots,r$. The vectors $\rho_1,\ldots,\rho_r$ form a basis for W. In the proof of Theorem, we observed that if $\beta = (b_1,\ldots,b_n)$ is in W, then

$$\beta = c_1\rho_1 + \ldots + c_r\rho_r,$$

and $c_i = b_{ki}$; in other words, the unique expression for β as a linear combination of $\rho_1,\ldots,\rho_r$ is

$$\beta = \sum_{i=1}^{r} b_{ki}\rho_i \quad \ldots(4)$$

Thus any vector β is determined if one knows the coordinates b_{ki}, $i = 1,\ldots, r$. For example, ρ_s is the unique vector in W which has k_sth coordinate 1 and k_ith coordinate 0 for $i \neq s$.

Suppose β is in W and $\beta \neq 0$. We claim the first non-zero coordinate of β occurs in one of the columns k_s. Since

$$\beta = \sum_{i=1}^{r} b_{ki}\rho_i$$

and $\beta \neq 0$, we can write

$$\beta = \sum_{i=s}^{r} b_{ki}\rho_i, \qquad b_{ks} \neq 0 \quad \ldots(5)$$

Notes

From the conditions (1) one has $R_{ij} = 0$ if $i > s$ and $j \leq k_s$. Thus

$$\beta = (0,..., 0, \beta_{ks},...,b_n),\ b_{ks} \neq 0$$

and the first non-zero coordinate of β occurs in column k_8. Note also that for each k_8, $S = 1,..., r$, there exists a vector in W which has a non-zero k_sth coordinate, namely ρ_s.

It is now clear that R is uniquely determined by W. The description of R in terms of W is as follows. We consider all vectors $\beta = (b_1,...,b_n)$ in W. If $\beta \neq 0$, then the first non-zero coordinate of β must occur in some column t:

$$\beta = (0,...,0, b_t,..., b_n),\ b_t \neq 0$$

Let $k_1,...,k_r$ be those positive integers t such that there is some $\beta \neq 0$ in W, the first non-zero coordinate of which occurs in column t. Arrange $k_1,...,k_r$ in the order $k_1 < k_2 < ... < k_r$. For each of the positive integers k_s there will be one and only one vector ρ_s in W such that the k_sth coordinate of ρ_s is 1 and the k_ith coordinate of ρ_s is 0 for $i \neq s$. Then R is the $m \times n$ matrix which has row vectors $\rho_1,...,\rho_r, 0, ..., 0$.

Corollary. Each $m \times n$ matrix A is row-equivalent to one and only one row-reduced echelon matrix.

Proof: We know that A is row-equivalent to at least one row-reduced echelon matrix R. If A is row-equivalent to another such matrix R', then R is row-equivalent to R'; hence, R and R' have the same row space and must be identical.

Corollary: Let A and B be $m \times n$ matrices over the field F. Then A and B are row-equivalent if and only if they have the same row space.

Proof: We know that if A and B are row-equivalent, then they have the same row space. So suppose that A and B have the same row space. Now A is row-equivalent to a row-reduced echelon matrix R and B is row-equivalent to a row-reduced echelon matrix R'. Since A and B have the same row space, R and R' have the same row space. Thus $R = R'$ and A is row-equivalent to B.

To summarize—if A and B are $m \times n$ matrices over the field F, the following statements are equivalent:

1. A and B are row-equivalent.
2. A and B have the same row space.
3. $B = PA$, where P is an invertible $m \times m$ matrix.

A fourth equivalent statement is that the homogeneous systems $AX = 0$ and $BX = 0$ have the same solutions; however, although we know that the row-equivalence of A and B implies that these systems have the same solutions, it seems best to leave the proof of the converse until later.

5.4 Summary

- Such an equation is called a linear combination of the equations in (1). Evidently any solution of the entire system of equations (1) will also be the solution of this new equation. This is the fundamental idea of the elimination process.
- A particular e is defined on the class of all m rowed matrices over F. One reason that we restrict ourselves to these simple types of row operations is that having performed such an operation e on a matrix A, we can recapture A by performing a similar operation on $e(A)$.
- An $m \times n$ matrix B is called row-reduced if:
  (a) the first non-zero entry in each non-zero row of B is equal to 1;

Notes

(b) each column of B which contains the leading non-zero entry of some row has all its other entries 0.

5.5 Keywords

Equivalent: Two systems of linear equations are equivalent if each equation in each system is a linear combination of the equations in the other system.

Row-equivalent: If A and B are $m \times n$ matrices over the field F, we say that B is **row-equivalent** to A if B is obtained from A by a finite sequence of elementary row operations.

5.6 Review Questions

1. Find all solutions to the system of equations

$$(1 - i)x_1 - ix_2 = 0$$

$$2x_1 + (1 - i)x_2 = 0$$

2. Let $A = \begin{bmatrix} 3 & -1 & 2 \\ 2 & 1 & 1 \\ 1 & -3 & 0 \end{bmatrix}$

For which triples (y_1, y_2, y_3) does this system $AX = Y$ have a solution?

Answers: Self Assessment

1. Row-reduced matrix is $\begin{bmatrix} 0 & 1 & 1/4 \\ 1 & 0 & 3/8 \\ 0 & 0 & 3/8 \end{bmatrix}$ the solution is $x_1 = x_2 = x_3 = 0$

3. Row-reduced matrix is $\begin{bmatrix} 0 & 1 & -\frac{64}{24} \\ 1 & 0 & -\frac{5}{4} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ the solution is $x_1 = \frac{67}{24}C, x_2 = \frac{5}{4}C, x_3 = C$ where C is a constant.

4. Row-reduced matrix is $\begin{bmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 0 \end{bmatrix}$. The solution is $x_1 = x_2 = 0$

5.7 Further Readings

Books

Kenneth Hoffman and Ray Kunze *Linear Algebra*

I.N. Herstein *Topics in Algebra*

Unit 6: Computation Concerning Subspaces

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- See that the units (3), (4) and (5) are quite suitable to find if a set of vectors $\alpha_1, \alpha_2,...\alpha_m$ are linearly independent.
- Determine whether another vector β is a linear combination of $\alpha_1,...\alpha_m$.
- See that the detailed examples in this unit clarify most ideas covered in the last few units.

Introduction

This unit mostly summarizes the ideas of row-operations in helping to find out the basis of a vector-subspace.

One can understand how a vector α belongs to the vector sub-space spanned by the basis vectors.

6.1 Computation Concerning Subspaces

In this unit we should like to show how elementary row operations helps us in understanding in a concrete way the subspaces of F^n. This discussion applies to any n-dimensional vector space over the field F, if one selects a fixed ordered basis β and describes each vector α in V by the n-tuple $(x_1, x_2,...,x_n)$ which gives the co-ordinates of α in the ordered basis β.

Suppose we are given m vectors $\alpha_1,...,\alpha_m$ in F^n. We consider the following questions.

1. How does one determine if the vectors $\alpha_1, \alpha_2,...,\alpha_m$ are linearly independent? How does one find the dimension of the subspace W spanned by these vectors?
2. Given β in F^n, how does one determine whether β is a linear combination of $\alpha_1,...,\alpha_m$, i.e., whether β is in the subspace W?
3. How can one give an explicit description of the subspace W?

The third question is a little vague, since it does not specify what is meant by an 'explicit description'; however, we shall clear up this point by giving the sort of description we have in mind. With this description, questions (1) and (2) can be answered immediately.

Notes

Let A be the $m \times n$ matrix with row vectors α_i:

$$\alpha_i = (A_{i1},...,A_{in})$$

Perform a sequence of elementary row operations, starting with A and terminating with a row-reduced echelon matrix R. We have previously described how to do this. At this point, the dimension of W (the row space of A) is apparent, since this dimension is simply the number of non-zero row vectors of R. If $\rho_1,...,\rho_r$ are the non-zero row vectors of R, then $\mathcal{B} = \{\rho_1,...,\rho_r\}$ is a basis for W. If the first non-zero coordinate of ρ_i is the k_ith one, then we have for $i \leq r$

(a) $R(i, j) = 0$, if $j < k_i$

(b) $R(i, k_j) = \delta_{ij}$

(c) $k_1 < ... < k_r$

The subspace W consists of all vectors

$$\beta = c_1\rho_1 + ... + c_r\rho_r$$

$$= \sum_{i=1}^{r} c_i(R_{i1},..., R_{in})$$

The coordinates $b_1,...,b_n$ of such a vector β are then

$$b_j = \sum_{i=1}^{r} c_i R_{ij} \qquad ...(1)$$

In particular, $b_{ki} = c_j$, and so if $\beta = (b_1,...,b_n)$ is a linear combination of the ρ_i, it must be the particular linear combination.

$$\beta = \sum_{i=1}^{r} b_{ki}\rho_i \qquad ...(2)$$

The conditions on β that (2) should hold are

$$b_j = \sum_{i=1}^{r} b_{ki} R_{ij} \qquad j = 1,...,n. \qquad ...(3)$$

Now (3) is the explicit description of the subspace W spanned by $\alpha_1,...,\alpha_m$, that is, the subspace consists of all vectors β in F^n whose coordinates satisfy (3). What kind of description is (3)? In the first place it describes W as all solutions $\beta = (b_1,...,b_n)$ of the system of homogeneous linear equations (3). This system of equations is of a very special nature, because it expresses $(n - r)$ of the coordinates as linear combinations of the r distinguished coordinates $b_{k1},...,b_{kr}$. One has complete freedom of choice in the coordinates b_{ki}, that is, if $c_1,...,c_r$ are any r scalars, there is one and only one vector β in W which has c_i as its k_ith coordinate.

The significant point here is this: Given the vectors α_i, row-reduction is a straightforward method of determining the integers $r, k_1,...,k_r$ and the scalars R_{ij} which give the description of the subspace spanned by $\alpha_1,...,\alpha_m$. One should observe that every subspace W of F^n has a description of the type (3). We should also point out some things about question (2). We have already stated how one can find an invertible $m \times m$ matrix P such that $R = PA$. The knowledge of P enables one to find the scalars $x_1,...,x_m$ such that

$$\beta = x_1\alpha_1 + ... + x_m\alpha_m$$

when this is possible. For the row vectors of R are given by

$$\rho_i = \sum_{j=1}^{m} P_{ij}\alpha_j$$

Notes

so that if β is a linear combination of the α_j, we have

$$\beta = \sum_{i=1}^{r} b_{ki}\rho_i$$

$$= \sum_{i=1}^{r} b_{ki} \sum_{j=1}^{m} P_{ij}\alpha_j$$

$$= \sum_{j=1}^{m} \sum_{i=1}^{r} b_{ki} P_{ij}\alpha_j$$

and thus $$x_j = \sum_{i=1}^{r} b_{ki} P_{ij}$$

is one possible choice for the x_j (there may be many).

The question of whether $\beta = (b_1,...,b_n)$ is a linear combination of the α_i, and if so, what the scalars x_i are, can also be looked at by asking whether the system of equations

$$\sum_{i=1}^{m} A_{ij}x_i = b_j, \qquad j = 1,...,n$$

has a solution and what the solutions are. The coefficient matrix of this system of equations is then $n \times m$ matrix B with column vectors $\alpha_1,...,\alpha_m$. In unit 5, we discussed the use of elementary row operations in solving a system of equations $BX = Y$. Let us consider one example in which we adopt both points of view in answering questions about subspaces of F^n.

6.2 Illustrative Examples

Example 1: Let us pose the following problem. Let W be the subspace of R^4 spanned by the vectors

$$\alpha_1 = (1, 2, 2, 1)$$

$$\alpha_2 = (0, 2, 0, 1)$$

$$\alpha_3 = (-2, 0, -4, 3)$$

(a) Prove that α_1, α_2, α_3 form a basis for W, i.e., that these vectors are linearly independent.

(b) Let $\beta = (b_1, b_2, b_3, b_4)$ be a vector in W. What are the coordinates of β relative to the ordered basis $\{\alpha_1, \alpha_2, \alpha_3\}$?

(c) Let

$$\alpha_1' = (1, 0, 2, 0)$$

$$\alpha_2' = (0, 2, 0, 1)$$

$$\alpha_3' = (0, 0, 0, 3)$$

Show that α_1', α_2', α_3' form a basis for W.

Notes

(d) If β is in W, let X denote the coordinate matrix of β relative to the α-basis and X' the coordinate matrix of β relative to the α′-basis. Find the 3 × 3 matrix P such that $X = PX'$ for every such β.

To answer these questions by the first method we form the matrix A with row vectors $\alpha_1, \alpha_2, \alpha_3$, find the row-reduced echelon matrix R which is row-equivalent to A and simultaneously perform the same operations on the identity to obtain the invertible matrix Q such that $R = QA$:

$$\begin{bmatrix} 1 & 2 & 2 & 1 \\ 0 & 2 & 0 & 1 \\ -2 & 0 & -4 & 3 \end{bmatrix} \to R = \begin{bmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \to Q = \frac{1}{6}\begin{bmatrix} 6 & -6 & 0 \\ -2 & 5 & -1 \\ 4 & -4 & 2 \end{bmatrix}$$

(a) Clearly R has rank 3, so α_1, α_2 and α_3 are independent.

(b) Which vectors $\beta = (b_1, b_2, b_3, b_4)$ are in W? We have the basis for W given by ρ_1, ρ_2, ρ_3, the row vectors of R. One can see at a glance that the span of ρ_1, ρ_2, ρ_3 consists of the vectors β for which $b_3 = 2b_1$. For such a β we have

$$\begin{aligned} \beta &= b_1\rho_1 + b_2\rho_2 + b_4\rho_4 \\ &= [b_1, b_2, b_4]R \\ &= [b_1\ b_2\ b_4]QA \\ &= x_1\alpha_1 + x_2\alpha_2 + x_3a_3 \end{aligned}$$

where $x_i = [b_1\ b_2\ b_4]Q_i$:

$$\left.\begin{aligned} x_1 &= b_1 - \frac{1}{3}b_2 + \frac{2}{3}b_4 \\ x_2 &= -b_1 + \frac{5}{6}b_2 - \frac{2}{3}b_4 \\ x_3 &= \quad -\frac{1}{6}b_2 + \frac{1}{3}b_4 \end{aligned}\right\} \quad \text{... (1)}$$

(c) The vectors $\alpha_1', \alpha_2', \alpha_3'$ are all of the form (y_1, y_2, y_3, y_4) with $y_3 = 2y_1$ and thus they are in W. One can see at a glance that they are independent.

(d) The matrix P has for its columns

$$P_j = \left[\alpha_j'\right]_{\mathcal{B}}$$

where $\beta = \{\alpha_1, \alpha_2, \alpha_3\}$. The equations (1) tell us how to find the coordinate matrices for $\alpha_1', \alpha_2', \alpha_3'$.

For example with $\beta = \alpha_1'$ we have $b_1 = 1$, $b_2 = 0$, $b_3 = 2$, $b_4 = 0$, and

$$x_1 = 1 - \frac{1}{3}(0) + \frac{2}{3}(0) = 1$$

$$x_2 = -1 + \frac{5}{6}(0) + \frac{2}{3}(0) = -1$$

$$x_3 = -\frac{1}{6}(0) + \frac{1}{3}(0) = 0$$

Notes

Thus $\alpha_1' = \alpha_1 - \alpha_2$. Similarly we obtain $\alpha_2' = \alpha_2$ and $\alpha_3' = 2\alpha_1 - 2\alpha_2 + \alpha_3$.

Hence

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

Now let us see how we would answer the questions by the second method which we described. We form the 4 × 3 matrix B with column vectors $\alpha_1, \alpha_2, \alpha_3$:

$$B = \begin{bmatrix} 1 & 0 & -2 \\ 2 & 2 & 0 \\ 2 & 0 & -4 \\ 1 & 1 & 3 \end{bmatrix}$$

We inquire for which y_1, y_2, y_3, y_4 the system $BX = Y$ has a solution.

$$\begin{bmatrix} 1 & 0 & -2 & y_1 \\ 2 & 2 & 0 & y_2 \\ 2 & 0 & -4 & y_3 \\ 1 & 1 & 3 & y_4 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & -2 & y_1 \\ 0 & 2 & 4 & y_2 - 2y_1 \\ 0 & 0 & 0 & y_3 - 2y_1 \\ 0 & 1 & 5 & y_4 - y_1 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & -2 & y_1 \\ 0 & 0 & -6 & y_2 - 2y_4 \\ 0 & 1 & 5 & y_4 - y_1 \\ 0 & 0 & 0 & y_3 - 2y_1 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 & y_1 - \frac{1}{3}y_2 + \frac{2}{3}y_4 \\ 0 & 0 & 1 & \frac{1}{6}(2y_4 - y_2) \\ 0 & 1 & 0 & -y_1 + \frac{5}{6}y_2 - \frac{2}{3}y_4 \\ 0 & 0 & 0 & y_3 - 2y_1 \end{bmatrix}$$

Thus the condition that the system $BX = Y$ have a solution is $y_3 = 2y_1$. So $\beta = (b_1, b_2, b_3, b_4)$ is in W if and only if $b_3 - 2b_1$. If β is in W, then the coordinates (x_1, x_2, x_3) in the ordered basis $\{\alpha_1, \alpha_2, \alpha_3\}$ can be read off from the last matrix above. We obtain once again the formulas (1) for those coordinates

The questions (*c*) and (*d*) are now answered as before.

Example 2: We consider the 5 × 5 matrix

$$A = \begin{bmatrix} 1 & 2 & 0 & 3 & 0 \\ 1 & 2 & -1 & -1 & 0 \\ 0 & 0 & 1 & 4 & 0 \\ 2 & 4 & 1 & 10 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

and the following problems concerning A

(a) Find an invertible matrix P such that PA is a row-reduced echelon matrix R.

(b) Find a basis for the new row space W of A.

(c) Say which vectors $(b_1, b_2, b_3, b_4, b_5)$ are in W.

(d) Find the coordinate matrix of each vector $(b_1, b_2, b_3, b_4, b_5)$ in W in the ordered basis chosen in (b).

(e) Write each vector $(b_1, b_2, b_3, b_4, b_5)$ in W as a linear combination of the rows of A.

(f) Give an explicit description of the vector space V of all 5 × 1 column matrices X such that $AX = 0$.

Notes

(g) Find a basis for V.

(h) For what 5×1 column matrices Y does the equation $AX = Y$ have solutions X?

To solve these problems we form the augmented matrix A' of the system $AX = Y$ and apply an appropriate sequence of row operations to A'.

$$\begin{bmatrix} 1 & 2 & 0 & 3 & 0 & y_1 \\ 1 & 2 & -1 & -1 & 0 & y_2 \\ 0 & 0 & 1 & 4 & 0 & y_3 \\ 2 & 4 & 1 & 10 & 1 & y_4 \\ 0 & 0 & 0 & 0 & 1 & y_5 \end{bmatrix} \to \begin{bmatrix} 1 & 2 & 0 & 3 & 0 & y_1 \\ 0 & 0 & -1 & -4 & 0 & -y_1 + y_2 \\ 0 & 0 & 1 & 4 & 0 & y_3 \\ 0 & 0 & 1 & 4 & 1 & -2y_1 + y_4 \\ 0 & 0 & 0 & 0 & 1 & y_5 \end{bmatrix} \to$$

$$\begin{bmatrix} 1 & 2 & 0 & 3 & 0 & y_1 \\ 0 & 0 & 1 & 4 & 0 & y_1 - y_2 \\ 0 & 0 & 0 & 0 & 0 & -y_1 + y_2 + y_3 \\ 0 & 0 & 0 & 0 & 1 & -3y_1 + y_2 + y_4 \\ 0 & 0 & 0 & 0 & 1 & y_5 \end{bmatrix} \to \begin{bmatrix} 1 & 2 & 0 & 3 & 0 & y_1 \\ 0 & 0 & 1 & 4 & 0 & y_1 - y_2 \\ 0 & 0 & 0 & 0 & 1 & y_5 \\ 0 & 0 & 0 & 0 & 0 & -y_1 + y_2 + y_3 \\ 0 & 0 & 0 & 0 & 0 & -3y_1 + y_2 + y_4 - y_5 \end{bmatrix}$$

(a) If

$$PY = \begin{bmatrix} y_1 \\ y_1 - y_2 \\ y_5 \\ -y_1 + y_2 + y_3 \\ -3y_1 + y_2 + y_4 - y_5 \end{bmatrix}$$

for all Y, then

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

hence PA is the row-reduced echelon matrix

$$R = \begin{bmatrix} 1 & 2 & 0 & 3 & 0 \\ 0 & 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

It should be stressed that the matrix P is not unique. There are, in fact, many invertible matrices P (which arise from different choices for the operations used to reduce A') such that $PA = R$.

(b) As a basis for W we may take the non-zero rows

$$\rho_1 = (1\ 2\ 0\ 3\ 0)$$

Notes

$\rho_2 = (0\ 0\ 1\ 4\ 0)$

$\rho_3 = (0\ 0\ 0\ 0\ 1)$

of R

(c) The row-space W consists of all vectors of the form

$$\beta = c_1\rho_1 + c_2\rho_2 + c_3\rho_3$$
$$= (c_1, 2c_1, c_2, 3c_1 + 4c_2, c_3)$$

where c_1, c_2, c_3 are arbitrary scalars. Thus $(b_1, b_2, b_3, b_4, b_5)$ is in W if and only if

$(b_1, b_2, b_3, b_4, b_5) = b_1\rho_1 + b_3\rho_2 + b_5\rho_3$

which is true if and only if

$$b_2 = 2b_1$$
$$b_4 = 3b_1 + 4b_3.$$

These equations are instances of the general system (3) in unit 5, and using them we may tell at a glance whether a given vector lies in W. Thus (–5, –10, 1, –11, 20) is a linear combination of the rows of A, but (1, 2, 3, 4, 5) is not.

(d) The coordinate matrix of the vector $(b_1, 2b_1, b_3, 3b_1 + 4b_3, b_5)$ in the basis $\{\rho_1, \rho_2, \rho_3\}$ is evidently

$$\begin{bmatrix} b_1 \\ b_3 \\ b_5 \end{bmatrix}$$

(e) There are many ways to write the vectors in W as linear combinations of the rows of A.

$$\beta = (b_1, 2b_1, b_3, 3b_1 + 4b_3, b_5)$$
$$= [b_1, b_3, b_5, 0, 0] \cdot R$$
$$= [b_1, b_3, b_5, 0, 0] \cdot PA$$

$$= [b_1, b_3, b_5, 0, 0] \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ -1 & 1 & 1 & 0 & 0 \\ -3 & 1 & 0 & 1 & -1 \end{bmatrix} A$$

$$= [b_1 + b_3, -b_3, 0, 0, b_5] \cdot A$$

In particular, with $\beta = (-5, -10, 1, -11, 20)$ we have

$$\beta = (-4, -1, 0, 0, 20) \begin{bmatrix} 1 & 2 & 0 & 3 & 0 \\ 1 & 2 & -1 & -1 & 0 \\ 0 & 0 & 1 & 4 & 0 \\ 2 & 4 & 1 & 10 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Notes

(f) The equations in the system $RX = 0$ are

$$x_1 + 2x_2 + 3x_4 = 0$$
$$x_3 + 4x_4 = 0$$
$$x_5 = 0$$

Thus V consists of all columns of the form

$$X = \begin{bmatrix} -2x_2 - 3x_4 \\ x_2 \\ -4x_4 \\ x_4 \\ 0 \end{bmatrix}$$

where x_2 and x_4 are arbitrary.

(g) The columns

$$\begin{bmatrix} -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad \begin{bmatrix} -3 \\ 0 \\ -4 \\ 1 \\ 0 \end{bmatrix}$$

form a basis of V.

(h) The equation $AX = Y$ has solutions X if and only if

$$-y_1 + y_2 + y_3 = 0$$
$$-3y_1 + y_2 + y_4 - y_5 = 0$$

Self Assessment

1. In C^3, let

$$\alpha_1 = (1, 0, -i), \alpha_2 = (1 + i, 1 - i, 1), \alpha_3 = (i, i, i)$$

Prove that these vectors form a basis for C^3. What are the co-ordinates of the vector (a, b, c) in this basis?

2. Let $\alpha_1 = (1, 1, -2, 1)$, $\alpha_2 = (3, 0, 4, -1)$, $\alpha_3 = (-1, 2, 5, 2)$

Let

$\alpha = (4, -5, 9, -7)$, $\beta = (3, 1, -4, 4)$, $\gamma = (-1, 1, 0, 1)$

Which of the vectors α, β, γ are in the sub-space of R^4 spanned by the α_i?

6.3 Summary

- In this unit it is shown how elementary row operations help us in understanding the basis of the subspace F^n.
- The detailed examples show how to go from one basis vector to another by means of an invertible matrix.

Notes

- Given the vectors α_i, row-reduction is a straightforward method of determining the integers $r, k_1,...,k_r$ and the scalars R_{ij} which give the description of the subspace spanned by $\alpha_1,...,\alpha_m$.
- The question of whether $\beta = (b_1,...,b_n)$ is a linear combination of the α_i, and if so, what the scalars x_i are, can also be looked at by asking whether the system of equations

$$\sum_{i=1}^{m} A_{ij}x_i = b_j, \qquad j = 1,...,n$$

has a solution and what the solutions are.

- The unit helps in finding an invertible matrix P such that the co-ordinates of a vector α in the two system of basis β and β' are related by the relation $X = PX'$ for every basis β.

6.4 Keywords

Basis of the Subspace: The basis of the subspace W is found by the row vectors of R. So one can test whether a vector β belongs to W or not.

Row Reduction of a Matrix: The row reduction of a matrix A helps whether a set of vectors α_1, α_2, α_3 form a basis by forming the matrix A with row vectors and finding its rank.

6.5 Review Questions

1. Let $\beta = (u_1, u_2,...,u_n)$ and $\beta' = (v_1, v_2, v_3,..,v_n)$ be two bases of a vector space V. Show that the base change matrix P is uniquely determined by the two bases β and β' and is an invertible matrix.
2. Solve completely the system of equations $AX = 0$ and $AX = B$, where

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

Answers: Self Assessment

1. $\left[\frac{a-b}{5}(1-2i), \frac{a}{5}(1-2i)+\frac{b}{5}(7i-1)-ic, \frac{a}{5}(3-i)-\frac{b}{5}(6-i)-c(1+i)\right]$
2. α, β

6.6 Further Readings

Books

Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I.N. Herstein, *Topics in Algebra*

Michael Artin, *Algebra*

Notes

Unit 7: Algebra of Linear Transformation

CONTENTS

Objectives

After studying this unit, you will be able to:

- Know that linear transformation on the space is quite important. It helps in understanding the space under various transformations.
- See that the knowledge of the basis and dimension help us that the properties of linear transformation on the basis vector is central to the ideas of matrix mechanics.

Introduction

It will be seen that in the development of the algebra linear transformation plays an important part in understanding the properties of spaces. It is seen that the set of linear transformations also satisfy the properties of vector spaces.

7.1 Homomorphism

Consider two vector spaces V and W over the same field F i.e.

$$V = \{v, F, +, \oplus, \odot\}$$
$$W = \{w, F, +, +, \odot\}$$

The vectors of two different systems might have different names, and the vector operations of two systems might be defined in different ways.

A mapping H of V into W is called a homomorphism provided that all $\alpha, B \in V$ and all $a \in F$,

$$(\alpha \oplus B)\, H = \alpha H + \beta H \quad ...(1)$$

and $$(\alpha \odot \alpha)\, H = a\,.\,\alpha H \quad ...(2)$$

If every vector of W is in the range of H, H is said to be *homomorphism* of V onto W.

A one-to-one homomorphism H of V onto W is called an *isomorphism*. If such a mapping exists, V, and W are said to be isomorphic.

Notes

We now show that

$$(\alpha \odot \alpha \oplus b \odot \beta)H = (a \cdot \alpha)\, H + (b \,.\, \beta)H \qquad ...(3)$$

clearly equation 1 follows from equation (3) by selecting $a = 1 = b$ and equation (2) follows by choosing $b = 0$.

7.2 Linear Transformation

Condition (3) is the requirement of linearly and since homomorphism is a mapping we call a homomorphism a *linear transformation*.

Thus a linear transformation T from a vector space V to a vector space W, both over the same field is a mapping of V onto W such that for all $\alpha, \beta \in V$ and for all $a, b, \in F$,

$$(a\alpha + b\beta)T = a\,(\alpha T) + b\,(\beta T)$$

Example 1: Identity transformation. If V is any vector space, then the identity transformation I defined by $I\alpha = \alpha$, is linear transformation from V into V.

The zero transformation 0, defined by $0\alpha = 0$, is a linear transformation from V into V.

Example 2: If V be the space of polynomial function f from the field F into F, given by

$$f(x) = C_0 + C_1 x + C_2 x^2 + ... + C_n x^n$$

Let $$Df(x) = C_1 + 2C_2 x + 3C_3 x^2 + ... + nC_n x^{n-1}$$

Then D is a linear transformation from V into V the differentiation transformation.

Example 3: In two dimension space V_2, the transformation

$(x, y)T = (x \cos \theta - y \sin \theta, x \sin \theta + y \cos \theta)$ is a linear transformation

Example 4: In the space V_2 represented geometrically by the plane the transformation

$(x, y)T = (ax, by)$

Example 5: Let R be the field of real numbers and let V be the space of all functions from into R which are continuous. Define T by

$$(Tf)(x) = \int_0^x f(t)dt.$$

Then T is a linear transformation from V into V. The function Tf is not only continuous but has a continuous first derivative. The linearity of integration is one of its fundamental properties.

Example 6: Let A being a fixed $m \times n$ matrix with entries in the field F. The function T defined by $T(X) = AX$ is a linear transformation from $F^{n \times 1}$ into $F^{m \times 1}$. The function U defined by $U(\alpha) = \alpha A$ is a linear transformation from F^m into F^n.

Example 7: Let P be a fixed $m \times m$ matrix with entries in the field F and let Q be a fixed $n \times m$ matrix over F. Define a function T from the space $F^{m \times n}$ into itself by $T = PAQ$.

Notes

Then T is a linear transformation from $F^{m \times n}$ into $F^{m \times n}$,

because

$$\begin{aligned} T(CA + B) &= P(CA + B)Q \\ &= (CPA + PB)Q \\ &= C\,PAQ + PBQ \\ &= CT(A) + T(B) \end{aligned}$$

Example 8: The linear transformation preserves the linear combination; that is, if $\alpha_1, \alpha_2, \ldots \alpha_n$ are vectors in V and $C_1, C_2, \ldots C_n$ are scalars, then

$$T(C_1\alpha_1 + C_2\alpha_2 + \ldots + C_n\alpha_n) = C_1(T\alpha_1) + C_2T(\alpha_2) + \ldots + C_n(T\alpha_n).$$

This follows readily from the definition. For example

$$T(C_1\alpha_1 + C_2\alpha_2) = C_1(T\alpha_1) + C_2(T\alpha_2)$$

Theorem 1: Let V be a finite dimensional vector space over the field F and let $(\alpha_1, \alpha_2, \ldots \alpha_n)$ be an ordered basis for V. Let W be a vector space over the same field F and let $\beta_1, \beta_2, \ldots \beta_n$, be a set of any vectors in W. There is precisely one linear transformation T from V into W such that

$$T\alpha_i = \beta_i,\ i = 1, 2, \ldots n$$

Proof: To prove that there is some linear transformation T with $T\alpha_i = \beta i$, we proceed as follows, given α in V, there is a unique n-tuple $(x_1, x_2, \ldots x_n)$ such that

$$\alpha = x_1\alpha_i + x_2\alpha_2 + \ldots + x_n\alpha_n$$

For this α we define

$$T\alpha = x_1\beta_1 + x_2\beta_2 + \ldots + x_n\beta_n.$$

Then T is a well define rule for associating with each vector α in V a vector $T\alpha$ in W. From the definition it is clear that $T\alpha_j = \beta_j$ for each j. To see that T is linear, let

$$\beta = y_1\alpha_1 + y_2\alpha_2 + \ldots + y_n\alpha_n$$

be in V and let C be any scalar. Now

$$C\alpha + \beta = (Cx_1 + y_1)\alpha_1 + (Cx_2 + y_2)\alpha_2 + \ldots + (Cx_n + y_n)\alpha_n$$

and so by definition

$$T(C\alpha + \beta) = (Cx_1 + y_1)\beta_1 + (Cx_2 + y_2)\beta_2 + \ldots + (Cx_n + y_n)\beta_n$$

on the other hand

$$\begin{aligned} C(T\alpha) + T\beta &= e\sum_{i=1}^{n} x_i\beta_i + \sum_{i=1}^{n} y_i\beta_i \\ &= \sum_{i=1}^{n} (Cx_i + y_i)\beta_i \end{aligned}$$

and thus

$$T(C\alpha + \beta) = C(T\alpha) + (T\beta)$$

Notes

If U is a linear transformation from V into W with $U\alpha_i = \beta_i$, $i = 1, 2, \ldots n$, then for the vector $\alpha = \sum_{i=1}^{n} x_i\alpha_i$, we have

$$U\alpha = U\left(\sum_{i=1}^{n} x_i\alpha_i\right)$$
$$= \sum_{i=1}^{n} x_i(U\,\alpha_i)$$
$$= \sum_{i=1}^{n} x_i\beta_i$$

So that U is exactly the rule T which we defined above. This shows that the linear transformation T with $T\alpha_i = \beta_i$ is unique.

Relations and operations of Linear Transformations

1. Two linear transformations T_1 and T_2 from v to w are said to be equal if and only if

$$\alpha T_1 = \alpha T_2 \text{ for all } \alpha \in v.$$

2. The sum $T_1 \oplus T_2$ of linear transformation from v to w are defined, respectively, by

$$\alpha(T_1 \oplus T_2) = \alpha T_1 + \alpha T_2 \text{ for all } \alpha \in v.$$

3. The scalar multiple $C \odot T_1$ of linear transformations from v to w are defined as

$$\alpha(c \odot T_1) = c(\alpha T_1), \text{ for all } \alpha \in v, c \in F.$$

Special Linear Transformation

(a) The zero linear transformation Z is defined from v to w by

$$\alpha Z = \ominus \text{ for every } \alpha \in v$$

(b) Negative transformation $(-T)$ from v to w, is defined by

$$\alpha(-T) = -\alpha T \text{ for every } \alpha \in v$$

(c) Identity linear transformation I from v to v is defined by

$$\alpha I = \alpha \text{ for every } \alpha \in v$$

(d) Product transformation $T_1 \boxdot T_2$.

Let v, w and y be vector spaces over the field F; let T_1 be a linear transformation from v to w and T_2 be a linear transformation from w to y. Then the product transformation $T_1 \boxdot T_2$ is the mapping from v to y defined by

$$\alpha(T_1 \boxdot T_2) = (\alpha T_1)T_2 \text{ for every } \alpha \in v.$$

Thus for every T we have

$$T \oplus Z = T$$

$$T \oplus -T = Z$$

$$T \boxdot I = I \boxdot T + T.$$

Notes

Example 9: In the space V_2 let T_1, T_2 and T_3 be defined by

$(x, y)T_1 = (x, 0)$

$(x, y)T_2 = (0, y)$

$(x, y)T_3 = (y, x)$

All these transformations are linear, now

$(x, y)T_1T_2 = (x, 0)T_2 = (0, 0)$, so $T_1T_2 = Z$

But $T_1 \neq Z$ and $T_2 \neq Z$ Hence a product of non-zero transformation can be the zero transformation. Also

$(x, y)T_2T_3 = (0, y)T_3 = (y, 0)$

But

$(x, y)T_3T_2 = (y, x)T_2 = (0, x)$. Hence

$\boldsymbol{T}_2T_3 \neq T_3\ T_2$.

So the multiplication of transformation is not commutative. Observe that

$(x, y)T_1T_1 = (x, 0)T_1 = (x, 0) = (x, y)T_1$,

so that $T_1^2 = T_1$. Thus there exist idempotent transformation i.e.

$$T_1^k = T_1$$

for integer k, other than I and Z.

Rank and Nullity of a Linear Transformation

Consider a linear transformation from a space v into a space w. The domain of T is the space v and the range of T is a subset R_T of w, the set of all images αT of the vectors of v:

$R_T = \{\beta \in w \mid \beta = \alpha T \text{ for some } \alpha \in v\}$

Another set associated with any vector space homomorphism T is the Kernel K_T of the homomorphism, which is defined to be the set of all vectors in v which are mapped into θ.

$$K_T = \{\alpha \in v \mid \alpha T = 0\}.$$

To see that K_T is a subspace of v, let $\alpha, \beta \in K_T$, and $C \in F$. Then

$$(\alpha + \beta)T = \alpha T + \beta T = \theta + \theta = \theta,$$

so that $\alpha + \beta \in K_T$, also $(C\ \alpha)T = C(\alpha\ T) = \theta$, so $c\ \alpha \in K_T$,

Thus K_T is a subspace of v.

These two subspaces, R_T and K_T, are called respectively the range space of T and the null space of T.

The range space R_T of a linear transformation T is the set of all images $\alpha T \in w$ as ranges over v. The rank p (T) of a linear transformation T is the dimension of its range space.

The nullity v (T) of a linear transformation T is the dimension of its null space.

Consider an n dimensional vector space v_n. If T is a linear transformation from v_n to w, then

$$P(T)\ = v(T) = n$$

Notes

Theorem 2: Let $\{\alpha_1, \alpha_2, ...\alpha_{v(T)}\}$ be a basis for K_T. Extend this basis to any basis $\{\alpha_1, \alpha_2, ...\alpha_{v(T)}, \alpha_{v(T)+1}, ... \alpha_n\}$ for v_n.

Then $\{\alpha_{v(T)+1} T, ..., \alpha_n T\}$ is a basis for R_T.

Proof: Let $\{\alpha_1, \alpha_2, ...\alpha_v\}$ be any basis for v_n. Any vector of R_T is of the form ξT for some $\xi \in V_n$. Let

$$\xi T = \sum_{i=1}^{n} a_1 \alpha_i ;$$

then

$$\xi T = \left(\sum_{i=1}^{n} a_i \alpha_i \right) T = \sum_{i=1}^{n} a_i (\alpha_i T) = \sum_{i=v(T)+1}^{n} a_i (\alpha_i T),$$

since

$$\alpha_i T = \theta \text{ for } i = 1, 2, ... v(T)$$

Hence $(\alpha_{v(T)+1} T, ..., \alpha_n T)$ spans R_T. As the dimension of R_T is not known we have to prove linear independence of the above vectors. Suppose scalars b_i, not all zero, exist such that

$$\theta = \sum_{v(T)+1}^{n} b_i (\alpha_i T) = \sum_{i=v(T)+1}^{n} b_i \alpha_i T$$

Then $\sum_{v(T)+1}^{n} b_i \alpha_i \in K_T$; but $\{\alpha_1, ...\alpha_{v(T)}\}$ spans K_T, so for suitable scalars c_i

$$\sum_{v(T)+1}^{n} b_i \alpha_i = \sum_{i=1}^{v(t)} c_i \alpha_i$$

This contradicts the linear independence of $\{\alpha_1, ...\alpha_n\}$, so the vectors $\{\alpha_{v(T)+1}, ...\alpha_n\}$ are linearly independent and therefore form a basis of R_T.

Theorem 3: If T is a linear transformation from V_n to w, then

$$p\ (T) + v(T) = n.$$

Self Assessment

1. In the space of all polynomials $p(x)$ of all degrees define mapping M and D by:

   $D\ p(x) = \frac{d}{dx} p(x), M\ p(x) = x\ p(x)$

   Find

   (i) $DM - MD$

   (ii) $M^2D^2 + MD$

2. Let v be the infinite dimensional space of all real polynomials. Let D and J be the Linear Transformation defined by

   $D\ p(x) = \frac{d}{dx} p(x)$

   $J\ p(x) = \int_0^x p(t)dt$

   for $p(x) \in v$,

Notes

Find

(i) $DJ\,p(x)$

(ii) Is $JD = DJ$?

3. Which of the following functions T from R^2 into R^2 are linear transformations?

(i) $T(x_1, x_2) = (1 + x_1, x_2)$;

(ii) $T(x_1, x_2) = (x_2, x_1)$;

(iii) $T(x_1, x_2) = (x_1^2, x_2)$;

(iv) $T(x_1, x_2) = (x_1 - x_2, 0)$.

7.3 Algebra of Linear Transformation

In the study of linear transformation from v into w it is of fundamental importance that the set of these transformations inherits a natural vector space structure.

Theorem 4: Let v and w be vector spaces over the field F. Let T and U be linear transformations from v into w. The function $(T + U)$ defined by

$$(T + U)(\alpha) = T\alpha + U\alpha$$

is a linear transformation from v into w. IF c is any element of F, the function (cT) defined by

$$(CT)(\alpha) = C(T\alpha)$$

is a linear transformation from v into w. The set of all linear transformations from v into w, together with the addition and scalar multiplication defined above is a vector space over the field F.

Proof: Suppose T and U are linear transformations from v into w and that we define $(T + U)$ as above. Then

$$\begin{aligned}(T + U)(C\alpha + \beta) &= T(C\alpha + \beta) + U(C\alpha + \beta)\\ &= C(T\alpha) + T\beta + C(U\alpha) + U\beta\\ &= C(T\alpha + U\alpha) + (T\beta + U\beta)\\ &= C(T + U)\alpha + (T + U)\beta\end{aligned}$$

which shows that $T + U$ is a linear transformation.

Similarly

$$\begin{aligned}(CT)(d\alpha + \beta) &= C[T(d\alpha + \beta]\\ &= C[d(T\alpha) + T\beta]\\ &= Cd(T\alpha) + C(T\beta)\\ &= d[c(T\alpha)] + c(T\beta)\\ &= d[(CT)\alpha] + C(T\beta)\end{aligned}$$

which shows that (CT) is a linear transformation. One must directly check that the vector addition and scalar multiplication are also satisfied along the above set of linear transformations of v into w.

We shall denote the space of linear transformations from v into w by $L(v, w)$. It is to be understood that $L(v, w)$ is defined only when v and w are vector spaces over the same field F.

Notes

Theorem 5: Let v be an n-dimensional vector space over the filed F; and let w be an m-dimensional vector space over F. Then the space $L(v, w)$ is finite dimensional and has dimension mn.

Thus let F be field, v and w vector spaces over F and L the set of all linear transformations from v into w. The system

$$£ = \{L, F, +, .; \oplus, \odot\}$$

is a vector space over F.

A special situation arises when we consider the system of all linear transformations of a vector space v into v itself £ is then a vector space in which the "vectors" are linear mappings of v into v. So we can define a product $S \odot T$ of vectors. This vector space over F in which a suitable product of vectors is defined is called an algebra of linear transformations over F.

A linear algebra £ over the field F is a system

$$£ = \{L, F, +, .; \oplus, \odot, \boxdot\}$$

which satisfies postulates:

(a) the system $\{L, F, T, ..., \oplus, \odot\}$ is a vector space over F.

(b) $\boxdot$ is a binary operation on £, which is closed, associative and bilinear

i.e.

closed $T_1, T_2 \in £$

Associative $T_1(T_2T_3) = (T_1T_2)T_3$

Bilinear $T_1(aT_2 + bT_3) = aT_1T_2 + bT_1T_3$

$(aT_2 + bT_3)\ T_1 = aT_2T_1 + bT_3T_1$

Also the dimension of £ is defined to be its dimension as a vector space.

Theorem 6: Let v, w and z be vector spaces over the field F. Let T be a linear transformation from v into w and u a linear transformation from w into z. Then the composed function UT defined by $(UT)\ (\alpha) = U(T(\alpha))$ is a linear transformation from v into z.

Proof:

$$\begin{aligned}(UT)\ (C\alpha + \beta) &= U[T(C\alpha + \beta)] \\ &= U(CT\alpha + T\beta) \\ &= C[U(T\alpha)] + U\ (T\beta) \\ &= C(UT)(\alpha) + (UT)(\beta)\end{aligned}$$

we shall be primarily concerned with linear transformation of a vector space into itself. So we from now on we write 'T is a linear operator on V' instead of writing 'T is a linear transformation from v into V'.

Definition: If v is a vector space over the field, a linear operator on v is a linear transformation from v into v.

Lemma: Let v be a vector space over the field F; let U, T_1 and T_2 be linear operators on v; let c be an element of F.

(a) $IU = UI = U$;

(b) $U(T_1 + T_2) = UT_1 + UT_2$; $(T_1 + T_2)\ U = T_1U + T_2U$;

(c) $C(UT_1) = (eU)\ T_1 = U(eT_1)$.

Notes

Proof: (a) This property of the identity function is obvious. We have stated here merely for emphasis.

(b)

$$[U(T_1 + T_2)](\alpha) = U[(T_1 + T_2)(\alpha)]$$
$$= U(T_1\alpha + T_2\alpha)$$
$$= U(T_1\alpha)] + U(T_2\alpha)$$
$$= (UT_1)(\alpha) + (UT_2)(\alpha)$$

so that

$$U(T_1 + T_2) = UT_1 + UT_2$$

Also
$$[(T_1 + T_2)U](\alpha) = (T_1 + T_2)(U\alpha)$$
$$= T_1(U\alpha)] + T_2(U\alpha)$$
$$= (T_1U)(\alpha) + (T_2U)(\alpha)$$

so that $(T_1 + T_2)U = T_1U + T_2U$.

(c) It is easy to prove (c) in a simple way.

Non-singular Transformations

A linear transformation T from v and w is said to be non-singular transformation if and only if there exists a mapping T^* from R_T onto v such that $TT^* = I$, where I is the identity mapping on V. Thus $T^* = T^{-1}$. Thus $TT^{-1} = T^{-1}T = I$, T^{-1} is called inverse of T.

The function T from v into w is called invertible if there exists a function U from w into v such that UT is the identity function on v and TU is the identity function on w. If T is invertible, the function U is unique and is denoted by T^{-1}. Further more T is invertible if and only if

1. T is 1:1, that is, $T\alpha = T\beta$ implies $\alpha = \beta$;
2. T is onto, that is, the range of T is w.

Theorem 7: Let v and w be vector spaces over the field F and let T be a linear transformation from v into w. If T is invertible, then the inverse function T^{-1} is a linear transformation from w onto v.

Proof: What we are proving here is that if a linear transformation T is invertible, then the inverse T^{-1} is also linear.

Let β_1 and β_2 be vectors in w and let c be a scalar. We wish to show that

$$T^{-1}(C\beta_1 + \beta_2) = CT^{-1}\beta_1 + T^{-1}\beta_2$$

Let $\alpha_i = T^{-1}\beta_i$, $i = 1, 2$, that is, let α_i be the unique vector in v such that $T\alpha_i = \beta_i$. Since T is linear,

$$T(C\alpha_1 + \alpha_2) = CT\alpha_1 + T\alpha_2$$
$$= C\beta_1 + \beta_2.$$

Thus $C\alpha_1 + \alpha_2$ is the unique vector in v which is sent by T into $C\beta_1 + \beta_2$ and so

$$T^{-1}(C\beta_1 + \beta_2) = C\alpha_1 + \alpha_2$$
$$= CT^{-1}\beta_1 + T^{-1}\beta_2$$

and thus T^{-1} is linear.

Notes

Theorem 8: Let T be a linear transformation on v_n to w_n the following statements are equivalent.

1. T is non-singular
2. For all $\alpha, \beta \in v_n$, if $\alpha T = \beta T$, then $\alpha = \beta$.
3. $K_T = [\theta]$
4. $v(T) = 0$
5. T is onto, that is, the range of T is w_n i.e. $p(T) = n$.
6. T maps any basis for v_n onto a basis for w_n.

Proof: Let n = dim v = din w. Now

rank (T) + nullity (T) = n

Since T is non-singular if and only if nullity (T) = 0 and rank (T) = n. Therefore T is non-singular if and only if $T(v_n) = w_n$. So, if either condition (1) or (2) holds the other is satisfied as well and T is invertible.

The above equations are also equivalent, there is some basis $(\alpha_1, \alpha_2, \alpha_n)$ for v such that $(T\alpha_1, T\alpha_2, ..., T\alpha_n)$ is basis for w.

Example 10: Let F be a field and let T be the linear operator on F^2 defined by

$$T(x_1, x_2) = (x_1, x_2, x_1)$$

Then T is non-singular.

Proof: If T is singular than $T(x_1, x_2) = 0$, means we have

$$x_1 + x_2 = 0$$

$$x_1 = 0$$

so the solution is $x_1 = 0$, $x_2 = 0$. We also see that T is onto; for let (z_1, z_2) be any vector in F^2. To show that (z_1, z_2) is in the range of T we must find scalars z_1 and z_2 such that

$$x_1 + x_2 = z_1$$

$$x_1 = z_2$$

and the obvious solution is $x_1 = z_2$, $x_2 = z_1 - z_2$. This last result gives us an explicit for T^{-1}, namely

$$T^{-1}(x_1, x_2) = (z_2, z_1 - z_2)$$

Self Assessment

4. If T and U be the linear operator on R^2 defined by

   $T(x_1, x_2) = (x_2, x_1)$ and $U(x_1, x_2) = (x_1, 0)$

   give rules like the ones defining T and U for each of the transformations

   (i) $U + T$

   (ii) UT

   (iii) TU

Notes

5. Let T be the unique linear operator on C^3 for which

$T\in_1 = (1, 0, i)$, $T\in_2 = (0, 1, 1,)$ $T\in_3 = (i, 1, 0)$.

Is T invertible?

7.4 Summary

- The properties of linear transformations are important in understanding the properties of the vector space.
- The basis vectors play an important part in the study of linear transformations.
- It is also explained that not all transformations are linear.
- A linear transformation T from a vector space V to a vector space W, both over the same field is a mapping of V onto W such that for all $\alpha, \beta \in V$ and for all $a, b, \in F$,

$$(a\alpha + b\beta)T = a(\alpha T) + b(\beta T)$$

7.5 Keywords

Homomorphism: If every vector of W is in the range of H, H is said to be homomorphism of V onto W.

Isomorphism: A one-to-one homomorphism H of V onto W is called an isomorphism. If such a mapping exists, V, and W are said to be isomorphic.

Linear Transformation: If T_1 is a linear transformation of v into w and T_2 is the linear transformation of w into z space, then $T_1 T_2$ is a linear transformation of v into z.

7.6 Review Questions

1. Let T be a linear transformation on R^3 defined by

$T(x_1, x_2, x_3) = (3x_1, x_1 - x_2, 2x_1 + x_2 + x_3)$

(a) Is T invertible? If so, find a rule for T^{-1} like the one which defines T.

(b) Find the value of

$(T^2 - I)(T - 3I)(x_1, x_2, x_3)$.

2. Let $C^{2\times2}$ be the complex vector space of 2 × 2 matrices with complex entries. Let

$$B = \begin{bmatrix} 1 & -1 \\ -4 & 4 \end{bmatrix}$$

and let T be a linear operator on $C^{2\times2}$ defined by

$$T(A) = BA - AB$$

for any $A \in C^{2\times2}$. What is the rank of T?

3. A transformation T on vector $\vec{V}$ of a vector space w is defined by

$$T(\vec{V}) + \vec{A} \times \vec{V}$$

where the given vector $\vec{A} \in W$ and 'x' means the vector product. Find

$$(T^2 + A^2T)(\vec{V}).$$

Answers: Self Assessment **Notes**

1. (i) I $\rightarrow$ identity transformation
   (ii) $(MD)^2$
2. (i) $DJ\ p(x) = I\ p(x)$
   (ii) no $JD \neq DJ$
3. (ii), (iv) are linear transformations.
4. (i) $(U + T)\ (x_1, x_2) = (x_1 + x_2, x_1)$
   (ii) $(U + T)\ (x_1, x_2) = (x_2, 0)$
   (iii) $(TU)\ (x_1, x_2) = (0, x_1)$
5. Yes T is invertible as $\in_1, \in_2, \in_3$ are standard basis of C^3 space.

7.7 Further Readings

Books Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I.N. Herstein, *Topics in Algebra*

Michael Artin, *Algebra.*

Notes

Unit 8: Isomorphism

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand the linear transformation T is such that T transforms a subspace S of independent vectors of vector space into an independent subspace $T(S)$ of W.
- See that isomorphism is a homomorphism if the linear transformation T on V onto W is one-one.
- Know that for finite vector space the linear transformation T is non-singular if and only if dim V = dim W and T is isomorphism of V onto W.

Introduction

In dealing with two vector spaces over the same field, a transformation T from V into W can be homomorphism or isomorphism.

After studying this unit one can see that a fine n-dimensional vector space and a space of n-tuple co-ordinate space over the same field are isomorphic and so studying of one space gives all information about the other space.

8.1 Isomorphism

If V and W are vector spaces over the field F, any one-one linear transformation T of V onto W is called an isomorphism of V onto W. If there exists an isomorphism of V onto W, we say that V is isomorphic to W.

Note that V is trivially isomorphic to V, the identity transformation operator being an isomorphism of V onto V. Also, if V is isomorphic to W via an isomorphism T, then W is isomorphic to V, because then T is invertible and so T^{-1} is an isomorphism of W onto V. Thus it is easily verified that if V is isomorphic to W and W is isomorphic to Z, then V is isomorphic to Z. Briefly, isomorphism is an equivalence relation on the class of vector spaces. If there exists an isomorphism of V onto W, we sometimes say that V and W are isomorphic.

Theorem 1: Every n-dimensional vector space V_n over the field F is isomorphic to the space F^n.

Proof: Let V_n be an n-dimensional space over the field F and let $\beta = (\alpha_1, \alpha_2 ... \alpha_n)$ be the ordered basis for V. We defined a function T from V into F^n, as follows:

Notes

If α vector is *V*, let $T\alpha$ be the *n*-tuple $(x_1, x_2 ... x_n)$ of co-ordinates of α relative to the ordered basis β, i.e. the *n*-tuple such that

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + ... + x_n\alpha_n.$$

given α in *V*, there is a unique *n*-tuple $(x_1, x_2 ... x_n)$ of scalars. Thus *n*-tuple is unique, because if we also have

$$\alpha = \sum_{i=1}^{n} z_i d_i$$

then $$\sum_{i=1}^{n} (x_i - z_i) d_i = 0$$

and the linear independence of the α, tells us that $x_i - z_i = 0$ for each *i*. We call the *i*th co-ordinate of α relative to the ordered basis

$$\beta = \{\alpha_1, \alpha_2, ... \alpha_n\}$$

Let another vector γ be given by

$$\gamma = \sum_{i=1}^{n} y_i \alpha_i$$

then $$\alpha + \gamma = \sum_{i=1}^{n} (x_i + y_i)\alpha_i$$

that the *i*th co-ordinate of $(\alpha + \gamma)$ in this ordered basis β is $(x_i + y_i)$. Similarly the *i*th co-ordinate of $(c\alpha)$ is $c\alpha_i$. One should note that every *n*-tuple $(x_1, x_2, ... x_n)$ in F^n is the *n*-tuple of co-ordinates of some vector in *V*. Thus, there is a one-one correspondence between the set of all vectors in *V* and the set of all *n*-tuples in F^n.

For many purposes one often regards isomorphic vector spaces as being the same, although the vectors and operations in the spaces may be quite different, that is, one often identifies isomorphic spaces. Let us denote the space of linear transformation from *V* into *W* by *L*(*V*,*W*) over the same field *F*.

A Few Comments and Theorems

Suppose *T* is an isomorphism of *V* onto *W*. If *S* is a subset of *V*, then we have the following theorem:

Theorem 2: Let *T* be a linear transformation from *V* into *W*. Then *T* is non-singular if and only if *T* carries each linearly independent subset of *V* onto a linearly independent sub-set of *W*.

Proof: First suppose that *T* is non-singular. Let *S* be a linearly independent subset of *V*. If $\alpha_1, \alpha_2, ... \alpha_n$ are vectors in S, then the vectors $T\alpha_1, T\alpha_2, ... T\alpha_k$ are linearly independent, for if

$$c_1(T\alpha_1) + c_2(T\alpha_2) + ... + c_k(T\alpha_k) = 0$$

Notes

then $T(c_1\alpha_1 + c_2\alpha_2 + ... + c_k\alpha_k) = 0$

and since T is non-singular

$$c_1\alpha_1 + c_2\alpha_2 + ... + c_k\alpha_k = 0$$

from which it follows that each $c_i = 0$, because S is an independent set. The argument shows that the image of S under T is independent.

Suppose that T carries independent subsets onto independent subsets. Let α be a non-zero vector in V. Then the set S consisting of the one vector α is independent. The image of S is the set consisting of the one vector $T\alpha$, and this set is independent. Therefore $T\alpha \neq 0$, because the set consisting of the zero vector alone is dependent. This shows that the null space of T is zero subspace i.e., T is non-singular.

Thus in deciding whether S is independent it does not matter whether we look at S or $T(S)$. From this one sees that an isomorphism is 'dimension preserving', that is any finite-dimensional subspace of V has the same dimension as the image under T. Here is a very simple illustration of this idea. Suppose A is an $m \times n$ matrix over the field F. We have really given two definitions of the solution space of the matrix A. The first is the set of all n-tuples $(x_1, x_2 ... x_n)$ in F^n which satisfy each of the equations in the system $AX = 0$. The second is the set of all $n \times 1$ column matrices X such that $AX = 0$. The first solution space is thus a subspace of F^n and the second is a subspace of the space of all $n \times 1$ matrices over F. Now there is a completely obvious isomorphism between F^n and F^{n+1}, namely

$$(x_1, x_2, ... x_n) \rightarrow \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}.$$

Under this isomorphism, the first space of A is carried onto the second solution space. These spaces have the same dimension, and so if we want to prove a theorem about the dimension of the solution space, it is immaterial which space we choose to discuss.

Example 1: $F^{(n)}$ is isomorphic $F^{(m)}$ if and only if $n = m$.

Proof: Here $F^{(n)}$ has, as one basis, the set of n vectors (1, 0, 0, …, 0), (0, 1, …, 0), … (0, 0, …, 1). Likewise $F^{(m)}$ has a basis containing m vectors. An isomorphism maps a basis of $F^{(n)}$ onto a basis of $F^{(m)}$. This is only possible if the dimensions of $F^{(n)}$ and $F^{(m)}$ are the same. Hence $n = m$.

Example 2: Prove that

(a) $F^{(1)}$ is not isomorphic to $F^{(n)}$ for $n > 1$.

(b) $F^{(2)}$ is not isomorphic to $F^{(3)}$.

Example 3: Let $V = C$ be the set of complex numbers, remembering only the addition of two elements as $\alpha + \beta$ and multiplication r α of a complex element α by a real number. Then the linear transformation T mapping $R^2 \rightarrow C$ sending $(a, b) \rightarrow a + b\,i$ is an isomorphism.

Notes

Example 4: Let $F^{n\times n}$ denote the set of $n \times n$ matrices with entries in a field F. This set is a vector space over F and it is isomorphic to the space of column vectors of length n^2.

Self Assessment

1. Show that $F^{m\times n}$ is isomorphic to F^{mn}.
2. Let V be the set of complex numbers regarded as a vector space over the field of real numbers. Define a function T from V into the space of 2 × 2 real matrices, as follows. If $z = x + iy$ with x and y real numbers, then

$$T(z) = \begin{bmatrix} x+7y & 5y \\ -10y & x-7y \end{bmatrix}.$$

   (a) Verify that $T(z_1 z_2) = T(z_1)T(z_2)$

   (b) Verify that T is a one-one (real) linear transformation of V into the space of 2×2 real matrices.

8.2 Summary

- A homomorphism is a mapping T of the space V into W over the same field F, preserving all the algebraic structures of the system. If T, in addition is one-to-one we call the mapping an isomorphism.
- Two spaces V and W are isomorphic only if the dim V = dim W.

8.3 Keywords

Isomorphism: T is an isomorphism of V into W over the same field F if T transforms a subset S of independent vectors into $T(S)$ a set of independent vectors of W.

Transformation: A transformation T of the space V into W is isomorphic if T is a non-singular transformation.

8.4 Review Questions

1. Let U and V be finite dimensional vector space over the field F. Prove that U and V are isomorphic if and only if dim U = dim V.
2. Let V and W be vector spaces over the field F and let T_1 be an isomorphism of V onto W. Prove that $T_2 \to T_1 T_2 T_1^{-1}$ is an isomorphism of $L(V,V)$ onto $L(W,W)$.

8.5 Further Readings

Books

Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I.N. Herstein, *Topics in Algebra*

Notes

Unit 9: Representation of Transformations by Matrices

CONTENTS

Objectives

After studying this unit, you will be able to:

- Know that the matrix of the linear transformation depends on the basis vectors of V as well as basis vectors of W where T is a linear transformation from V to W.
- See that the matrix of T depends upon the ordered basis relative to β and β' and the matrix of T relative to ordered basis β is different from the previous matrix.
- See that when T defines a transformation from V to V then the idea of similar matrices does come up.
- Understand how to find the matrix of T with the help of detailed solved examples.

Introduction

With the help of linear transformation one can deduce the rules for addition of matrices and multiplication of two matrices.

One can also understand geometrically the meaning of linear transformation clearly.

9.1 Representation of Transformations by Matrices

Although we have been discussing linear transformations for some time, it has always been in a detached way; to us a linear transformation has been a symbol (very often T) which acts in a certain way on a vector space. When one gets right down to it, outside of the few concrete examples encountered in the problems, we have really never come face to face with specific linear transformations. At the same time it is clear that if one were to pursue the subject further there would often arise the need of making a thorough and detailed study of a given linear transformation. To mention one precise problem, presented with a linear transformation; how does go about, in a "practical" and computable way, finding its characteristic roots?

What we seek first is a simple notation, or, perhaps more accurately, representation, for linear transformations. We shall accomplish this by use of a particular basis of the vector space and by

Notes

use of the action of a linear transformation on this basis. Once this much is achieved by means of the operations in $A(V)$, we can induce operations for the symbols created, making of them an algebra. This new object, infused with an algebraic life of its own, can be studied as a mathematical entity having an interest by itself. This study is what comprises the subject of matrix theory.

However to ignore the source of these matrices, that is, to investigate the set of symbol independently of what they represent, can be costly. Instead we shall always use the interplay between the abstract, $A(V)$, and the concrete, the matrix algebra, to obtain information one about the other.

Let V be an n-dimensional vector space over the field F and let W be an m-dimensional vector space over F. Let $\mathcal{B} = \{\alpha_1, ..., \alpha_n\}$ be an ordered basis for V and $\mathcal{B}' = \{\beta_1, ..., \beta_m\}$ an ordered basis for W. If T is any linear transformation from V into W, then T is determined by its action on the vectors α_j. Each of the n vectors $T\alpha_j$ is uniquely expressible as a linear combination

$$T\alpha_j = \sum_{i=1}^{m} A_{ij}\beta_i \qquad ...(1)$$

of the β_i the scalars $A_{ij}, ...A_{mj}$ being the coordinates of $T\alpha_j$ in the ordered basis $\mathcal{B}'$. Accordingly, the transformation T is determined by the mn scalars A_{ij} via the formula (1). The $m \times n$ matrix A defined by $A(i, j) = A_{ij}$ is called the matrix of T relative to the pair of ordered basis $\mathcal{B}$ and $\mathcal{B}'$. Our immediate task is to understand explicitly how the matrix A determines the linear transformation T.

If $\alpha = x_1\alpha_1 + ... + x_n\alpha_n$ is a vector in V, then

$$T\alpha = T\left(\sum_{j=1}^{n} x_j\alpha_j\right)$$

$$= \sum_{j=1}^{n} x_j\left(T\alpha_j\right)$$

$$= \sum_{j=1}^{n} x_j \sum_{j=1}^{m} A_{ij}\beta_i$$

$$= \sum_{i=1}^{m} \left(\sum_{j=1}^{n} A_{ij}x_j\right)\beta_i.$$

If X is the coordinate matrix of α in the ordered basis β, then the computation above shows that AX is the coordinate matrix of the vector $T\alpha$ in the ordered basis β' , because the scalar

$$\sum_{j=1}^{n} A_{ij}x_j$$

is the entry in the ith row of the column matrix AX. Let us also observe that if A is any $m \times n$ matrix over the field F, then

Notes

$$T\left(\sum_{j=1}^{n} x_j \alpha_j\right) = \sum_{i=1}^{m}\left(\sum_{j=1}^{n} A_{ij} x_j\right)\beta_i \qquad ...(2)$$

defines a linear transformation T from V into W, the matrix of which is A, relative to $\mathcal{B}$, $\mathcal{B}'$.

Theorem 1: Let V be an n-dimensional vector space over the field F and W an m-dimensional vector space over F. Let $\mathcal{B}$ be an ordered basis for V and $\mathcal{B}'$ an ordered basis for W. For each linear transformation T from V into W, there is an $m \times n$ matrix A with entries in F such that

$$[T\alpha]\mathcal{B}' = A[\alpha]\mathcal{B}$$

for every vector α in V. Furthermore, $T \to A$ is a one-one correspondence between the set of all linear transformations from V into W and the set of all $m \times n$ matrices over the field F.

The matrix A which is associated with T in Theorem 1 is called the matrix of T relative to the ordered basis $\mathcal{B}, \mathcal{B}'$. Note that Equation (1) says that A is the matrix whose columns $A_1, ..., A_n$ are given by

$$A_j = \left[T\alpha_j\right]\mathcal{B}', \quad j = 1, ..., n.$$

If U is another linear transformation from V into W and B $\left[B_1, ..., B_n\right]$ is the matrix of U relative to the ordered basis $\mathcal{B}, \mathcal{B}'$ then $cA + B$ is the matrix of $cT + U$ relative $\mathcal{B}, \mathcal{B}'$. That is clear because

$$cA_j + B_j = c\left[T\alpha_j\right]\mathcal{B}' + \left[U\alpha_j\right]\mathcal{B}'$$

$$= \left[cT\alpha_j + U\alpha_j\right]\mathcal{B}'$$

$$= \left[(cT + U)\alpha_j\right]\mathcal{B}'.$$

Theorem 2: Let V be an n-dimensional vector space over the field F and let W be an m-dimensional vector space over F. For each pair of ordered bases $\mathcal{B}, \mathcal{B}'$ for V and W respectively, the function which assigns to a linear transformation T its matrix relative to $\mathcal{B}, \mathcal{B}'$ is an isomorphism between the space $L(V, W)$ onto the set of $m \times n$ matrices over the field F.

Proof: We observed above that the function in question is linear, and as stated in Theorem 1, this function is one-one and maps $L(V, W)$ onto the set of $m \times n$ matrices.

We shall be particularly interested in the representation by matrices of linear transformations of a space into itself, i.e., linear operators on a space V. In this case it is most convenient to use the same ordered basis in each case, that is, to take $\mathcal{B} = \mathcal{B}'$. We shall then call the representing matrix simply the matrix of T relative to the ordered basis $\mathcal{B}$. Since this concept will be so important to us, we shall review its definition. If T is a linear operator on the finite-dimensional vector space V and $\mathcal{B} = \{\alpha_1, ..., \alpha_n\}$ is an ordered basis for V, the matrix of T relative to $\mathcal{B}$ (or, the matrix of T in the ordered basis $\mathcal{B}$) is the $n \times n$ matrix A whose entries A_{ij} are defined by the equations

$$T\alpha_j = \sum_{i=1}^{n} A_{ij}\alpha_i, \quad j = 1, ..., n \qquad ...(3)$$

One must always remember that this matrix representing T depends upon the ordered basis $\mathcal{B}$, and that there is a representing matrix for T in each ordered basis for V. (For transformations of

Notes

one space into another the matrix depends upon two ordered bases, one for V and one for W). In order that we shall not forget this dependence, we shall use the notation

$$[T]_{\mathcal{B}}$$

for the matrix of the linear operator T in the ordered basis $\mathcal{B}$. The manner in which this matrix and the ordered basis describe T is that for each α in V

$$[T_\alpha]_{\mathcal{B}} = [T]_{\mathcal{B}}[\alpha]_{\mathcal{B}}.$$

Example 1: Let V be the space of $n\times1$ column matrices over the field F; let W be the space of $m \times 1$ matrices over F; and let A be a fixed $m \times n$ matrix over F. Let T be the linear transformation of V into W defined by $T(X) = AX$. Let β be the ordered basis for V analogous to the standard basis in F^n, i.e., the i^{th} vector in $\mathcal{B}$ in the $n \times 1$ matrix X_i with a 1 in row i and all other entries 0. Let $\mathcal{B}'$ be the corresponding ordered basis for W, i.e. the jth vector in $\mathcal{B}'$ is the $m\times1$ matrix Y_i with a 1 in row j and all other entries 0. Then the matrix of T relative to the pair $\mathcal{B},\mathcal{B}'$ is the matrix A itself. This is clear because the matrix AX_j is the j^{th} column of A.

Example 2: Let F be a field and let T be the operator of F^2 defined by

$$T(x_1,x_2) = (x_1,0).$$

It is easy to see that T is a linear operator in F^2. Let $\mathcal{B}$ be the standard ordered basis for $F^2, \mathcal{B} = \{\in_1,\in_2\}$. Now

$$T\in_1 = T(1,0) = (1,0) = 1_{\in_1} + 0_{\in_2}$$

$$T\in_2 = T(0,1) = (0,0) = 0_{\in_1} + 0_{\in_2}$$

so the matrix of T in the ordered basis $\mathcal{B}$ is

$$[T]_{\mathcal{B}} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

Example 3: Let V be the space of all polynomial functions from R into R of the form

$$f(x) = c_0 + c_1x + c_2x^2 + c_3x^3$$

that is, the space of polynomial functions of degree three or less. The differentiation operator D maps V into V, since D is 'degree' decreasing'. Let $\mathcal{B}$ be the ordered basis for V consisting of the four functions f_1, f_2, f_3, f_4 defined by $f_i(x) = x^{i-1}$. Then

$$(Df_1)(x) = 0, \qquad Df_1 = 0f_1 + 0f_2 + 0f_3 + 0f_4$$

$$(Df_2)(x) = 1, \qquad Df_2 = 1f_1 + 0f_2 + 0f_3 + 0f_4$$

$$(Df_3)(x) = 2x, \qquad Df_3 = 0f_1 + 2f_2 + 0f_3 + 0f_4$$

$$(Df_4)(x) = 3x^2, \qquad Df_4 = 0f_1 + 0f_2 + 3f_3 + 0f_4$$

Notes

so that the matrix of D in the ordered basis $\mathcal{B}$ is

$$[D]_{\mathcal{B}} = -\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

We have seen what happens to representing matrices when transformations are added, namely, that the matrices add. We should now like to ask what happens when we compose transformations. More specifically, let V, W and Z be vector spaces over the field F of respective dimensions n, m and p. Let T be a linear transformation from V into W and U a linear transformation from W into Z. Suppose we have ordered basis

$$\mathcal{B} = \{\alpha_1, ..., \alpha_n\}, \quad \mathcal{B}' = \{\beta_1, ..., \beta_m\}, \quad \mathcal{B}'' = \{\gamma_1, ..., \gamma_p\}$$

for the respective spaces V, W and Z. Let A be the matrix of T relative to the pair $\mathcal{B}', \mathcal{B}$ and let $\mathcal{B}$ be the matrix of U relative to the pair $\mathcal{B}'', \mathcal{B}'$. It is then easy to see that the matrix C of the transformation UT relative to the pair $\mathcal{B}, \mathcal{B}''$ is the product of B and A; for, if α is any vector in V.

$$[T\alpha]_{\mathcal{B}'} = A[\alpha]_{\mathcal{B}}$$

$$[U(T\alpha)]_{\mathcal{B}''} = B[T\alpha]_{\mathcal{B}'}$$

and so $[(UT)(\alpha)]_{\mathcal{B}''} = BA[\alpha]_{\mathcal{B}}$

and hence, by the definition and uniqueness of the representing matrix, we must have $C = BA$. One can also see this by carrying out the computation

$$(UT)(\alpha_j) = U(T\alpha_j)$$

$$= U\left(\sum_{k=1}^{m} A_{kj}\beta_k\right)$$

$$= \sum_{k=1}^{m} A_{kj}(U\beta_k)$$

$$= \sum_{k=1}^{m} A_{kj} \sum_{i=1}^{p} B_{ik}\gamma_i$$

$$= \sum_{i=1}^{p} \left(\sum_{k=1}^{m} B_{ik}A_{kj}\right)\gamma_i$$

so that we must have

$$C_{ij} = \sum_{k=1}^{m} B_{ik}A_{kj}. \qquad ...(4)$$

Notes

We motivated the definition (4) of matrix multiplication via operations on the rows of a matrix. One sees here that a very strong motivation for the definition is to be found in composing linear transformations. Let us summarize formally.

Theorem 3: Let V, W, and Z be finite-dimensional vector spaces over the field F; let T be a linear transformation from V into W and U a linear transformation from W into Z. If $\mathcal{B}$,$\mathcal{B}'$ and $\mathcal{B}''$ are ordered basis for the spaces V, W and Z respectively, if A is the matrix of T relative to the pair $\mathcal{B}$,$\mathcal{B}'$ and $\mathcal{B}''$ is the matrix of U relative to the pair $\mathcal{B}'$,$\mathcal{B}''$, then the matrix of the composition UT relative to the pair $\mathcal{B}$, $\mathcal{B}''$ is the product matrix $C = BA$.

We remark that Theorem 3 gives a proof that matrix multiplication is associative – a proof which requires no calculations.

It is important to note that if T and U are linear operators on a space V and we are representing by a single ordered basis $\mathcal{B}$, then Theorem 3 assumes the simple form $[UT]_{\mathcal{B}} = [U]_{\mathcal{B}}[T]_{\mathcal{B}}$. Thus in this case, the correspondence which $\mathcal{B}$ determines between operators and matrices is not only a vector space isomorphism but also preserve products. A simple consequence of this is that the linear operator T is invertible if and only if $[T]_{\mathcal{B}}$ is an invertible matrix. For, the identity operator I is represented by the identity matrix in any order basis, and thus

$$UT = TU = I$$

is equivalent to

$$[U]_{\mathcal{B}}[T]_{\mathcal{B}} = [T]_{\mathcal{B}}[U]_{\mathcal{B}} = I.$$

Of course, when T is invertible

$$\left[T^{-1}\right]_{\mathcal{B}} = [T]_{\mathcal{B}}^{-1}.$$

Now we should like to inquire what happens to representing matrices when the ordered basis is changed. For the sake of simplicity, we shall consider this question only for linear operators on a space V, so that we can use a single ordered basis. The specific question is this. Let T be a linear operator on the finite-dimensional space V, and let

$$\mathcal{B}=\{\alpha_1,...,\alpha_n\} \text{ and } \mathcal{B}'=\{\alpha_1',...,\alpha_n'\}$$

be two ordered basis for V. How are the matrices $[T]_{\mathcal{B}}$ and $[T]_{\mathcal{B}'}$ related? There is a unique (invertible) $n \times n$ matrix P such that

$$[\alpha]_{\mathcal{B}} = P[\alpha]_{\mathcal{B}'} \qquad ...(5)$$

for every vector α in V. It is the matrix $P = [P_1,...,P_n]$ where $Pj = \left[\alpha_j'\right]_{\mathcal{B}}$. By definition

$$[T\alpha]_{\mathcal{B}} = [T]_{\mathcal{B}}[\alpha]_{\mathcal{B}}. \qquad ...(6)$$

Applying (5) to the vector $T\alpha$, we have

$$[T\alpha]_{\mathcal{B}} = P[T\alpha]_{\mathcal{B}'}. \qquad ...(7)$$

Combining (5), (6) and (7), we obtain

$$[T]_{\mathcal{B}} P[\alpha]_{\mathcal{B}'} = P[T\alpha]_{\mathcal{B}'}$$

$$P^{-1}[T]_{\mathcal{B}} P[\alpha]_{\mathcal{B}'} = [T\alpha]_{\mathcal{B}'}$$

Notes

and so it must be that

$$[T]_{\mathcal{B}'} = P^{-1}[T]_{\mathcal{B}} P. \qquad ...(8)$$

This answers our questions.

Before stating this result formally, let us observe the following. There is a unique linear operator U which carries $\mathcal{B}$ onto $\mathcal{B}'$, defined by

$$U\alpha_j = \alpha'_j, \quad j = 1,...,n$$

This operator U is invertible since it carries a basis for V onto a basis for V. The matrix P (above) is precisely the matrix of the operator U in the ordered basis $\mathcal{B}$. For, P is defined by

$$\alpha'_j = \sum_{i-1}^{n} P_{ij}\alpha_i$$

and since $U\alpha_j = \alpha'_j$, this equation can be written as

$$U\alpha_j = \sum_{i=1}^{n} P_{ij}\alpha_i.$$

So P = $[U]_{\mathcal{B}}$, by definition.

Theorem 4: Let V be a finite-dimensional vector space over the field F, and let

$$B = \{\alpha_1,...,\alpha_n\} \text{ and } \mathcal{B}' = \{\alpha'_1,...,\alpha'_n\}$$

be ordered basis for V. Suppose T is linear operator on V. If $P = \{P_1,...,P_n\}$ is the $n \times n$ matrix with columns $P_j = P^{-1}[T]_{\mathcal{B}}$, then

$$[T]_{\mathcal{B}'} = P^{-1}[T]_{\mathcal{B}} P.$$

Alternatively, if U is the invertible operator on V defined by $U\alpha_j = \alpha'_j, j = 1,...,n$ then

$$[T]_{\mathcal{B}'} = [U]^{-1}_{\mathcal{B}'}[T]_{\mathcal{B}}[U]_{\mathcal{B}}.$$

Self Assessment

1. Let T be the linear transformation $T : R^3 \to R^3$, defined by

   $T(x,y,z) = (2y+z, x-4y, 3z)$

   find the matrix T, with respect to the basis

   $E_1 = (1,1,1), E_2 = (1,1,0)$ and $E_3 = (1,0,0)$

2. A transformation T is defined by

$$T(x,y) = \frac{1}{\sqrt{2}}\{(x-y), x+y\}$$

(i) Show that T is linear

(ii) Find the matrix M represented by T w.r.t. basis (1,0) and (0,1)

Notes

9.2 Illustrative Examples

Example 4: Let T be the linear transformation defined by

$$T(x_1, x_2) = (x, 0).$$

The matrix of T in the standard basis $\varepsilon_1 = (1,0), \varepsilon_2 = (0,1)$

is $[T]_\beta = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

Let β' be the ordered basis for R^2 given by $\varepsilon'_1 = (1,1), \varepsilon'_2 = (2,1).$

Then $\varepsilon'_1 = \varepsilon_1 + \varepsilon_2, \varepsilon'_2 = 2\varepsilon_1 + \varepsilon_2,$ so that P matrix is

$$P = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \text{ and } P^{-1} = \begin{bmatrix} -1 & 2 \\ 1 & -1 \end{bmatrix}$$

Thus $[T]_{\beta'} = P^{-1} T_\beta P$

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

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

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

We can easily check that this is correct because

$$T \in'_1 = (1,0) = -\in'_1 + \in'_2$$

$$T \in'_2 = (2,0) = -2 \in'_1 + 2 \in'_2 .$$

Example 5: Let V be the space of polynomial functions from R into R which have 'degree' less than or equal to 3. As in Example 3, let D be the differentiation operator on V, and let

$$\mathcal{B} = \{f_1, f_2, f_3, f_4\}$$

be the ordered basis for V defined by $f_1(x) = x^{i-1}$. Let t be a real number and define $g_1(x) = (x+t)^{i-1}$, that is

$$g_1 = f_1$$

Notes

$$g_2 = tf_1 + f_2$$

$$g_3 = t^2 f_1 + 2tf_2 + f_3$$

$$g_4 = t^3 f_1 + 3t^2 f_2 + 3tf_3 + f_4.$$

Since the matrix

$$P = \begin{bmatrix} 1 & t & t^2 & t^3 \\ 0 & 1 & 2t & 3t^2 \\ 0 & 0 & 1 & 3t \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

is easily seen to be invertible with

$$P^{-1} = \begin{bmatrix} 1 & -t & t^2 & -t^3 \\ 0 & 1 & -2t & 3t^2 \\ 0 & 0 & 1 & -3t \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

it follows that $\mathcal{B}' = \{g_1, g_2, g_3, g_4\}$ is an ordered basis for V. In Example 3, we found that the matrix of D in the ordered basis $\mathcal{B}$ is

$$[D]_{\mathcal{B}} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

The matrix of D in the ordered basis $\mathcal{B}'$ is thus

$$P^{-1}[D]_{\mathcal{B}} P = \begin{bmatrix} 0 & -t & t^2 & t^3 \\ 0 & 1 & -2t & 3t^2 \\ 0 & 0 & 1 & -3t \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & t & t^2 & t^3 \\ 0 & 1 & 2t & 3t^2 \\ 0 & 0 & 1 & 3t \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & -t & t^2 & t^3 \\ 0 & 1 & -2t & 3t^2 \\ 0 & 0 & 1 & -3t \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 2t & 3t^2 \\ 0 & 0 & 2 & 6t \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

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

Thus D is represented by the same matrix in the ordered basis $\mathcal{B}$ and $\mathcal{B}'$. Of course, one can see this somewhat more directly since

$$Dg_1 = 0$$

$$Dg_2 = g_1$$

Notes

$$Dg_3 = 2g_2$$

$$Dg_4 = 3g_3.$$

This example illustrates a good point. If one knows the matrix of a linear operator in some ordered basis $\mathcal{B}$ and wishes to find the matrix in another ordered basis $\mathcal{B}'$, it is often most convenient to perform the coordinate change using the invertible matrix P; however, it may be a much simpler task to find the representing matrix by a direct appeal to its definition.

Definition: Let A and B be $n \times n$ (square) matrices over the field F. We say that B is similar to A over F if there is an invertible $n \times n$ matrix P over F such that $\beta = P^{-1}AP$.

According to Theorem 4, we have the following: If V is an n-dimensional vector space over F and $\mathcal{B}$ and $\mathcal{B}'$ are two ordered bases for V_i then for each linear operator T on V the matrix $B = [T]_{\mathcal{B}'}$ is similar to the matrix $A = [T]_{\mathcal{B}'}$. The argument also goes in the other direction. Suppose A and B are $n \times n$ matrices and that B is similar to A. Let V be any n-dimensional space over F and let $\mathcal{B}$ be an ordered basis for V. Let T be the linear operator on V which is represented in the basis $\mathcal{B}$ by A. If $\beta = P^{-1}AP$, let $\mathcal{B}'$ be the ordered basis for V obtained from $\mathcal{B}$ by P, i.e.

$$\alpha_j' = \sum_{i=1}^{n} P_{ij}\alpha_i.$$

Then the matrix of T in the ordered basis $\mathcal{B}'$ will be B.

Thus the statement that B is similar to A means that on each n-dimensional space over F the matrices A and B represent the same linear transformation in two (possibly) different ordered basis.

Note that each $n \times n$ matrix A is similar to itself, using $P = I$; if B is similar to A, then A is similar to B, for $B = P^{-1}AP$ implies that $A = \left(P^{-1}\right)^{-1} BP^{-1}$; if B is similar to A and C is similar to B, then C is similar to A, for $B = P^{-1}AP$ and $C = Q^{-1}BQ$ imply that $C = (PQ)^{-1}A(PQ)$. Thus, similarity is an equivalence relation on the set of $n \times n$ matrices over the field F. Also note that the only matrix similar to the identity matrix I is I itself, and that the only matrix similar to the zero matrix is the zero matrix itself.

Self Assessment

3. Let T be the linear transformation on R^3 defined by

$$T(x_1, x_2, x_3) = (3x_1 + x_3, -2x_1 + x_2, -x_1 + 2x_2 + 4x_3)$$

(i) What is the matrix of T in the standard ordered basis for R^3?

(ii) What is the matrix of T in the ordered basis $(\alpha_1, \alpha_2, \alpha_3)$ where

$$\alpha_1 = (1,0,1), \alpha_2 = (-1,2,1) \text{and } \alpha_3 = (2,1,1)$$

4. Let T be the linear transformation from R^3 into R^2 defined by

$$T(x_1, x_2, x_3) = (x_1 + x_2, 2x_3 - x_1)$$

If B is the standard ordered basis for R^3 and β' is the standard ordered basis for R^2, what is the matrix of T relative to the pair β, β'?

Notes

9.3 Summary

- One can identify the effect of linear transformation on the space and study its effects by means of algebra of matrices.
- This way one has insight of the meaning of similar matrices.
- The linear transformation T for R^3 to R^2.

9.4 Keywords

Degree Decreasing: The differentiation operator D maps V into V, since D is 'degree' decreasing.

Linear Transformation: The statement that B is similar to A means that on each n-dimensional space over F the matrices A and B represent the same linear transformation in two (possibly) different ordered basis.

Unique Linear Operator: A unique linear operator U which carries $\mathcal{B}$ onto $\mathcal{B}'$, defined by $U\alpha_j = \alpha'_j,\ j = 1,...,n$

9.5 Review Questions

1. Let T be the linear transformation on R^2 defined by

   $T(x_1, x_2) = (-x_2, x_1)$

   (a) What is the matrix of T in the standard basis for R^2?

   (b) What is the matrix of T in the standard basis $\beta(\alpha_1, \alpha_2)$ where $\alpha_1 = (1,2)$ and $\alpha_2 = (1,-1)$?

2. Let $(\alpha_1, \alpha_2, \alpha_3)$ be the basis for V_3 and let $\beta_1 = \alpha_1 - 2\alpha_2, \beta_2 = \alpha_1 + \alpha_2 + \alpha_3, \beta_3 = \alpha_2 - \alpha_3$

   (a) Prove $(\beta_1, \beta_2, \beta_3)$ is a basis and express $\alpha_1, \alpha_2, \alpha_3$ as a linear combination of β_1, β_2 and β_3.

   (b) If T is defined by $T\alpha_i = \beta_i,\quad i = 1,2,3,...$

   find a matrix A which represents T relative to α basis.

9.6 Further Readings

Books

Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I.N. Herstein, *Topics in Algebra*

Michael Artin, *Algebra*

Unit 10: Linear Functionals

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand in a better way the discussion of subspaces, linear equations and co-ordinates.
- See that a few examples of linear functional cited in this unit.
- Know the concept of dual basic vectors for the dual vector space V^*.
- See that how to obtain the basis of the dual spaces which is done by examples.

Introduction

The concept of linear function is important in the study of finite dimensional spaces because the linear functional method helps to organize and clarify the discussion of subspaces.

The method is illustrated by means of a few theorems and a few solved examples.

10.1 Linear Functionals

If V is a vector space over the field F, a linear transformation f from V into the scalar field F is also called a **linear functional** on V. If we start from scratch, this means that f is a function from V into F such that

$$f.(c\alpha + \beta) = cf(\alpha) + f(\beta)$$

for all vectors α and β in V and all scalars c in F. The concept of linear functional is important in the study of finite-dimensional spaces because it helps to organize and clarify the discussion of subspaces, linear equations, and coordinates.

Example 1: Let F be a field and let $a_1, ..., a_n$ be scalars in F. Define a function f on F^n by

$$f(x_1,...,x_n) = a_1x_1 + ... + a_nx_n$$

Then f is a linear functional on F^n. It is the linear functional which is represented by the matrix $[a_1 \ ... \ a_n]$ relative to the standard ordered basis for F^n and the basis $\{1\}$ for F:

Notes

$$a_j = f(\varepsilon_j), \qquad j = 1, \ldots, n.$$

Every linear functional on F^n is of this form, for some scalars $a_1, \ldots, a_n$. That is immediate from the definition of linear functional because we define $a_j = f(\varepsilon_j)$ and use the linearity

$$\begin{aligned} f(x_1, \ldots, x_n) &= f\left(\sum_j x_j \varepsilon_j\right) \\ &= \sum_j x_j f(\varepsilon_j) \\ &= \sum_j a_j x_j \end{aligned}$$

Example 2: Here is an important example of a linear functional. Let n be a positive integer and F is field. If A is an $n \times n$ matrix with entries in F, the **trace** of A is the scalar

$$tr\, A = A_{11} + A_{22} + \ldots + A_{nn}.$$

The trace function is a linear functional on the matrix space $F^{n \times n}$ because

$$\begin{aligned} tr(cA + B) &= \sum_{i=1}^{n} (cA_{ii} + B_{ii}) \\ &= c\sum_{i=1}^{n} cA_{ii} + \sum_{i=1}^{n} B_{ii} \\ &= c\, tr\, A + tr\, B. \end{aligned}$$

Example 3: Let V be the space of all polynomial functions from the field F into itself. Let t be an element of F. If we define

$$L_t(p) = p(t)$$

then L_t is a linear functional on V. One usually describes this by saying that, for each t, 'evaluation at t' is a linear functional on the space of polynomial functions. Perhaps we should remark that the fact that the functions are polynomials plays no role in this example. Evaluation at t is a linear functional on the space of all functions from F into F.

Example 4: This may be the most important linear functional in mathematics. Let $[a, b]$ be a closed interval on the real line and let $C([a, b])$ be the space of continuous real-valued functions on $[a, b]$. Then

$$L(g) = \int_a^b g(t)\, dt$$

Theorem 1: Let V be an n-dimensional vector space over the field F, and let W be an m-dimensional vector space over F. Then the space $L(V, W)$ is finite-dimensional and has dimension mn.

Proof: Let

$$\beta = \{\alpha_1, \alpha_2, \ldots \alpha_n\} \text{ and } \beta' = \{\beta_1, \beta_2, \ldots \beta_n\}$$

Notes

be ordered basis for V and W, respectively. For each pair of integers (p, q) with $1 \le p \le m$ and $1 \le q \le n$, we define a linear transformation $E^{p,q}$ from V into W by

$$E^{p,q}(\alpha_i) = \begin{cases} 0 & \text{if } i \neq q \\ \beta_p & \text{if } i = q \end{cases}$$

$$= \delta_{iq}\, \beta_b$$

According to the theorem 1 of unit 7, there is a unique linear transformation from V into W satisfying these conditions. The claim is that the mn transformations $E^{p,q}$ from a basis for $L(V, W)$.

Let T be a linear transformation from V into W. For each j, $i \le j \le n$, let $A_{1j}, A_{2j}, \ldots A_{mj}$ be the co-ordinates of the vector $T\alpha_j$ in the ordered basis β', i.e.,

$$T\alpha_j = \sum_{p=1}^{m} A_{pj}\, \beta_p \qquad \ldots(1)$$

we wish to show that

$$T = \sum_{p=1}^{m}\sum_{q=1}^{n} A_{pq}\, E^{p,q} \qquad \ldots(2)$$

Let U be the linear transformation in the right hand member of (2). Then for each j

$$U\alpha_j = \sum_{p}\sum_{q} A_{pq}\, E^{p,q}(\alpha_j)$$

$$= \sum_{p}\sum_{q} A_{pq}\, \delta_{jq}\, \beta_p$$

$$= \sum_{p=1}^{m} A_{pj}\, \beta_p$$

$$= T\alpha_j$$

and consequently $U = T$. Now (2) shows that the $E^{p,q}$ span $L(V, W)$; we must prove that they are independent. But this is clear from what we did above; for, if the transformation

$$U = \sum_{p}\sum_{q} A_{pq}\, E^{p,q}$$

is the zero transformation, then $U\alpha_j = 0$ for each j, so

$$\sum_{p=1}^{m} Ap_j \beta_j = 0$$

and the independence of the β_p implies that $A_{pj} = 0$ for every p and j.

If V is finite-dimensional vector space, the collection of linear functionals of V forms a vector space in a natural way. It is the space $L(V, F)$. We denote this space by V^*. From the above theorem we know the following about the space V^* that

$$\dim V^* = \dim V. \qquad \ldots(3)$$

Notes

Let $\beta = (\alpha_1, \alpha_2, ...\alpha_n)$ be a basis for V. According to theorem 1 of unit 7, there is (for each i) a unique linear functional f_i on V such that

$$f_i(\alpha_i) = \delta_{ij} \quad ...(4)$$

In this way we obtain from β a set of n distinct linear functionals $f_1, f_2, ... f_n$ on V. These functionals are also linearly independent. For, suppose

$$f = \sum_{i=1}^{n} c_i f_i \quad ...(5)$$

Then

$$f(\alpha_j) = \sum_{i=1}^{n} c_i f_i(\alpha_j)$$

$$= \sum_{i=1}^{n} c_i \delta_{ij}$$

$$= c_j.$$

In particular, if f is the zero functional $f(\alpha_j) = 0$ for each j and hence the scalars c_j are all 0. Now $f_1, ...f_n$ are n linearly independent functionals, and since we know that V^* has dimension n, it must be that $\mathcal{B}^* = \{f_1, ..., f_n\}$ is a basis for V^*. This basis is called the dual basis of $\mathcal{B}$.

Theorem 2: Let V be a finite-dimensional vector space over the field F, and let $\mathcal{B} = \{\alpha_1, ..., \alpha_n\}$ be a basis for V. Then there is a unique dual basis $\mathcal{B}^* = \{f_1, ..., f_n\}$ for V^* such that $f_i(\alpha_j) = \delta_{ij}$. For each linear functional f on V we have

$$f = \sum_{i=1}^{n} f(\alpha_i) f_i \quad ...(6)$$

and for each vector α in V we have

$$\alpha = \sum_{i=1}^{n} f_1(\alpha)\, \alpha_i. \quad ...(7)$$

Proof: We have shown above that there is a unique basis which is 'dual' to $\mathcal{B}$. If f is a linear functional on V, then f is some linear combination (5) of the f_i, and as we observed after (5) the scalars c_j must be given by $c_j = f(\alpha_j)$. Similarly, if

$$\alpha = \sum_{i=1}^{n} x_i\, \alpha_i$$

is a vector in V, then

$$f_j(\alpha) = \sum_{i=1}^{n} x_i f_i(\alpha_i)$$

$$= \sum_{i=1}^{n} x_i \delta_{ij}$$

$$= x_j$$

Notes

so that the unique expression for α as a linear combination of the α_i, is

$$\alpha = \sum_{i=1}^{n} f_i(\alpha)\alpha_i.$$

Equation (7) provides us with a nice way of describing what the dual basis is. It says if $\mathcal{B} = \{\alpha_1, \alpha_2 ..., \alpha_n\}$ is an ordered basis for V and $\mathcal{B}^* = \{f_1, ..., f_n\}$ is the dual basis, then f_i is precisely the function which assigns to each vector α in V the ith coordinate of α relative to the ordered basis $\mathcal{B}$. Thus we may also call the f_i the coordinate functions for $\mathcal{B}$. The formula (6), when combined with tells us the following:

If f is in V^*, and we let $f(\alpha_i) = a_i$, then when

$$\alpha = x_1\alpha_1 + ... + x_n\alpha_n$$

we have

$$f(x) = a_1x_1 + ... + a_nx_n. \quad ...(8)$$

In other words, if we choose an ordered basis $\mathcal{B}$ for V and describe each vector in V by its n-tuple of coordinates $(x_1, ...x_n)$ relative to $\mathcal{B}$, then every linear functional on V has the form. This is the natural generalization of Example 1, which is the special case $V = F^n$ and $\mathcal{B} = \{\varepsilon_1, ..., \varepsilon_n\}$.

Example 5: Let V be the vector space of all polynomial functions from R into R which have degree less than or equal to 2. Let t_1, t_2 and t_3 be any three distinct real numbers, and let

$$L_i(p) = p(t_i)$$

Then L_1, L_2 and L_3 are linear functionals on V. These functionals are linearly independent; for, suppose

$$L = c_1L_1 + c_2L_2 + c_3L_3$$

If $L = 0$, i.e., if $L(p) = 0$ for each p in V, then applying L to the particular polynomial 'functions' 1, x, x^2, we obtain

$$c_1 + c_2 + c_3 = 0$$

$$t_1c_1 + t_2c_2 + t_3c_3 = 0$$

$$t_1^2c_1 + t_2^2c_2 + t_3^2c_3 = 0$$

From this it follows that $c_1 = c_2 = c_3 = 0$, because (as a short computation shows) the matrix

$$\begin{bmatrix} 1 & 1 & 1 \\ t_1 & t_2 & t_3 \\ t_1^2 & t_2^2 & t_3^2 \end{bmatrix}$$

is invertible when t_1, t_2 and t_3 are distinct. Now the L_i are independent and since V has dimension 3, these functional from a basis for V^*. What is the basis for V, of which this is the dual? Such a basis $\{p_1, p_2, p_3\}$ for V must satisfy

$$L_i(p_i) = \delta_{ij}$$

or

$$p_j(t_i) = \delta_{ij}.$$

Notes

These polynomial functions are easily shown to be

$$p_1(x) = \frac{(x-t_2)(x-t_3)}{(t_1-t_2)(t_1-t_3)}$$

$$p_2(x) = \frac{(x-t_1)(x-t_3)}{(t_2-t_1)(t_2-t_3)}$$

$$p_3(x) = \frac{(x-t_1)(x-t_2)}{(t_3-t_1)(t_3-t_2)}$$

The basis $\{p_1, p_2, p_3\}$ for V is interesting, because according to (7) we have to each p in V.

$$p = p(t_1)p_1 + p(t_2)p_2 + p(t_3)p_3.$$

Thus, if c_1, c_2 and c_3 are any real numbers, there is exactly one polynomial function p over R which has degree at most 2 and satisfies $p(t_j) = -c_j, j = 1,2,3.$ This polynomial function is $p = c_1p_1 + c_2p_2 + c_3p_3$.

Now let us discuss the relationship between linear functionals and subspaces. If f is a non-zero linear functional, then the rank of f is 1 because the range of f is a non-zero subspace of the scalar field and must (therefore) be the scalar field. If the underlying space V is finite-dimensional, the rank plus nullity theorem tells us that the null space N_f has dimension

$$\dim N_f = \dim V - 1.$$

In a vector space of dimension n, a subspace of dimension $n - 1$ is called a **hyperspace**. Such spaces are sometimes called hyperplanes or subspaces of co-dimension 1. Is every hyperspace the null space of a linear functional? The answer is easily seem to be yes. It is not much more difficult to show that each d-dimensional subspace of an n-dimensional space is the intersection of the null spaces of $(n - d)$ linear functionals (Theorem below).

Definition: If V is a vector space over the field F and S is a subset of V, the **annihilator** of S is the set $S°$ of linear functionals on V such that $f(\alpha) = 0$ for every α in S.

It should be clear that $S°$ is a subspace of V^*, whether S is a subspace of V or not. If S is the set consisting of the zero vector alone, then $S° = V^*$. If $S = V$, then $S°$ is the zero subspace of V^*. (This is easy to see when V is finite-dimensional.)

Theorem 3. Let V be a finite-dimensional vector space over the field F, and let W be a subspace of V. Then

$$\dim W + \dim W° = \dim V.$$

Proof: Let k be the dimension of W and $\{\alpha_1, ..., \alpha_k\}$ a basis for W. Choose vector $\alpha_{k+1}, ..., \alpha_n$, in V such that $\{\alpha_1,..., \alpha_n\}$ is a basis for V. Let $\{f_1, ..., f_n\}$ be the basis for V^* which is dual to this basis for V.

This claim is that $\{f_{k+1},...f_n\}$ is a basis for the annihilator $W°$. Certainly f_i belongs to $W°$ for $i \geq k + 1$, because

$$f_i(\alpha_i) = \delta_{ij}$$

and $\delta_{ij} = 0$ if $i \geq k + 1$ and $j \leq k$; from this it follows that, for $i \geq k + 1$, $f_i(\alpha) = 0$ whenever α is a linear combination of $\alpha_1,...,\alpha_k$. The functionals $f_{k+1},...,f_n$ are independent, so all we must show is that they span $W°$. Suppose f is in V^*.

Notes

Now,

$$f = \sum_{i=1}^{n} f(\alpha_i) f_i$$

so that if f is in W° we have $f(\alpha_i) = 0$ for $i \leq k$ and

$$f = \sum_{i=k+1}^{n} f(\alpha_i) f_i.$$

We have shown that if dim $W = k$ and dim $V = n$ then dim $W^\circ = n - k$.

Corollary: If W is a k-dimensional subspace of an n-dimensional vector space V, then W is the intersection of $(n - k)$ hyperspaces in V.

Proof: This is a corollary of the proof of Theorem 3 rather than its statement. In the notation of the proof, W is exactly the set of vectors α such that $f_i(\alpha) - 0$, $i = k+1,...,n$. In case $k = n - 1$, W is the null space of f_n.

Corollary: If W_1 and W_2 are subspaces of a finite-dimensional vector space, then $W_1 = W_2$ if and only if $W_1^0 = W_2^0$.

Proof: If $W_1 = W_2$, then of course $W_1^0 = W_2^0$. If $W_1 \neq W_2$, then one of then two subspaces contains a vector which is not in the other. Suppose there is a vector α which is in W_2 but not in W_1. By the previous corollaries (or the proof of Theorem 3) there is a linear functional f such that $f(\beta) = 0$ for all β in W, but $f(\alpha) \neq 0$. Then f is in W_1^0 but not in W_2^0 and $W_1^0 \neq W_2^0$.

10.2 System of Linear Equations

The first corollary says that, if we select some ordered basis for the space, each k-dimensional subspace can be described by specifying $(n - k)$ homogeneous linear conditions on the coordinates relative to that basis.

Let us look briefly at system of homogeneous linear equations from the point of view of linear functionals. Suppose we have a system of linear equations,

$$\begin{aligned} A_{11}x_1 + \cdots + A_{1n}x_n &= 0 \\ \vdots \qquad\qquad & \vdots \\ A_{m1}x_1 + \cdots + A_{mn}x_n &= 0 \end{aligned}$$

for which we wish to find the solutions. If we let f_i, $i = 1,...,m$, be the linear functional on F^n defined by

$$f_i(x_i,....,x_n) = A_{ix}x_i + ... + A_{in}x_n$$

then we are seeking the subspace of F^n of all α such that

$$f_i(\alpha) = 0, \qquad i = 1,...,m.$$

In other words, we are seeking the subspace annihilated by $f_1,...,f_m$. Row-reduction of the coefficient matrix provides us with a systematic method of finding this subspace. The n-tuple $(A_{i1},....A_{in})$ gives the coordinates of the linear functional f_i relatives to the basis which is dual to the standard basis for F^n. The row space of the coefficient matrix may thus be regarded as the space of linear functionals spanned by $f_1,...,f_m$. The solution space is the subspace annihilated by this space of functionals.

Notes

Now one may look at the system of equations from the 'dual' point of view. That is, suppose that we are given m vectors in F^n.

$$\alpha_1 = (A_{i1}, ..., A_{in})$$

and we wish to find the annihilator of the subspace spanned by these vectors. Since a typical linear functional on F^n has the form

$$f(x_1, ...x_n) = c_1x_1 + ... + c_nx_n$$

the condition that f be in this annihilator is that

$$\sum_{j=1}^{n} A_{ij}c_j = 0, \qquad i = 1, ..., m$$

that is, that $(c_1, ..., c_n)$ be a solution of the system $AX = 0$. From this point of view, row-reduction gives us a systematic method of finding the annihilator of the subspace spanned by a given finite set of vectors in F^n.

Example 6: Here are three linear functionals on R^4:

$$f_1(x_1, x_2, x_3, x_4) = x_1 + 2x_2 + 2x_3 + x_4$$

$$f_2(x_1, x_2, x_3, x_4) = 2x_2 + x_4$$

$$f_3(x_1, x_2, x_3, x_4) = -2x_1 - 4x_2 + 3x_4.$$

The subspace which they annihilate may be found explicitly by finding the row-reduced echelon form of the matrix

$$A = \begin{bmatrix} 1 & 2 & 2 & 1 \\ 0 & 2 & 0 & 1 \\ -2 & 0 & -4 & 3 \end{bmatrix}$$

A short calculation, shows that A goes over $2R$ as

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

Therefore, the linear functionals

$$g_1(x_1, x_2, x_3, x_4) = x_1 + 2x_3$$

$$g_2(x_1, x_2, x_3, x_4) = x_2$$

$$g_3(x_1, x_2, x_3, x_4) = x_4$$

span the same subspace of $(R^4)^*$ and annihilate the same subspace of R^4 as do f_1, f_2, f_3. The subspace annihilated consists of the vectors with

$$x_1 = -2x_3$$

$$x_2 = x_4 = 0$$

Notes

Example 7: Let W be the subspace of R^4 which is spanned by the vectors

$$\alpha_1 = (2, -2, 3, 4, -1) \qquad \alpha_3 = (0, 0, -1, -2, 3)$$

$$\alpha_2 = (-1, 1, 2, 5, 2) \qquad \alpha_4 = (1, -1, 2, 3, 0).$$

How does one describe W^0, the annihilator of W? Let us form the 4×5 matrix A with row vectors $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, and find the row-reduced echelon matrix R which is row-equivalent of A:

$$A = \begin{bmatrix} 2 & -2 & 3 & 4 & -1 \\ -1 & 1 & 2 & 5 & 2 \\ 0 & 0 & -1 & -2 & 3 \\ 1 & -1 & 2 & 3 & 0 \end{bmatrix} \rightarrow R = \begin{bmatrix} 1 & -1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

If f is a linear functional on R^5:

$$f(x_1, ..., x_5) = \sum_{j=1}^{5} c_j x_j$$

then f is in W° if and only if $f(\alpha_i) = 0, i = 1, 2, 3, 4,$ i.e., if and only if

$$\sum_{j=1}^{5} A_{ij} c_j = 0, \qquad 1 \le i \le 4.$$

This is equivalent to

$$\sum_{j=1}^{5} R_{ij} c_j = 0, \qquad 1 \le i \le 3$$

or

$$c_1 - c_2 - c_4 = 0$$

$$c_3 + 2c_4 = 0$$

$$c_5 = 0$$

We obtain all such linear functionals f by assigning arbitrary values to c_2 and c_4, say $c_2 = a$ and $c_4 = b$, and then finding the corresponding $c_1 = a + b$, $c_3 = -2b$, $c_5 = 0$. So W° consists of all linear functionals f of the form

$$f(x_1, x_2, x_3, x_4, x_5) = (a + b)x_1 + ax_2 - 2bx_3 + bx_4$$

The dimension of W^* is 2 the basis (f_1, f_2) for W^* can be found by first taking $a = 1$, $b = 0$ and then $a = 0$ and $b = 1$:

$$f_1(x_1, x_2, x_3, x_4, x_5) = x_1 + x_2$$

$$f_2(x_1, x_2, x_3, x_4, x_5) = x_1 - 2x_3 + x_4$$

The above general f in W^* is $f = a\, f_1 + b\, f_2$.

Notes

Self Assessment

1. Let W be the subspace of R^5 which is spanned by the vectors

$\alpha_1 = \varepsilon_1 + 2\varepsilon_2 + \varepsilon_3,\ \alpha_2 = \varepsilon_2 + 3\varepsilon_3 + 3\varepsilon_4 + \varepsilon_5$
$\alpha_3 = \varepsilon_1 + 4\varepsilon_2 + 6\varepsilon_3 + 4\varepsilon_4 + \varepsilon_5$

Find a basis for W^*.

2. Let W be the subspace spanned by R^5, which is spanned by the vectors

$\alpha_1 = (1, 2, 0, 3, 0),\ \alpha_2 = (1, 2, -1, -1, 0)$
$\alpha_3 = (0, 0, 1, 4, 0),\ \alpha_4 = (2, 4, 1, 10, 1)$
$\alpha_5 = (0, 0, 0, 0, 1)$

How does one describe W^*, the annihilator of W.

10.3 Summary

- The concept of linear functional helps us to clarify the discussion of subspaces, linear equations and co-ordinates.
- In this unit the idea of dual basis for V^* is obtained i.e. if $B = (\alpha_1, \alpha_2, ...\alpha_n)$ be the basis of V then there is a unique dual basis $\beta^* = (f_1, ...f_n)$ for V^*.
- The concept of linear functional is important in the study of finite-dimensional spaces because it helps to organize and clarify the discussion of subspaces, linear equations, and coordinates.
- Let V be the space of all polynomial functions from the field F into itself. Let t be an element of F. If we define

$$L_t(p) = p(t)$$

then L_t is a linear functional on V. One usually describes this by saying that, for each t, 'evaluation at t' is a linear functional on the space of polynomial functions.

10.4 Keywords

Dual Basis: In particular, if f is the zero functional $f(\alpha_j) = 0$ for each j and hence the scalars c_j are all 0. Now $f_1, ...f_n$ are n linearly independent functionals, and since we know that V^* has dimension n, it must be that $\mathcal{B}^* = \{f_1, ..., f_n\}$ is a basis for V^*. This basis is called the dual basis of $\mathcal{B}$.

Linear Functional: If V is a vector space over the field F, a linear transformation f from V into the scalar field F is also called a linear functional on V.

Trace: If A is an $n \times n$ matrix with entries in F, the trace of A is the scalar $tr\, A = A_{11} + A_{22} + ... + A_{nn}$.

10.5 Review Questions

1. In R^3, $\alpha_1 = (1, 0, 1)$ $\alpha_2 = (0, 1, -2)$, $\alpha_3 = (-1, -1, 0)$

If f is a linear functional on R^3 such that

Notes

$f(\alpha_1) = 1, f(\alpha_2) = -1, f(\alpha_3) = 3$

and if $\alpha = (a, b, c)$, find $f(\alpha)$.

2. Let $\beta = (\alpha_1, \alpha_2, \alpha_3)$ be the basis for C^3 defined by

$\alpha_1 = (1, 0, -1), \alpha_2 = (1, 1, 1), \alpha_3 = (2, 2, 0).$

Find the dual basis of β.

Answers: Self Assessment

1. The dimension of W^* is 2 and the basis (f_1, f_2) for W^* is given by

$f_1(x_1, x_2, ...x_5) = -4x_1 - 3x_2 + 2x_3 + x_4$
$f_2(x_1, x_2, ...x_5) = -5x_1 + 2x_2 + x_3 + x_5$

2. The dimension of W^* is 2 and the basis (f_1, f_2) for W^* is given by

$f_1(x_1, x_2, x_3, x_4, x_5) = -2x_1 + x_2$
$f_2(x_1, x_2, x_3, x_4, x_5) = -3x_1 + 4x_3 + x_4$

10.6 Further Readings

Books

Ervin Kreyszig, *Introductory Functional Analysis with Applications*

Kenneth Hoffman and Ray Kunze, *Linear Algebra*

Notes

Unit 11: The Double Dual

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand the meanings of V^* and V^{**} and their corresponding basis β^* and β^{**}.
- Know that the mapping $\alpha \to L_\alpha$ is an isomorphism of V onto V^{**}.
- See that if S is any subset of a finite dimensional vector space then $\left(S^0\right)^0$ is the subspace spanned by S.
- Understand that the T', the transpose of the linear transformation T is often called the adjoint of T; however in this unit we use only the word transpose.
- See that if A be the matrix of T relative to basis β, β' and β be the matrix of T', relative to dual basis β'^* and β^α then $B_{ij} = A_{ji}$.

Introduction

In this unit the idea of dual and double dual finite dimensional spaces and their basis vectors are explained.

Also the transpose T' of the linear transformation is introduced. The alternate name of the transpose transformation is word adjoint transformation.

11.1 The Double Dual

One question about dual bases which we did not answer in the last section was whether every basis for V^* is the dual of some basis for V. One way to answer that question is to consider V^{**}, the dual space of V^*.

Notes

If α is a vector in V, then α includes a linear functional L_α on V^* defined by

$$L_\alpha(f) = f(\alpha), \quad f \text{ in } V^*. \qquad ...(1)$$

The fact that L_α is linear is just a reformulation of the definition of linear operations in V^*:

$$\begin{aligned} L_\alpha(cf+g) &= (cf+g)(\alpha) \\ &= (cf)(\alpha) + g(\alpha) \\ &= cf(\alpha) + g(\alpha) \\ &= cL_\alpha(f) + L_\alpha(g). \end{aligned} \qquad ...(2)$$

If V is finite-dimensional and $\alpha \neq 0$, then $L_\alpha \neq 0$; in other words, there exists a linear functional f such that $f(\alpha) \neq 0$. The proof is very simple. Choose an ordered basis $\mathcal{B}=\{\alpha_1,...,\alpha_n\}$ for V such that $\alpha_1=\alpha$ and let f be the linear functional which assigns to each vector in V its first coordinate in the ordered basis $\mathcal{B}$.

Theorem 1: Let V be a finite-dimensional vector space over the field F. For each vector α in V define

$$L_\alpha(f) = f(\alpha), \quad f \text{ in } V^*.$$

The mapping $\alpha \to L_\alpha$ is then an isomorphism of V onto V^{**}.

Proof: We showed that for each α the function L_α is linear. Suppose α and β are in V and c is in F, and let $\gamma = c\alpha + \beta$. Then for each f in V^*.

$$\begin{aligned} L_\gamma(f) &= f(\gamma) \\ &= f(c\alpha+\beta) \\ &= cf(\alpha) + f(\beta) \end{aligned}$$

and so

$$\begin{aligned} &= cL_\alpha(f) + L_\beta(f) \\ L_\gamma &= CL_\alpha + L_\beta \end{aligned}$$

This shows that the mapping $\alpha \to L_\alpha$ is a linear transformation from V into V^{**}. This transformation is non-singular; for, according to the remarks above $L_\alpha = 0$ if and only if $\alpha = 0$. Now $\alpha \to L_\alpha$ is a non-singular linear transformation from V into V^{**}, and since

$$\dim V^{**} = \dim V^* = \dim V \qquad ...(3)$$

Therefore this transformation is invertible, and is therefore an isomorphism of V onto V^{**}.

Corollary: Let V be a finite-dimensional vector space over the field F. If L is a linear functional on the dual space V^* of V, then there is a unique vector α in V such that

$$L(f) = f(\alpha) \qquad ...(4)$$

for every f in V^*.

Notes

Corollary: Let V be a finite-dimensional vector space over the field F. Each basis for V^* is the dual of some basis for V.

Proof: Let $\mathcal{B}^*=\{f_1,...,f_n\}$ be a basis for V^*. By Theorem 2 of unit 10 there is a basis $\{L_1,...,L_n\}$ for V^{**} such that

$$L_i(f_i)=\delta_{ij}. \qquad ...(5)$$

Using the corollary above, for each i there is a vector α, in V such that

$$L_i(f) = f(\alpha_i)$$

for every f in V^*, i.e., such that $L_i = L_{\alpha i}$. It follows immediately that $\{\alpha_1,...,\alpha_n\}$ is a basis for V and that $\mathcal{B}^*$ is the dual of this basis.

In view of Theorem 1, we usually identify α with L_α and say that V 'is' the dual space of V^* or that the spaces V, V^* are naturally in duality with one another. Each is the dual space of the other. In the last corollary we have an illustration of how that can be useful. Here is a further illustration.

If E is a subset of V^*, then the annihilator E^0 is (technically) a subset of V^{**}. If we choose to identify V and V^{**} as in Theorem (1), then E^0 is a subspace of V, namely, the set of all α in V such that $f(\alpha) = 0$ for all f in E. In a corollary of Theorem 3 of unit 10 we noted that each subspace W is determined by its annihilator W°. How is it determined? The answer is that W is the subspace annihilated by all f in W°, that is, the intersection of the null spaces of all f's in W°. In our present notation for annihilators, the answer may be phrased very simply: $W = (W^\circ)^\circ$.

Theorem 2: If S is any subset of a finite-dimensional vector space V, then $(S^\circ)^\circ$ is the subspace spanned by S.

Proof: Let W be the subspace spanned by S. Clearly $W^\circ = S^\circ$. Therefore, what we are to prove is that $W = W^{\circ\circ}$. We have given one proof. Here is another. By Theorem 3 of unit 10.

$$\left.\begin{aligned}\dim W + \dim W^\circ &= \dim V\\ \dim W^\circ + \dim W^{\circ\circ} &= \dim V^*\end{aligned}\right\} \qquad ...(6)$$

and since $\dim V = \dim V^*$ we have

$$\dim W = \dim W^{\circ\circ}.$$

Since W is a subspace of $W^{\circ\circ}$, we see that $W = W^{\circ\circ}$.

The results of this section hold for arbitrary vector spaces; however the proofs require the use of the so-called Axiom of Choice. Here we shall not tackle annihilators for general vector spaces. But, there are two results about linear functionals on arbitrary vector spaces which are so fundamental that we should include them.

Let V be a vector space. We want to define hyperspaces in V. Unless V is finite-dimensional, we cannot do that with the dimension of the hyperspace. But, we can express the idea that a space N falls just one dimension short of filling out V, in the following way:

1. N is a proper subspace of V;
2. If W is a subspace of V which contains N, then either $W = N$ or $W = V$.

Conditions (1) and (2) together say that N is a proper subspace and there is no larger proper subspace, in short, N is a maximal proper subspace.

Notes

Definition: If V is a vector space, a *hyperspace* in V is a maximal proper subspace of V.

Theorem 3. If f is a non-zero linear functional on the vector space V, then the null space of f is a hyperspace in V. Conversely, every hyperspace in V is the null space of a (not unique) non-zero linear functional on V.

Proof: Let f be a non-zero linear functional on V and N_f its null space. Let α be a vector in V which is not in N_f i.e., a vector such that $f(\alpha) \neq 0$. We shall show that every vector in V is in the subspace spanned by N_f and α. That subspace consists of all vectors

$$\gamma + c\alpha, \qquad \gamma \text{ in } N_f, \; c \text{ in } F.$$

Let β be in V. Define

$$c = \frac{f(\beta)}{f(\alpha)}$$

which makes sense because $f(\alpha) \neq 0$. Then the vector $\gamma = \beta - c\alpha$ is in N_f since

$$\begin{aligned} f(\gamma) &= f(\beta - c\alpha) \\ &= f(\beta) - cf(\alpha) \\ &= 0. \end{aligned} \qquad \ldots(7)$$

So β is in the subspace spanned by N_f and α.

Now let N be a hyperspace in V. Fix some vector α which is not in N. Since N is a maximal proper subspace, the subspace spanned by N and α is the entire space V. Therefore each vector β in V has the form

$$\beta = \gamma + c\alpha, \qquad \gamma \text{ in } N, \; c \text{ in } F.$$

The vector γ and the scalar c are uniquely determined by β. If we have also

$$\beta = \gamma' + c'\alpha, \qquad \gamma' \text{ in } N, \; c' \text{ in } F. \qquad \ldots(8)$$

then $\qquad (c' - c)\alpha = \gamma - \gamma'$

If $c' - c \neq 0$, then α would be in N; hence, $c' = c$ and $\gamma' = \gamma$. Another way to phrase our conclusion is this: If β is in V, there is a unique scalar c such that $\beta - c\alpha$ is in N. Call that scalar $g(\beta)$. It is easy to see that g is a linear functional on V and that N is the null space of g.

Lemma: If f and g are linear functionals on a vector space V, then g is a scalar multiple of f if and only if the null space of g contains the null space of f, that is, if and only if $f(\alpha) = 0$ implies $g(\alpha) = 0$.

Proof: If $f = 0$ then $g = 0$ as well and g is trivially a scalar multiple of f. Suppose $f \neq 0$ so that the null space N_f is a hyperspace in V. Choose some vector α in V with $f(\alpha) \neq 0$ and let

$$c = \frac{g(\alpha)}{f(\alpha)}. \qquad \ldots(9)$$

The linear functional $h = g - cf$ is 0 on N_f since both f and g are 0 there, and $h(\alpha) = g(\alpha) - cf(\alpha) = 0$.

Notes

Thus h is 0 on the subspace spanned by N_f and α – and that subspace is V. We conclude that $h = 0$, i.e. that $g = cf$.

Theorem 4: Let $g, f_1, ..., f_r$ be linear functionals on a vector space V with respective null space $N, N_1, ..., N_r$. Then g is a linear combination of $f_1, ..., f_r$ if and only if N contains the intersection $N_1 \cap ... \cap N_r$.

Proof: If $g = c_1 f_1 + ... + c_r f_r$ and $f_i(\alpha) = 0$ for each i, then clearly $g(\alpha) = 0$. Therefore, N contains $N_1 \cap ... \cap N_r$.

We shall prove the converse (the 'if' half of the theorem) by induction on the number r. The preceding lemma handles the case $r = 1$. Suppose we know the result for $r = k - 1$, and let $f_1, ..., f_r$ be linear functionals with null spaces $N_1, ..., N_k$ such that $N_1 \cap ... \cap N_k$ is contained in N, the pull space of g. Let $g', f_1', ..., f_{k-1}'$ be the restrictions of $g, f_1, ..., f_{k-1}$ to the subspace N_k. Then $g', f_1', ..., f_{k-1}'$ are linear functionals on the vector space N_k. Furthermore, if α is a vector in N_k and $f_i'(\alpha) = 0$, $i = 1, ..., k-1$, then α is in $N_1 \cap ... \cap N_k$ and so $g'(\alpha) = 0$. By the induction hypothesis (the case $r = k - 1$), there are scalars c_i such that

$$g' = c_1 f_1' + ... + c_{k-1} f_{k-1}'$$

Now let

$$h = g - \sum_{i=1}^{k-1} c_i f_i. \qquad ...(10)$$

Then h is a linear functional on V and (10) tells us that $h(\alpha) = 0$ for every α in N_k. By the preceding leema, h is a scalar multiple of f_k. If $h = c_k f_k$, then

$$g = \sum_{i=1}^{k} c_i f_i.$$

Self Assessment

1. Let n be a positive integer and F a field. Let W be the set of all vectors $(x_1, ..., x_n)$ in F^n such that $x_1 + ... + x_n = 0$.

   (a) Prove that W^0 consists of all linear functionals f of the form

   $$f(x_1, ..., x_n) = c \sum_{j=1}^{n} x_j.$$

Notes

(b) Show that the dual space W^* of W can be 'naturally' identified with the linear functionals

$$f(x_1,...,x_n) = c_1x_1 + ... + c_nx_n$$

on F^n which satisfy $c_1 + ... + c_n = 0$.

2. Use Theorem 4 to prove the following. If W is a subspace of a finite-dimensional vector space V and if $\{g_1,...,g_r\}$ is any basis for W^0, then

$$W = \bigcap_{i=1}^{r} N_g.$$

11.2 The Transpose of a Linear Transformation

Suppose that we have two vector spaces over the field F, V and W, and a linear transformation T from V into W. Then T induces a linear transformation from W^* into V^*, as follows. Suppose g is a linear functional on W, and let

$$f(\alpha) = g(T\alpha) \qquad ...(11)$$

for each α in V. Then (11) defines a function f from V into F, namely the composition of T, a function from V into W, with g, a function from W into F. Since both T and g are linear, Theorem 5 of unit 7 tells us that f is also linear, i.e., f is a linear functional on V. Thus T provides us with a rule T^t which associates with each linear functional g on W a linear functional $f = T^tg$ on V, defined by (11). Note also that T^t is actually a linear transformation from W^* into V^*; for, if g_1 and g_2 are in W^* and c is a scalar

$$\begin{aligned}\left[T^t(cg_1 + g_2)\right](\alpha) &= (cg_1 + g_2)(T\alpha)\\ &= cg_1(T\alpha) + g_2(T\alpha)\\ &= c(T^tg_1)(\alpha) + (T^tg_2)(\alpha) \qquad ...(12)\end{aligned}$$

so that $T^t(cg_1 + g_2) = cT^tg_1 + T^tg_2$. Let us summarize.

Theorem 5: Let V and W be vector spaces over the field F. For each linear transformation T from V into W, there is a unique linear transformation T^t from W^* into V^* such that

$$(T^tg)(\alpha) = g(T\alpha) \qquad ...(13)$$

for every g in W^* and α in V.

We shall call T^t the transpose of T. This transformation T^t is often called the adjoint of T; however, we shall not use this terminology.

Theorem 6: Let V and W be vector spaces over the field F, and let T be a linear transformation from V into W. The null space of T^t is the annihilator of the range of T. If V and W are finite-dimensional, then

(i) rank T^t = rank (T)

(ii) the range of T^t is the annihilator of the null space T. ...(14)

Notes

Proof: If g is in W^*, then by definition

$$(T^t g)(\alpha) = g(T\alpha)$$

for each α in V. The statement that g is in the null space of T^t means that $g(T\alpha) = 0$ for every α in V. Thus the null space of T^t is precisely the annihilator of the range of T.

Suppose that V and W are finite-dimensional, say dim $V = n$ and dim $W = m$. For (i): Let r be the rank of T, i.e., the dimension of the range of T. By Theorem 3 of unit 10, the annihilator of the range of T then has dimension $(m-r)$. By the first statement of this theorem, the nullity of T^t must be $(m-r)$. But then since T^t is a linear transformation on an m-dimensional space, the rank of T^t is $m-(m-r)=r$, and so T and T^t have the same rank. For (ii): Let N be the null space of T. Every functional in the range of T^t is in the annihilator of N; for suppose $f = T^t g$ for some g in W^*; then, if α is in N

$$f(\alpha) = (T^t g)(\alpha) = g(T\alpha) = g(0) = 0.$$

Now the range of T^t is a subspace of the space N^0, and

$$\dim N^0 = n - \dim N = \text{rank}(T) = \text{rank}(T^t) \qquad ...(15)$$

so that the range of T^t must be exactly N^0.

Theorem 7: Let V and W be finite-dimensional vector spaces over the field F. Let $\mathcal{B}$ be an ordered basis for V with dual basis $\mathcal{B}^*$, and let $\mathcal{B}'$ be an ordered basis for W with dual basis $\mathcal{B}'^*$. Let T be a linear transformation from V into W; let A be the matrix of T relative to $\mathcal{B},\mathcal{B}'$ and let B be the matrix of T^t relative to $\mathcal{B}'^*,\mathcal{B}^*$. Then $B_{ij} = A_{ji}$.

Proof: Let

$$\mathcal{B}=\{\alpha_1,...,\alpha_n\},\mathcal{B}'=\{\beta_1,...,\beta_m\},$$
$$\mathcal{B}^*=\{f_1,...,f_n\},\mathcal{B}'^*=\{g_1,...,g_m\}.$$

By definition,

$$\left.\begin{aligned} T\alpha_j &= \sum_{i=1}^{m} A_{ij}\beta_i i \quad j=1,...,n \\ T^t g_j &= \sum_{i=1}^{n} B_{ij} f_i j \quad j=1,...,m \end{aligned}\right] \qquad ...(16)$$

On the other hand,

$$(T^t g_j)(\alpha_i) = g_j(T\alpha_i)$$

$$= g_j\left(\sum_{k=1}^{m} A_{ki}\beta_k\right)$$

Notes

$$= \sum_{k=1}^{m} A_{ki} g_j(\beta_k)$$

$$= \sum_{k=1}^{m} A_{ki} \delta_{jk}$$

$$= A_{ji}.$$

For any linear functional f on V

$$f = \sum_{i=1}^{m} f(\alpha_i) f_i. \qquad ...(17)$$

If we apply this formula to the functional $f = T^t g_j$ and use the fact that $(T^t g_j)(\alpha_i) = A_{ji}$, we have

$$T^t g_j = \sum_{i=1}^{n} A_{ji} f_i. \qquad ...(18)$$

from which it immediately follow that $B_{ij} = A_{ji}$.

Definition: If A is an $m \times n$ matrix over the field F, the transpose of A is $n \times m$ matrix A^t defined by $A^t_{ij} = A_{ji}$.

Theorem 8: Thus states that if T is a linear transformation from V into W, the matrix of which in some pair of bases is A, then the transpose transformation T^t is represented in the dual pair of bases by the transpose matrix A^t.

Theorem 9: Let A be any $m \times n$ matrix over the field F. Then the row rank of A is equal to the column rank of A.

Proof: Let $\mathcal{B}$ be the standard ordered basis for F^n and $\mathcal{B}'$ the standard ordered basis for F^m. Let T be the linear transformation from F^n into F^m such that the matrix of T relative to the pair $\mathcal{B}, \mathcal{B}'$ is A, i.e.,

$$\left.\begin{array}{ll} . & T(x_1,...,x_n) = (y_1,...,y_m) \\ \text{where} & y_i = \sum_{j=1}^{n} A_{ij} x_j. \end{array}\right] \qquad ...(19)$$

The column rank of A is the rank of transformation T, because the range of T consists of all m-tuples which are linear combinations of the column vectors of A.

Relative to the dual bases $\mathcal{B}'^*$ and $\mathcal{B}^*$, the transpose mapping T^t is represented by the matrix A^t. Since the columns of A^t are the rows of A, we see by the same reasoning that the row rank of A (the column rank of A^t) is equal to the rank of T^t. By Theorem 7, T and T^t have the same rank, and hence the row rank of A is equal to the column rank of A.

Notes

Now we see that if A is an $m \times n$ matrix over F and T is the linear transformation from F^n into F^m defined above, then

$$\text{rank } (T) = \text{row rank } (A) = \text{column rank } (A) \quad ...(20)$$

and we shall call this number simply the rank of A.

Example 1: This example will be of a general nature – more discussion than example. Let V be an n-dimensional vector space over the field F, and let T be a linear operator on V. Suppose $\mathcal{B}=\{\alpha_1,...,\alpha_n\}$ is an ordered basis for V. The matrix of T in the ordered basis $\mathcal{B}$ is defined to be the $n \times n$ matrix A such that

$$T\alpha_j = \sum_{j=1}^{n} A_{ij}\alpha_i \quad ...(21)$$

in other words, A_{ij} is the ith coordinate of the vector $T\alpha_j$ in the ordered basis $\mathcal{B}$. If $\{f_1,...,f_n\}$ is the dual basis of $\mathcal{B}$, this can be stated simply

$$A_{ij} = f_i\left(T\alpha_j\right) \quad ...(22)$$

Let us see what happens when we change basis. Suppose

$$\mathcal{B}'=\{\alpha_1',...,\alpha_n'\}$$

is another ordered basis for V, with dual basis $\{f_1',...,f_n'\}$. If B is the matrix of T in the ordered basis $\mathcal{B}'$, then

$$B_{ij} = f_i'\left(T\alpha_j'\right). \quad ...(23)$$

Let U be the invertible linear operator such that $U\alpha_j = \alpha_j'$. Then the transpose of U is given by $U^t f_t' = f_i$. It is easy to verify that since U is invertible, so is U^t and $(U^t)^{-1} = (U^{-1})^t$. Thus $f_t' = \left(U^{-1}\right)^t f_i, i = 1,...,n$. Therefore,

$$\begin{aligned} B_{ij} &= \left[\left(U^{-1}\right)^t f_i\right]\left(T\alpha_j'\right) \\ &= f_i\left(U^{-1}T\alpha_j'\right) \\ &= f_i\left(U^{-1}TU\alpha_j\right). \end{aligned} \quad ...(24)$$

Now what does this say? Well, $f_i\left(U^{-1}TU\alpha_j\right)$ is the i, j entry of the matrix of $U^{-1}TU$ in the ordered basis $\mathcal{B}$. Our computation above shows that this scalar is also the i, j entry of the matrix of T in the ordered basis $\mathcal{B}'$. In other words

Notes

$$\left.\begin{aligned}[T]_{\mathcal{B}'} &= \left[U^{-1}TU\right]_{\mathcal{B}} \\ &= \left[U^{-1}\right]_{\mathcal{B}}[T]_{\mathcal{B}}[U]_{\mathcal{B}} \\ &= [U]_{\mathcal{B}}^{-1}[T]_{\mathcal{B}}[U]_{\mathcal{B}}\end{aligned}\right] \quad ...(25)$$

and this is precisely the change-of-basis formula which we derived earlier.

Self Assessment

3. Let V be a finite dimensional vector space over the field F and let T be a linear operator on V. Let C be a scalar and suppose there is a non-zero vector α in V such that $T\alpha = c\alpha$. Prove that there is a non-zero linear functional F on V such that $T'f = cf$.

4. For all A, B matrices in F^m, prove that–

   (a) $(A')' = A$

   (b) $(A+B)' = A'+B'$

   (c) $(AB)' = B'A'$

11.3 Summary

- A vector α induces a linear functional α_α in V^* and the mapping $\alpha \to L_\alpha$ is an isomorphism of V and V^{**}.
- If T is the linear transformation from V into W then it also induces a transformation from W^* into V^* through its transpose.
- The alternate name of the transpose transformation is word adjoint transformation.

11.4 Keywords

Adjoint: T^t is the transpose of T. This transformation T^t is often called the adjoint of T.

Transpose: If A is an $m \times n$ matrix over the field F, the transpose of A is $n \times m$ matrix A^t defined by $A_{ij}^t = A_{ji}$.

11.5 Review Questions

1. Let S be a set, F a field and $V(S,F)$ the space of all functions from S into F:

   $(f+g)(x) = f(x)+g(x)$
   $(cf)(x) = cf(x)$.

   Let W be any n-dimensional space of $V(S,F)$. Show that there exists points $x_1,...,x_n$ in S and functions $f_1, f_2,..., f_n$ in W such that $f_i(x_j) = S_{ij}$.

Notes

2. Let F be a field and let f be the linear functional on F^2 defined by $f(x_1, x_2) = ax_1 + bx_2$. For each of the following operations T, let $g = T'f$ and find $g(x_1, x_2)$

   (a) $T(x_1, x_2) = (-x_2, x_1)$;

   (b) $T(x_1, x_2) = (x_1 - x_2, x_1 + x_2)$.

11.6 Further Readings

Books

Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I N Herstein, *Topics in Algebra.*

Notes

Unit 12: Introduction and Characteristic Values of Elementary Canonical Forms

CONTENTS

Objectives

After studying this unit, you will be able to:

- Know that when the matrix of the linear transformation is in the diagonal form for some ordered basis the properties of the transformation can be seen at a glance.
- See that a matrix A of a linear operator T can be cast into a diagonal form under similarity transformations.
- See that a matrix A and $P^{-1}AP$ where P is an invertible have the same characteristic values.

Introduction

In this unit it is shown how a matrix has a diagonal form.

For this purpose the characteristic values and characteristic vectors are worked out and an invertible matrix is worked out of the characteristic vectors that can diagonalize the given matrix.

12.1 Overview

One of our primary aim in these units is to study linear transformation on finite dimensional vector spaces. So far we have studied many specific properties of linear transformations. In terms of ordered basis vectors we have represented such types of matrices by matrices. In terms of matrices we see lots of insight of the linear transformation. We also explored the linear algebra $L(V, V)$ consisting of the linear transformations of a space into itself.

In the next few units we shall concentrate ourselves with linear operators on a finite dimensional vector space. If we consider the ordered basis $\beta = (\alpha_1, \alpha_2, \ldots \alpha_n)$ then the effect of T on α_i is

$$T\alpha_i = \sum_{j=1}^{n} A_{ji}\beta_j \qquad i = 1, 2, \ldots n$$

where the new ordered basis is $\beta' = (\beta_1, \beta_2, \ldots \beta_n)$. If we now choose the basis $\beta = (\alpha_1, \alpha_2, \ldots \alpha_n)$ in such a way that

Notes

$$T\alpha_i = c_i\alpha_i \quad \dots (1)$$

for $i = 1$ to n then the matrix of the linear transformation is given by

$$D = \begin{bmatrix} C_1 & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & C_2 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & C_3 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \dots & \dots & C_n \end{bmatrix} \quad \dots(2)$$

with the help of equation (2) we would gain considerable information about T. Simple numbers associated with T, such as the rank of T or the determinant of T, would be determined with little more than a glance. The range of T would be the subspace spanned by those α_i's for which $c_i \neq 0$, and the null space would be spanned by the remaining α_i's. Indeed, it seems fair to say that, if we knew a basis β and a diagonal matrix D such that $[T] = D$, we could answer readily any question about T which might arise.

In the following we are interested in finding out if a linear operator can be represented by a diagonal matrix. How can we find the basis for such type of linear operator and what are the values of c_i's.

12.2 Characteristic Values

Guided by the equation (1) we should study vectors which on application of linear operator T transformed into the scalar multiples of themselves.

Let V be a vector space over the field F and T be a linear operator on V. A characteristic value of T is a scalar C in F such that there is a non-zero vector α in V with $T\alpha = c\alpha$. If c is a characteristic value of T, then

(a) Any α such that $T\alpha = c\alpha$, is called characteristic vector of T.

(b) The collection of all α such that $T\alpha = c\alpha$, is called the characteristic space associated with c.

If T is any linear operator and c is any scalar, the set of vectors α, such that $T\alpha = c\alpha$ is a sub-space of V. It is null space of linear transformation $(T - cI)$. We call c a characteristic value of T if this subspace is different from the zero subspace, i.e., if $(T - cI)$ fails to be 1:1. If the underlying space V is finite-dimensional, $(T - cI)$ fails to be 1:1 precisely when its determinant is different from 0.

Theorem 1: Let T be a linear operator on a finite-dimensional space V and let c be a scalar. The following are equivalent:

(i) c is a characteristic value of T.

(ii) The operator $(T - cI)$ is singular (not invertible)

(iii) det $(T - cI) = 0$.

The determinant criterion (iii) is very important because it tells us where to look for the characteristic values of T. Since det $(T - cI)$ is a polynomial of degree n in the variable c, we will find the characteristic values as the roots of that polynomial.

If $\mathcal{B}$ is any ordered basis of V and $A = [T]_\beta$, then $(T - cI)$ is invertible if and only if the matrix $(A - cI)$ is invertible. Accordingly, we make the following definition.

Definition: If A is an $n \times n$ matrix over the field F, a characteristic value of A in F is a scalar c in F such that the matrix $(A - cI)$ is singular (not invertible).

Notes

Since c is a characteristic value of A if and only if det $(A - cI) = 0$, we form the matrix $(xI - A)$ with polynomial entries, and consider the polynomial f = det $(xI - A)$. Clearly the characteristic values of A in F are just the scalars c in F such that $f(c) = 0$. For this reason f is called the characteristic polynomial of A. It is important to note that f is a monic polynomial which has degree exactly n. This is easily seen from the formula for the determinant of a matrix in terms of its entries.

Lemma: Similar matrices have the same characteristic polynomial.

Proof: If $B = P^{-1}AP$, then

$$\begin{aligned}\det(xI - B) &= \det(xI - P^{-1}PA)\\ &= \det(P^{-1}(xI - A)P)\\ &= \det P^{-1}.\det(xI - A).\det P\\ &= \det(xI - A)\end{aligned}$$

This lemma enables us to define sensibly the characteristic polynomial of the operator T as the characteristic polynomial of any $n \times n$ matrix which represents T in some ordered basis for V. Just as for matrices, the characteristic values of T will be the roots of the characteristic polynomial for T. In particular, this shows us that T cannot have more than n distinct characteristic values. It is important to point out that T may not have any characteristic values.

Example 1: Let T be the linear operator on R^2 which is represented in the standard ordered basis by the matrix

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

The characteristic polynomial for T (or for A) is

$$\det(xI - A) = \begin{bmatrix} x & 1 \\ -1 & x \end{bmatrix} = x^2 + 1.$$

Since this polynomial has no real roots, T has no characteristic values. If U is the linear operator on C^2 which is represented by A in the standard ordered basis, then U has two characteristic value, i and $-i$. Here we see a subtle point. In discussing the characteristic values of a matrix A, we must be careful to stipulate the field involved. The matrix A above has no characteristic values in R, but has the two characteristic values, i and $-i$ in C.

Example 2: Let A be the (real) 3×3 matrix

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

Then the characteristic polynomial for A is

$$\begin{bmatrix} x-3 & -1 & 1 \\ -2 & x-2 & 1 \\ -2 & -2 & x \end{bmatrix} = x^3 - 5x^2 + 8x - 4 = (x-1)(x-2)^2.$$

Thus the characteristic values of A are 1 and 2.

Notes

Suppose that T is the linear operator on R^3 which is represented by A in the standard basis. Let us find the characteristic vectors of T associated with the characteristic values, 1 and 2. Now

$$A - I = \begin{bmatrix} 2 & 1 & -1 \\ 2 & 1 & -1 \\ 2 & 2 & -1 \end{bmatrix}$$

It is obvious at a glance that $A-I$ has rank equal to 2 (and hence $T - I$ has nullity equal to 1). So the space of characteristic vectors associated with the characteristic value 1 is one-dimensional. The vector $\alpha_1 = (1, 0, 2)$ spans the null space of $T - I$. Thus $T\alpha = \alpha$ if and only if α is a scalar multiple of α_1. Now consider

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

Evidently $A - 2I$ also has rank 2, so that the space of characteristic vectors associated with value 2 has dimension 1. $T\alpha = 2\alpha$ is possible if α is a scalar multiple of $\alpha_2 = (1, 1, 2)$.

Example 3: Find the characteristic values and associated characteristic vector for the matrix

$$A = \begin{bmatrix} 8 & -6 & 2 \\ -6 & 7 & -4 \\ 2 & -4 & 3 \end{bmatrix}$$

Solution: We know that the characteristic equation is $|A - \lambda I| = 0$, *i.e.,*

$$\begin{bmatrix} 8-\lambda & -6 & 2 \\ -6 & 7-\lambda & -4 \\ 2 & -4 & 3-\lambda \end{bmatrix} = 0$$

or $\{(8 - \lambda)\} (7 - \lambda) (3 - \lambda) - 16\} + 6\{3 - \lambda\} (-6) + 8\} + 2 \{24 - 2(7 - \lambda)\} = 0$

or $-\lambda^3 + 18\lambda^2 - 45\lambda = 0$

or $\lambda(\lambda^2 + 18\lambda + 45) = 0$

or $\lambda(\lambda - 3) (\lambda - 15) = 0$

$\therefore \lambda = 0, 3, 15.$

Hence the characteristic roots are $\lambda_1 = 0$, $\lambda_2 = 3$, $\lambda_3 = 15$. The characteristic vector associated with is $\lambda_1 = 0$ is given by

$$\begin{bmatrix} 8 & -6 & 2 \\ -6 & 7 & -4 \\ 2 & -4 & 3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

This gives $8x_1 - 6x_2 + 2x_3 = 0$

$-6x_1 + 7x_2 - 4x_3 = 0$

$2x_1 - 4x_2 + 3x_3 = 0$

Notes

On solving these equations, we get

$$\frac{x_1}{1} = \frac{x_2}{2} = \frac{x_3}{2} = k_1 \text{ (say)}$$

Hence the required characteristic vector corresponding to the characteristic root $\lambda_1 = 0$, is

$$X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} k_1 \\ 2k_1 \\ 2k_1 \end{bmatrix}$$

The characteristic vector corresponding to the root $\lambda_2 = 3$ is given by

$$\begin{bmatrix} 8-3 & -6 & 2 \\ -6 & 7-3 & -4 \\ 2 & -4 & 3-3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

or
$$\begin{bmatrix} 5 & -6 & 2 \\ -6 & 4 & -4 \\ 2 & -4 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

This gives $5x_1 - 6x_2 + 2x_3 = 0$

$$6x_1 + 4x_2 - 4x_3 = 0$$

$$2x_1 - 4x_2 = 0$$

On solving these equations, we get

$$\frac{x_1}{2} = \frac{x_2}{1} = \frac{x_3}{-2} = k_2 \text{ (say) } k_2 \neq 0$$

Thus $x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 2k_2 \\ k_2 \\ -2k_2 \end{bmatrix}$ is the required characteristic vector for $\lambda = 3$.

Similarly, for $\lambda = 15$, the characteristic vector will be

$$\begin{bmatrix} 8-15 & -6 & 2 \\ -6 & 7-15 & -4 \\ 2 & -43 & 3-15 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

or
$$\begin{bmatrix} -7 & -6 & 2 \\ -6 & -8 & -4 \\ 2 & -4 & -12 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

which give $7x_1 + 6x_2 - 2x_3 = 0$

$$3x_1 + 4x_2 + 2x_3 = 0$$

$$x_1 - 2x_2 - 6x_3 = 0$$

On solving these, we get

$$\frac{x_1}{2} = \frac{x_2}{-2} = \frac{x_3}{1} = k_3 \text{ (say) } k_3 \neq 0$$

Notes

Hence, latent vector corresponding to the latent root, $\lambda_3 = 15$ will be

$$x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 2k_3 \\ -2k_3 \\ k_3 \end{bmatrix}$$

Example 4: If $a + b + c = 0$, find the characteristic values of the matrix

$$\begin{bmatrix} a & c & b \\ c & b & a \\ b & a & c \end{bmatrix}$$

Solution: We have the characteristic equation of A

$$|A - \lambda I| = 0$$

or
$$\begin{bmatrix} a-\lambda & c & b \\ c & b-\lambda & a \\ b & a & c-\lambda \end{bmatrix} = \begin{bmatrix} a+b+c-\lambda & c & b \\ a+b+c-\lambda & b-\lambda & a \\ a+b+c-\lambda & a & c-\lambda \end{bmatrix}$$

On replacing C_1 by $C_1 + C_2 + C_3$.

$$= \begin{bmatrix} -\lambda & c & b \\ -\lambda & b-\lambda & a \\ -\lambda & a & c-\lambda \end{bmatrix} \qquad [\because\ a + b + c = 0]$$

$$= \begin{bmatrix} -\lambda & c & b \\ 0 & b-\lambda-c & c-b \\ 0 & a-c & c-\lambda-b \end{bmatrix}$$

On operating $R_2 - R_1$ and $R_3 - R_1$

$$= \lambda\,[(a^2 + b^2 + c^2 - ab - bc - ca) - \lambda^2]$$

But $a + b + c = 0$, *i.e.*, $(a + b + c)^2 = 0$

or $a^2 + b^2 + c^2 + 2ab + 2bc + 2ca = 0$

or $$-(ab + bc + ca) = \frac{1}{2}(a^2 + b^2 + c^2)$$

$\because$ Characteristic equation becomes

$$\lambda\left[(a^2 + b^2 + c^2 + \frac{1}{2}(a^2 + b^2 + c^2) - \lambda^2\right] = 0$$

or $$\lambda\left[\frac{3}{2}(a^2 + b^2 + c^2) - \lambda^2\right] = 0$$

which gives $\lambda = 0$ or $\lambda = \pm\left[\frac{3}{2}(a^2 + b^2 + c^2)\right]^{1/2}$

Example 5: If A be a square matrix, show that the characteristic values of the matrix A are the same as those of its transpose A'.

Notes

Solution: The characteristic equation of the square matrix A is given by

$$|A - \lambda I| = 0$$

Similarly the characteristic equation of the matrix

$$A' \text{ is } (A' - \lambda I| = 0$$

Now, we have to prove that the characteristic roots of $|A - \lambda I| = 0$ and $|A' - \lambda I| = 0$ identical.

Since interchange of row and column does not change the value of the determinant, hence we have

$$|A - \lambda I| = |A' - \lambda I|$$

Hence the roots of the equations $|A - \lambda I| = 0$ and $|A' - \lambda I| = 0$ are same.

Lemma: If $\lambda \in F$ is a characteristic value of T, then for any polynomial $q(x) \in F(x)$, $q(\lambda)$ is a characteristic value of $q(T)$.

Proof: Suppose $\lambda \in F$ and $T\alpha = \lambda\alpha$ for non-zero vector α in V. Now $T^2\lambda = T(T\alpha) = T(\lambda\alpha) = \lambda T\alpha = \lambda^2\alpha$, continuing in this way we obtain $T^3\alpha = \lambda^3\alpha$, $T^4\alpha$, $T^4\alpha = \lambda^4\alpha$, ... $T^k\alpha = \lambda^k\alpha$, for all positive integers k. If

$$q(x) = a_0 x^m = a_1 x^{m-1} + ... + a_m \in F, \text{ then}$$

$$q(T) = a_0 T^m = a_1 T^{m-1} + ... + a_m,$$

hence $q(T)\alpha = a_0\lambda^m\alpha + a_1\lambda^{m-1}\alpha + ... + a_m\alpha$

$$= q(\lambda)d.$$

Thus $[q(T) - q(\lambda)I]\alpha = 0$, since $\alpha \neq 0$ so $q(\lambda)$ is characteristic value of $q(T)$.

Definition: Let T be a linear operator on the finite dimensional space V. We say that T is diagonalizable if there is a basis for V each vector of which is a characteristic vector of T.

The reason for the name should be apparent; for, if there is an ordered basis $\mathcal{B} = \{\alpha_1, ..., \alpha_n\}$ for V in which each α_i is a characteristic vector of T, then the matrix of T in the ordered basis $\mathcal{B}$ is diagonal. If $T\alpha_i = c_i\alpha_i$, then

$$[T]_{\mathcal{B}} = \begin{bmatrix} c_1 & 0 & ... & 0 \\ 0 & c_2 & ... & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & ... & c_n \end{bmatrix}$$

We certainly do not require that the scalars c_1, ... c_n be distinct; indeed, they may all be the same scalar (when T is a scalar multiple of the identity operator).

One could also define T to be diagonalizable when the characteristic vectors of T span V. This is only superficially different from our definition, since we can select a basis out of any spanning set of vectors.

For Examples 1 and 2 we purposely chose linear operators T on R^n which are not diagonalizable. In Example 1, we have a linear operator on R^2 which is not diagonalizable, because it has no characteristic values. In Example 2, the operator T has characteristic values; in fact, the characteristic polynomial for T factors completely over the real number field: $f = (x - 1)(x - 2)^2$. Nevertheless T fails to be diagonalizable. There is only a one-dimensional space of characteristic vectors associated with each of the two characteristic values of T. Hence, we cannot possibly form a basis for R^3 which consists of characteristic vectors of T.

Suppose that T is a diagonalizable linear operator. Let c_1, ... c_k be the distinct characteristic values of T. Then there is an ordered basis $\mathcal{B}$ in which T is represented by a diagonal matrix which has

Notes

for its diagonal entries the scalars c_i, each repeated a certain number of times. If c_i is repeated d_i times, then (we may arrange that) the matrix has the block form

$$[T]_{\mathcal{B}} = \begin{bmatrix} c_1 I_1 & 0 & \dots & 0 \\ 0 & c_2 I_2 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & c_k I_k \end{bmatrix}$$

where I_j is the $d_j \times d_j$ identity matrix. From that matrix we see two things. First, the characteristic polynomial for T is the product of (possibly repeated) linear factors:

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

If the scalar field F is algebraically closed, e.g., the field of complex numbers, every polynomial over F can be so factored; however, if F is not algebraically closed, we are citing a special property of T when we say that its characteristic polynomial has such a factorization. The second thing we see that d_i, the number of times which c_i is repeated as root of f, is equal to the dimension of the space of characteristic vectors associated with the characteristic value c_i. That is because the nullity of a diagonal matrix is equal to the number of zeros which it has on its main diagonal, and the matrix $[T - c_i I]_{\mathcal{B}}$ has d_i zeros on its main diagonal. This relation between the dimension of the characteristic space and the multiplicity of the characteristic value as a root of f does not seem exciting at first; however, it will provide us with a simpler way of determining whether a given operator is diagonalizable.

Lemma: Let T be a linear operator on the finite dimensional space V. Let $c_1, \dots, c_k$ be the distinct characteristic values of T and let W_i be the space of characteristic vectors associated with the characteristic value c_i. If $W = W_i + \dots + W_k$, then

$$\dim W = \dim W_1 + \dots + \dim W_k.$$

In fact if B_i is an ordered basis for W_i, then $\mathcal{B} = (\mathcal{B}_1, \dots, \mathcal{B}_k)$ is an ordered basis for W.

Proof: The space $W = W_i + \dots + W_k$ is the subspace spanned by all of the characteristic vectors of T. Usually when one forms the sum W of subspaces W_i, one expects that $\dim W < \dim W_i + \dots + \dim W_k$ because of linear relations which may exist between vectors in the various spaces. This lemma states that the characteristic spaces associated with different characteristic values are independent of one another.

Suppose that (for each i) we have a vector β_i in W_i, and assume that $\beta_i + \dots + \beta_k = 0$. We shall show that $\beta_i = 0$ for each i. Let f be any polynomial. Since $T\beta_i = c_i\beta_i$, the preceding lemma tells us that

$$\begin{aligned} 0 = f(T)0 &= f(T)\beta_1 + \dots + f(T)\beta_k \\ &= f(c_1)\beta_1 + \dots + f(c_k)\beta_k \end{aligned}$$

Choose polynomial $f_1, \dots, f_k$ such that

$$f_i(c_j) = \delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j. \end{cases}$$

Then

$$\begin{aligned} 0 = f_i(T) &= \sum_j \delta_{ij}\beta_j \\ &= \beta_i. \end{aligned}$$

Now, let β_i be an ordered basis for W_i, and let β be the sequence $\beta = (\beta_1, \dots, \beta_k)$. Then β spans the subspace $W = W_1 + \dots + W_k$. Also, β is a linearly independent sequence of vectors, for the following reason. Any linear relation between the vectors in β will have the form $\beta_1 + \dots + \beta_k = 0$, where β_i

Notes

is some linear combination of the vectors in β_i. From what we just did, we know that $\beta_i = 0$ for each i. Since each β_i is linearly independent, we see that we have only the trivial linear relation between the vectors in β.

Theorem 2: Let T be a linear operator on a finite-dimensional space V. Let $c_1, ..., c_k$ be the distinct characteristic values of T and let W_i be the null space of $(T - c_iI)$. The following are equivalent:

(i) T is diagonalizable

(ii) The characteristic polynomial for T is

$$f = (x - c_i)^{di} ... (x - c_k)^{dk}$$

and dim $W_i = di$, $i = 1, ... k$.

(iii) dim W_i + ... + dim W_k = dim V.

Proof: We have observed that (i) implies (ii). If the characteristic polynomial f is the product of linear factors, as in (ii), then $d_i + .. + d_k = \dim V$. For, the sum of the $d_i's$ is the degree of the characteristic polynomial, and that degree is dim V. Therefore (ii) implies (iii). Suppose (iii) holds. By the lemma, we must have $V = W_1 + ... + W_k$, i.e., the characteristic vectors of T span V.

The matrix analogue of Theorem 2 may be formulated as follows. Let A be an $n \times n$ matrix with entries in a field F, and let $c_1, ... c_k$ be the distinct characteristic values of A in F. For each i, let W_i be the space of column matrices X (with entries in F) such that

$$(A - c_iI)X = 0,$$

and let β_i be an ordered basis for W_i. The bases $\beta_1, ..., \beta_k$ collectively string together to form the sequence of columns of a matrix P:

$$P = [P_1, P_2, ...] = (\beta_1, ..., \beta_k)$$

The matrix A is similar over F to a diagonal matrix if and only if P is a square matrix. When P is square, P is invertible and $P^{-1} AP$ is diagonal.

Example 6: Let T be the linear operator on R^3 which is represented in the standard ordered basis by the matrix.

$$A = \begin{bmatrix} 5 & -6 & -6 \\ -1 & 4 & 2 \\ 3 & -6 & -4 \end{bmatrix}$$

Let us indicate how one might compute the characteristic polynomial, using various row and column operations:

$$\begin{bmatrix} x-5 & 6 & 6 \\ 1 & x-4 & -2 \\ -3 & 6 & x+4 \end{bmatrix} = \begin{bmatrix} x-5 & 0 & 6 \\ 1 & x-2 & -2 \\ -3 & 2-x & x+4 \end{bmatrix}$$

$$= (x-2)\begin{bmatrix} x-5 & 0 & 6 \\ 1 & 1 & -2 \\ -3 & -1 & x+4 \end{bmatrix}$$

$$= (x-2)\begin{bmatrix} x-5 & 0 & 6 \\ 1 & 1 & -2 \\ -2 & 0 & x+2 \end{bmatrix}$$

Notes

$$= (x-2)\begin{bmatrix} x-5 & 6 \\ -2 & x+2 \end{bmatrix}$$

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

$$= (x-2)^2(x-1).$$

What are the dimensions of the spaces of characteristic vectors associated with the two characteristic values? We have

$$A - I = \begin{bmatrix} 4 & -6 & -6 \\ -1 & 3 & 2 \\ 3 & -6 & -5 \end{bmatrix}$$

$$A - 2I = \begin{bmatrix} 3 & -6 & -6 \\ -1 & 2 & 2 \\ 3 & -6 & -6 \end{bmatrix}$$

We know that $A - I$ is singular and obviously rank $(A - I) \geq 2$. Therefore, rank $(A - I) = 2$. It is evident that rank $(A - 2I) = 1$.

Let W_1, W_2 be the spaces of characteristic vectors associated with the characteristic values 1, 2. We know that dim $W_1 = 1$ and dim $W_2 = 2$. By Theorem 2, T is diagonalizable. It is easy to exhibit a basis for R^3 in which T is represented by a diagonal matrix. The null space of $(T - I)$ is spanned by the vector $\alpha_1 = (3, -1, 3)$ and so $\{\alpha_1\}$ is a basis for W_1. The null space of $T - 2I$ (i.e., the space W_2) consists of the vectors (x_1, x_2, x_3) with $x_1 = 2x_2 + 2x_3$. Thus, one example of a basis for W_2 is

$$\alpha_2 = (2, 1, 0)$$

$$\alpha_3 = (2, 0, 1).$$

If $\beta = (\alpha_1, \alpha_2, \alpha_3)$, then $[T]_\beta$ is the diagonal matrix

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

The fact that T is diagonalizable means that the original matrix A is similar (over R) to the diagonal matrix D. The matrix P which enables us to change coordinates from the basis β to the standard basis is (of course) the matrix which has the transposes of $\alpha_1, \alpha_2, \alpha_3$ as its column vectors:

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

Furthermore, $AP = PD$, so that

$$P^{-1}AP = D.$$

Self Assessment

1. In each of the following cases, let T be the linear operator on R^2 which is represented by the matrix A in the standard ordered basis for R^2, and let U be the linear operator on C^2 represented by A in the standard ordered basis. Find the characteristic polynomial for T

Notes

and that for U, find the characteristic values of each operator, and for each such characteristic value c find a basis for the corresponding space of characteristic vectors.

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

2. Let T be the linear operator on R^3 which is represented in the standard ordered basis by the matrix

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

Prove that T is diagonalizable by exhibiting a basis for R^3, each vector of which is a characteristic vector of T.

3. Let $A = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 2 & -5 \\ 0 & 1 & -2 \end{bmatrix}$

Is A similar over the field R to a diagonal matrix? Is A similar over the field C to a diagonal matrix?

12.3 Summary

- When a matrix of a linear operator under a certain ordered basis is in the diagonal form then some properties of the linear operator can be real at a glance on this matrix.
- In this unit the characteristic values and the corresponding characteristic vectors of a matrix are found which help us in answering the question whether the given matrix is diagonalizable over the F or not.

12.4 Keywords

Invertible Matrix: The invertible matrix P formed out of the characteristic vectors of a vector A shows that A and PAP^{-1} are similar and also PAP^{-1} is in the diagonal form.

Null Space: If T is any linear operator and c is any scalar, the set of vectors α, such that $T\alpha = c\alpha$ is a sub-space of V. It is null space of linear transformation $(T - cI)$.

12.5 Review Questions

1. If T be the linear operator on C^3 which is represented in the ordered basis by the matrix

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

Prove that T is diagonalizable by exhibiting a basis for C^3, each vector of which is a characteristic vector of T.

Notes

2. If T be the linear operator on R^3 which is represented in the standard basis by the matrix

$$A = \begin{bmatrix} 5 & -6 & -6 \\ -1 & 4 & 2 \\ 3 & -6 & -4 \end{bmatrix}$$

Prove that T is diagonalizable. Find the diagonalizable matrix P that PAP^{-1} is diagonal.

Answers: Self Assessment

1. For $A = \begin{bmatrix} 1 & 4 \\ 2 & 3 \end{bmatrix}$, characteristic polynomial for T is $T^2 - 4t - 5I = 0$

$\lambda_1 = 5, \alpha_1 = (1, 1)$ $\lambda_1 = -1, \alpha_2 = (2, -1)$

For $A = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$, the characteristic polynomial for T is $T^2 - 2T = 0$ the characteristic roots are

$\lambda_1 = 0, \quad \alpha_1 = (1, 1)$

$\lambda_2 = 2, \quad \alpha_2 = (1, -1)$

2. In the matrix is diagonalizable has the characteristic values 1, 2, 5 with the characteristic vectors (2, 1, 4), (1, 1, 0), (0, 1, 1) respectively. The diagonalizing matrix is

$$\begin{bmatrix} 2 & 1 & 0 \\ 1 & 1 & 1 \\ 4 & 2 & 1 \end{bmatrix}$$

3. A is not similar over the real field F to a diagonal matrix. But A is similar over the field C to a diagonal matrix

$$\begin{bmatrix} 3 & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & -i \end{bmatrix}$$

12.6 Further Readings

Books Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I.N. Herstein, *Topics in Algebra*

Notes

Unit 13: Annihilating Polynomials

CONTENTS

Objectives

After studying this unit, you will be able to:

- Know about the polynomials over the field F, the degree of polynomial, monic polynomial, annihilating polynomials as well as minimal polynomials.
- Understand that the linear operator is annihilated by its characteristic polynomial.
- Understand that we consider all monic polynomials with coefficients in F and the degree of the minimal polynomial is the least positive integer such that a linear relation is obtained annihilated.

Introduction

In this unit we investigate more properties of a linear transformation.

We define certain terms like monic polynomial, minimal polynomial as well as annihilating polynomial and characteristic polynomial.

It is seen that the theorem of Cayley-Hamilton in this unit helps us in narrowing down the reach for the minimal polynomials of various operators.

13.1 Overview

Polynomial Over F. Let $F(x)$ be the subspace of F^n spanned by vectors 1, x, x^2..... An element of $F(x)$ is called a polynomial over F.

Degree of a Polynomial: $F(x)$ consists of all (finite) linear combinations of x and its powers. If f is a non-zero polynomial of the form

$$f = f_0x^0 + f_1x + f_2x^2 + \cdots + f_nx^n$$

such that $f_n \neq 0$ and $n \geq 0$ and $f_n = 0$ for all integers $k > n$; this integer is obviously unique and is called the *degree* of f.

The scalars $f_0, f_1, f_2, \cdots, f_n$ are sometimes called the coefficients of f in the field F.

Notes

Monic Polynomial: A polynomial $f(x)$ over a field F is called monic polynomial if the coefficient of highest degree term in it is unity i.e $f_n = 0$

Annihilating Polynomials: Let A be $n \times n$ matrix over a field F and $f(x)$ be a polynomial over F. Then if $f(A) = 0$. Then we say that the polynomial $f(x)$ annihilates the matrix A.

13.2 Annihilating Polynomials

It is important to know the class of polynomials that Annihilate T.

Suppose T is a linear operator on V, a vector space over the field F. If p is a polynomial over F, then $p(T)$ is again a linear operator on V. If q is another polynomial over F, then

$$(p+q)(T) = p(T)+q(T)$$

$$(pq)(T) = p(T)\,q(T)$$

Therefore, the collection of polynomials p which annihilate T, in the sense that

$$p(T) = 0,$$

is an ideal in the polynomial algebra $F[x]$. It may be the zero ideal, i.e., it may be that T is not annihilated by any non-zero polynomial. But, that cannot happen if the space V is finite-dimensional.

Suppose T is a linear operator on the n-dimensional space V. Look at the first $(n^2 + 1)$ powers of T:

$$I, T, T^2 \cdots, T^{n2}.$$

This is a sequence of $n^2 + 1$ operators in $L(V, V)$, the space of linear operators on V. The space $L(V, V,)$ has dimension n^2. Therefore, that sequence of $n^2 + 1$ operators must be linearly dependent. i.e., we have

$$c_0 I + c_1 T + \cdots + c_{n2} T^{n2} = 0$$

for some scalars c_i not all zero. So, the ideal of polynomials which annihilate T contains a non-zero polynomial of degree n^2 or less.

Definition. Let T be a linear operator on a finite-dimensional vector space V over the field F. The minimal polynomial for T is the (unique) monic generator of the ideal of polynomials over F which annihilate T.

The name '*minimal polynomial*' stems from the fact that generator of a polynomial ideal is characterized by being the monic polynomial of minimum degree in the ideal. That means that the minimal polynomial p for the linear operator T is uniquely determined by these three properties:

1. p is a monic polynomial over the scalar field F.
2. $p(T) = 0$
3. No polynomial over F which annihilates T has smaller degree than p has.

If A an $n \times n$ matrix over F, we define the **minimal polynomial** for A in an analogous way, as the unique monic generator of the ideal of all polynomials over F which annihilate A. If the operator T is represented in some ordered basis by the matrix A, then T and A have the same minimal polynomial. That is because $f(T)$ is represented in the basis by the matrix $f(A)$ so that $f(T) = 0$ if and only if $f(A) = 0$.

Notes

From the last remark about operators and matrices it follows that similar matrices have the same minimal polynomial. That fact is also clear from the definitions because

$$f(P^{-1}AP) = P^{-1}f(A)P$$

for every polynomial f.

There is another basic remark which we should make about minimal polynomials of matrices. Suppose that A is an $n \times n$ matrix with entries in the field F. Suppose that F_1 is a field which contains F as a subfield. (For example, A might be a matrix with rational entries, while F_1 is the field of real numbers. Or, A might be a matrix with real entries, while F_1 is the field of complex numbers.) We may regard A either as an $n \times n$ matrix over F or as an $n \times n$ matrix over F_1. On the surface, it might appear that we obtain two different minimal polynomials for A. Fortunately that is not the case; and we must see why. What is the definition of the minimal polynomial for A, regarded as an $n \times n$ matrix over the field F? We consider all monic polynomials with coefficients in F which annihilate A, and we choose the one of least degree. If f is a monic polynomial over F:

$$f = x^k + \sum_{j=0}^{k-1} a_j x^i \quad \ldots (1)$$

then $f(A) = 0$ merely says that we have a linear relation between the powers of A:

$$A^k + a_{k-1}A^{k-1} + \cdots + a_1 A + a_0 I = 0 \quad \ldots (2)$$

The degree of the minimal polynomial is the least positive integer k such that there is a linear relation of the form (2) between the powers $I, A, \cdots, A^k$. Furthermore, by the uniqueness of the minimal polynomial, there is for that k one and only one relation of the form (2); i.e., once the minimal k is determined, there are unique scalars $a_0, \cdots, a_{k-1}$ in F such that (2) holds. They are the coefficients of minimal polynomial.

Now (for each k) we have in (2) a system of n^2 linear equations for the 'unknowns' $a_0, \cdots, a_{k-1}$. Since the entries of A lie in F, the coefficients of the system of equations (2) are in F. Therefore, if the system has a solution with $a_0, \cdots, a_{k-1}$ in F_1 it has a solution with $a_0, \cdots, a_{k-1}$ in F. It should now be clear that the two minimal polynomials are the same.

What do we know thus far about the minimal polynomial for a linear operator on an n-dimensional space? Only that its degree does not exceed n^2. That turns out to be a rather poor estimate, since the degree cannot exceed n. We shall prove shortly that the operator is annihilated by its characteristic polynomial. First, let us observe a more elementary fact.

Theorem 1: Let T be a linear operator on an n-dimensional vector space V [or, let A be an $n \times n$ matrix]. The characteristic and minimal polynomials for T [for A] have the same roots, except for multiplicities.

Proof. Let p be the minimal polynomial for T. Let c be a scalar. What we want to show is that $p(c) = 0$ if and only if c is a characteristic value of T.

First, suppose $p(c) = 0$. Then

$$p = (x - c)q$$

where q is a polynomial. Since deg $q <$ deg p, the definition of the minimal polynomial p tells us that $q(T) \neq 0$. Choose a vector β such that $q(T)\ \beta \neq 0$. Let $\alpha = q(T)\beta$. Then

$$0 = p(T)\beta$$
$$= (T - cI)q(T)\beta$$

Notes

$$= (T - cI)\alpha$$

and thus, c is a characteristic value of T.

Now, suppose that c is a characteristic value of T, say $T\alpha = c\alpha$ with $\alpha \neq 0$. So

$$p(T)\alpha = p(c)\alpha.$$

Since $p(T) = 0$ and $\alpha \neq 0$, we have $p(c)$ 0.

Let T be a diagonalizable linear operator and let $c_1, \cdots, c_k$ be the distinct characteristic values of T. Then it is easy to see that the minimal polynomial for T is the polynomial.

$$p = (x - c_1) \cdots (x - c_k).$$

If α is a characteristic vector, then one of the operators $T - c_1 I, \cdots, T - c_k I$ sends α into 0. Therefore

$$(T - c_1 I) \cdots (T - c_k I)\,\alpha = 0$$

for every characteristic vector α. There is a basis for the underlying space which consists of characteristic vectors of T; hence

$$p(T) = (T - c_1 I) \cdots (T - c_k I) = 0.$$

What we have concluded is this. If T is a diagonalizable linear operator, then the minimal polynomial for T is a product of distinct linear factors. As we shall soon see, that property characterizes diagonalizable operators.

Example 1: Let's try to find the minimal polynomials for the operators in Example 1, 2, and 6 in unit 12. We shall discuss them in reverse order. The operator in Example 6 was found to be diagonalizable with characteristic polynomial.

From the preceding paragraph we know that the minimal polynomial for T is.

$$p = (x - 1)(x - x).$$

The reader might find it reassuring to verify directly that

$$(A - I)(A - 2I) = 0.$$

In Example 2, the operator T also had the characteristic polynomial $f = (x - 1)(x - 2)^2$. But, this T is not diagonalizable, so we don't know that the minimal polynomial is $(x - 1)\ (x - 2)$. What do be know about the minimal polynomial in this case? We know that its roots are 1 and 2, with some multiplicities allowed. Thus we search for p among polynomials of the form $(x - 1)^k$ $(x - 2)^l, k \geq 1, l \geq 1$. Try $(x - 1)\ (x - 2)$:

$$(A - I)\ (A - 2I) = \begin{bmatrix} 2 & 1 & -1 \\ 2 & 1 & -1 \\ 2 & 2 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 & -1 \\ 2 & 0 & -1 \\ 2 & 2 & -2 \end{bmatrix}$$

$$= \begin{bmatrix} 2 & 0 & -1 \\ 2 & 0 & -1 \\ 4 & 0 & -2 \end{bmatrix}$$

Thus, the minimal polynomial has degree at least 3. So, next we should try either $(x - 1)^2\ (x - 2)$ or $(x - 1)\ (x - 2)^2$. The second being the characteristic polynomial, would seem a less random choice. One can readily compute that $(A - I)\ (A - 2I)^2 = 0$. Thus the minimal polynomial for T is its characteristic polynomial.

Notes

In Example 1 in unit 12 we discussed the linear operator T on R^2 which is represented in the standard basis by the matrix.

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

The characteristic polynomial is $x^2 + 1$, which has no real roots. To determine the minimal polynomial, forget about T and concentrate on A. As a complex 2×2 matrix, A has the characteristic values i and $-i$. Both roots must appear in the minimal polynomial. Thus the minimal polynomial is divisible by $x^2 + 1$. It is trivial to verify that $A^2 + I = 0$. So the minimal polynomial is $x^2 + 1$.

Theorem* 2 *(Cayley-Hamilton): Let T be a linear operator on a finite dimensional vector space V. If f is the characteristic polynomial for T, then $f(T) = 0$; in other words, the minimal polynomial divides the characteristic polynomial for T.

Proof: The proof, although short, may be difficult to understand. Aside from brevity, it has the virtue of providing an illuminating and far from trivial application of the general theory of determinants.

Let K be the commutative ring with identity consisting of all polynomials in T. Of course, K is actually a commutative algebra with identity over the scalar field. Choose an ordered basis $\{\alpha_1, \cdots, \alpha_n\}$ for V, and let A be the matrix which represents T in the given basis. Then

$$T\alpha_i = \sum_{i=j}^{n} A_{ji}\alpha_j, \qquad 1 \le j \le n$$

These equations may be written in the equivalent form

$$\sum_{j=1}^{n} (\delta_{ij}T - A_{ji}I)\alpha_j = 0, \qquad 1 \le i \le n.$$

Let B denote the element of $K^{n \times n}$ with entries

$$B_{ij} = \delta_{ij}T - A_{ji}I.$$

When $n = 2$

$$B = \begin{bmatrix} T - A_{11}I & -A_{21}I \\ -A_{12}I & T - A_{22}I \end{bmatrix}$$

and

$$\begin{aligned} \det B &= (T - A_{11}I)(T - A_{22}I) - A_{12}A_{21}I \\ &= T^2 - (A_{11} + A_{22})T + (A_{11}A_{12} - A_{12}A_{21})I \\ &= f(T) \end{aligned}$$

where f is the characteristic polynomial:

$$f = x^2 - (\text{trace } A)x + \det A.$$

For the case $n > 2$, it is also clear that

$$\det B = f(T)$$

Notes

since f is the determinant of the matrix $xI - A$ whose entries are the polynomials

$$(xI - A)_{ij} = \delta_{ij}x - A_{ji}.$$

We wish to show that $f(T) = 0$. In order that $f(T)$ be the zero operator, it is necessary and sufficient that $(\det B)_{\alpha k} = 0$ for $k = 1, \cdots, n$. By the definition of B, the vectors $\alpha_1, \cdots \alpha_n$ satisfy the equations

$$\sum_{j=1}^{n} B_{ij}\alpha_j = 0, \quad 1 \le i \le n. \qquad \ldots (3)$$

When $n = 2$, it is suggestive to write (3) in the form

$$\begin{bmatrix} T - A_{11}I & -A_{21}I \\ -A_{12}I & T - A_{22}I \end{bmatrix}\begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

In this case, the classical adjoint, *adj B* is the matrix

$$\tilde{B} = \begin{bmatrix} T - A_{22}I & A_{21}I \\ A_{12}I & T - A_{11}I \end{bmatrix}$$

and

$$\tilde{B}B = \begin{bmatrix} \det B & 0 \\ 0 & \det B \end{bmatrix}.$$

Hence, we have

$$\begin{aligned} (\det B)\begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} &= (\tilde{B}B)\begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} \\ &= \tilde{B}\left(B\begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix}\right) \\ &= \begin{bmatrix} 0 \\ 0 \end{bmatrix}. \end{aligned}$$

In the general case, let $\tilde{B} = adj\ B$. Then by (3)

$$\sum_{j=1}^{n} \tilde{B}_{ki}B_{ij}\alpha_j = 0$$

for each pair k, i, and summing on i, we have

$$\begin{aligned} 0 &= \sum_{i=1}^{n}\sum_{j=1}^{n} \tilde{B}_{ki}B_{ij}\alpha_i \\ &= \sum_{j=1}^{n}\left(\sum_{i=1}^{n} \tilde{B}_{ki}B_{ij}\right)\alpha_j. \end{aligned}$$

Notes

Now $\tilde{B}\,B = (\det B)I$, so that

$$\sum_{i=1}^{n} \tilde{B}_{ki} B_{ij} = \delta_{kj} \det B.$$

Therefore

$$0 = \sum_{j=1}^{n} \delta_{ki} (\det B)\, \alpha_j$$

$$= (\det B)_{\alpha k}, \qquad 1 \le k \le n.$$

The Cayley-Hamilton theorem is useful to us at this point primarily because it narrows down the search for the minimal polynomials of various operators. If we know the matrix A which represents T in some ordered basis, then we can compute the characteristic polynomial f. We know that the minimal polynomial p divides f and that the two polynomials have the same roots. There is no method for computing precisely the roots of a polynomial (unless its degree is small); however, if f factors

$$f = (x - c_1)^{d1} \cdots (x - c_k)^{dk}, C_{11} \cdots, C_k, \text{distinct}, d_i \ge 1 \qquad \text{.... (4)}$$

then

$$p = (x - c_1)^{r1} \cdots (x - c_k)^{rk}, \qquad 1 \le r_j \le d_j \qquad \text{.... (5)}$$

That is all we can say in general. If f is the polynomial (4) and has degree n, then for every polynomial p as in (5) we can find an $n \times n$ matrix which has f as its characteristic polynomial and p as its minimal polynomial. We shall not prove this now. But, we want to emphasize the fact that the knowledge that the characteristic polynomial has the form (4) tells us that the minimal polynomial has the form (5), and it tells us nothing else about p.

Example 2: Let A be the 4×4 (rational) matrix

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

The powers of A are easy to compute

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

$$A^3 = \begin{bmatrix} 0 & 4 & 0 & 4 \\ 4 & 0 & 4 & 0 \\ 0 & 4 & 0 & 4 \\ 4 & 0 & 4 & 0 \end{bmatrix}$$

Thus $A^3 = 4A$, i.e., if $p = x^3 - 4x = x(x + 2)(x - 2)$, then $p(A) = 0$. The minimal polynomial for A must divide p. That minimal polynomial is obviously not of degree 1, since that would mean that A was a scalar multiple of the identity. Hence, the candidates for the minimal polynomial are:

Notes

p, $x(x+2)$, $x(x-2)$, x^2-4. The three quadratic polynomials can be eliminated because it is obvious at a glance that $A^2 \neq -2A$, $A^2 \neq 2A$, $A^2 \neq 4I$. Therefore p is the minimal polynomial for A. In particular 0, 2, and – 2 are the characteristic values of A. One of the factors x, $x-2$, $x+2$ must be repeated twice in the characteristic polynomial. Evidently, rank $(A) = 2$. Consequently there is a two-dimensional space of characteristic vectors associated with the characteristic value 0. From Theorem 2, it should now be clear that the characteristic polynomial is $x^2(x^2-4)$ and that A is similar over the field of rational numbers to the matrix

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

Example 3: Verify Cayley-Hamilton's theorem for the linear transformation T represented by the matrix A.

$$A = \begin{bmatrix} 0 & 0 & 1 \\ 3 & 1 & 0 \\ -2 & 1 & 4 \end{bmatrix}$$

Solution: The characteristic polynomial is given by

$$|A - xI| = \begin{bmatrix} 0-x & 0 & 1 \\ 3 & 1-x & 0 \\ -2 & 1 & 4-x \end{bmatrix}$$

$$= -x\left[(1-x)(4-x)\right] + (3+2-2x)$$

$$= -x\left(4-5x+x^2\right) + 5 - 2x$$

$$= -x^3 + 5x^2 - 6x + 5 = 0$$

or $$f(x) = x^3 - 5x^2 + 6x - 5 = 0$$

Now

$$A^2 = \begin{bmatrix} 0 & 0 & 1 \\ 3 & 1 & 0 \\ -2 & 1 & 4 \end{bmatrix}\begin{bmatrix} 0 & 0 & 1 \\ 3 & 1 & 0 \\ -2 & 1 & 4 \end{bmatrix} = \begin{bmatrix} -2 & 1 & 4 \\ 3 & 1 & 3 \\ -5 & 5 & 14 \end{bmatrix}$$

$$A^3 = \begin{bmatrix} -2 & 1 & 4 \\ 3 & 1 & 3 \\ -5 & 5 & 14 \end{bmatrix}\begin{bmatrix} 0 & 0 & 1 \\ 3 & 1 & 0 \\ -2 & 1 & 4 \end{bmatrix} = \begin{bmatrix} -5 & 5 & 14 \\ -3 & 4 & 15 \\ -13 & 19 & 51 \end{bmatrix}$$

So

$$f(A) = A^3 - 5A^2 + 6A - 5I$$

$$= \begin{bmatrix} -5 & 5 & 14 \\ -3 & 4 & 15 \\ -13 & 19 & 51 \end{bmatrix} - \begin{bmatrix} -10 & 5 & 20 \\ 15 & 5 & 15 \\ -25 & 25 & 14 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 6 \\ 18 & 6 & 0 \\ -12 & 6 & 24 \end{bmatrix} - \begin{bmatrix} 5 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 5 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = 0$$

where 0 being null matrix. So $f(A) = 0$

Self Assessment

Notes

1. Let A be the following 3×3 matrix over F;

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

Find the characteristic polynomial for A and also the minimal polynomial for A.

2. Let A be the following 3×3 matrix over F;

$$A = \begin{bmatrix} 1 & 3 & 7 \\ 4 & 2 & 3 \\ 1 & 2 & 1 \end{bmatrix}$$

Find the characteristic polynomial for A and also find the minimal polynomial for A.

13.3 Summary

- In this unit certain terms related to linear operator T are defined, i.e., the monic polynomial, annihilating polynomials, minimal polynomials as well as characteristic polynomials.
- With the help of Cayley-Hamilton theorem it becomes easier to search for the minimal polynomials of various operators.

13.4 Keywords

Annihilating Polynomial: Annihilating polynomial $f(x)$ over the field F is such that for a matrix A of $n \times n$ matrix over the field $f(A) = 0$, then we say that the polynomial annihilates the matrix. If a linear operator T is represented by the matrix then $f(T) = 0$ gives us the annihilating polynomial for the linear operator T.

Monic Polynomial: The monic polynomial is a polynomial $f(x)$ whose coefficient of the highest degree in it is unity.

13.5 Review Questions

1. Let A be the following 3×3 matrix over F;

$$A = \begin{bmatrix} 2 & 4 & 3 \\ 0 & -1 & 1 \\ 2 & 2 & -1 \end{bmatrix}$$

Find the characteristic polynomial and minimal polynomial for A.

2. Let A be the following 3×3 matrix over F;

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

Find the characteristic polynomial and minimal polynomial for A.

Notes

Answers: Self Assessment

1. The characteristic polynomial is given by

   $f(x) = x^3 - 6x^2 + 9x - 4 = 0$

   and that this is also the minimal polynomial for A.

2. The characteristic polynomial for A is

   $f(x) = x^3 - 4x^2 - 20x - 35 = 0$,

   and that this is also the minimal polynomial for A.

13.6 Further Readings

Books

Kenneth Hoffman and Ray Kunze *Linear Algebra*

I.N Herstein *Topics in Algebra*

Unit 14: Invariant Subspaces

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Know about few concepts which are useful in analysing further properties of the linear operator T.
- Understand concepts like invariant subspace, the restriction operator Tw, the T-conductor of a vector α into subspace W.
- See that all these concepts help us in understanding the structure of minimal polynomial of linear operator.
- Understand the restriction operator Tw helps in writing the matrix A of the linear operator in a block form and so the characteristic polynomial for Tw divides the characteristic polynomial for T.

Introduction

In this unit we are still studying the properties of a linear operator on the vector space V. The concept of invariant subspace, the restriction operator Tw help us in finding the characteristic polynomial of T as well as its annihilator and so it helps in diagonalization of the matrix A of the linear operator T.

14.1 Invariant Subspaces: Definitions

In this unit, we shall introduce a few concepts which are useful in analysing further the properties of a linear operator. We shall use these concepts to obtain characterizations of diagonalizable (and triangulable) operators in terms of their minimal polynomials.

Invariant Subspace

A subspace W of the vector space V is invariant of more precisely T-invariant if for each vector α in W the vector $T\alpha$ is in W, i.e., $T(w)$ is contained in W. When this is so T induces a linear operator on W, called restriction to W. We often denote the restriction by Tw. The linear operator Tw is defined by $Tw(\alpha) = T(\alpha)$, for α in W, but Tw is quite a different object from T since its domain is W and not V.

Notes

The T-conductor of ● into W

Let W be an invariant subspace for T and let α be a vector in V. The T-conductor of α into W is the set $S_T(\alpha; W)$, which consists of all polynomials g (over the scalar field), such that $g(T)\alpha$ is in W. Some authors call that collection of polynomials the 'stuffer'. In the special case $W = \{0\}$, the conductor is called T-annihilator of α.

14.2 Theorems and Examples

Example 1: If T is any linear operator on V, then V is invariant under T, as is the zero subspace. The range of T and the null space of T are also invariant under T.

Example 2: Let F be a field and let D be the differentiation operator on the space $F[x]$ of polynomials over F. Let n be a positive integer and let W be the subspace of polynomials of degree not greater than n. Then W is invariant under D. This is just another way of saying that D is 'degree decreasing'.

Example 3: Here is a very useful generalization of Example 1. Let T be a linear operator on V. Let U be any linear operator on V which commutes with T, i.e., $TU = UT$. Let W be the range of U and let N be the null space of U. Both W and N are invariant under T. If α is in the range of U, say $\alpha = U\beta$, then $T\alpha = T(U\beta) = U(T\beta)$ so that $T\alpha$ is in the range of U. If α is in N, then $U(T\alpha) = T(U\alpha) = T(0) = 0$; hence $T\alpha$ is in N.

A particular type of operator which commutes with T is an operator $U = g(T)$, where g is a polynomial. For instance, we might have $U = T - cI$, where c is a characteristic value of T. The null space of U is familiar to us. We see that this example includes the (obvious) fact that the space of characteristic vectors of T associated with the characteristic value c is invariant under T.

Example 4: Let T be the linear operator on R^2 which is represented in the standard ordered basis by the matrix

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

Then the only subspaces of R^2 which are invariant under T are R^2 and the zero subspace. Any other invariant subspace would necessarily have dimension 1. But, if W is the subspace spanned by some non-zero vector α, the fact that W is invariant under T means that α is a characteristic vector, but A has no real characteristic values.

When V is finite-dimensional, the invariance of W under T has a simple matrix interpretation, and perhaps we should mention it at this point. Suppose we choose an ordered basis $\mathcal{B} = \{\alpha_1,...,\alpha_n\}$ for V such that $\mathcal{B}' = \{\alpha_1,...,\alpha_r\}$ is an ordered basis for W (r = dim W). Let $A = [T]_{\mathcal{B}}$ so that

$$T\alpha_j = \sum_{i=1}^{n} A_{ij}\alpha_i \qquad ...(1)$$

Since W is invariant under T, the vector $T\alpha_j$ belongs to W for $j \le r$. This means that

$$T\alpha_j = \sum_{i=1}^{r} A_{ij}\alpha_i , \qquad j \le r \qquad ...(2)$$

Notes

In other words, $A_{ij} = 0$ if $j \leq r$ and $i \geq r$.

Schematically, A has the block form

$$A = \begin{bmatrix} B & C \\ 0 & D \end{bmatrix} \qquad ...(3)$$

where B is an $r \times r$ matrix, C is an $r \times (n - r)$ matrix, and D is an $(n - r) \times (n - r)$ matrix. The reader should note that according to (2) the matrix B is precisely the matrix of the induced operator Tw in the ordered basis $\mathcal{B}'$.

Most often, we shall carry out arguments about T and Tw without making use of the block form of the matrix A in (3). But we should note how certain relations between Tw and T are apparent from that block form.

Lemma: Let W be an invariant subspace for T, the characteristic polynomial for the restriction operator Tw divides the characteristic polynomial for T. The minimal polynomial for Tw divides the minimal polynomial for T.

Proof: We have

$$A = \begin{bmatrix} B & C \\ 0 & D \end{bmatrix}$$

where $A = [T]_{\mathcal{B}}$ and $B = [T_w]_{\mathcal{B}'}$. Because of the block form of the matrix

$$\det (xI - A) = \det (xI - B) \det (xI - D)$$

That proves the statement about characteristic polynomials. Notice that we used I to represent identity matrices of three different sizes.

The k^{th} power of the matrix A has the block form

$$A^k = \begin{bmatrix} B^k & C_k \\ 0 & D^k \end{bmatrix}$$

where C_k is some $r \times (n - r)$ matrix. Therefore, any polynomial which annihilates A also annihilates B (and D too). So, the minimal polynomial for B divides the minimal polynomial for A.

Example 5: Let T be any linear operator on a finite-dimensional space V. Let W be the subspace spanned by all of the characteristic vectors of T. Let $c_1,...,c_k$ be the distinct characteristic values of T. For each i, let W_i be the space of characteristic vectors associated with the characteristic value c_i, and let $\mathcal{B}_i$ be an ordered basis for W_i. The lemma before Theorem 2 of unit 12 tells us that $\mathcal{B}' = (\mathcal{B}_1,...,\mathcal{B}_k)$ is an ordered basis for W. In particular,

$$\dim W = \dim W_1 + ... + \dim W_k.$$

Let $\mathcal{B}' = \{\alpha_1,...,\alpha_r\}$ so that the first few α's form the basis $\mathcal{B}_1$, the next few $\mathcal{B}_2$, and so on. Then

$$T\alpha_i = t_i\alpha_i, \qquad i = 1,...,r$$

where $(t_1,..., t_r) = (c_1, c_1,..., c_1,..., c_k, c_k,..., c_k)$ with c_i repeated dim W_i times.

Now W is invariant under T, since for each α in W we have

$$\alpha = x_1\alpha_1 + ... + x_r\alpha_r$$

$$T_\alpha = t_1x_1\alpha_1 + ... + t_rx_r\alpha_r$$

Notes

Choose any other vectors $\alpha_{r+1},..., \alpha_n$ in V such that $\mathcal{B} = \{\alpha_1,...,\alpha_n\}$ is a basis for V. The matrix of T relative to $\mathcal{B}$ has the block form (3), and the matrix of the restriction operator Tw relative to the basis $\mathcal{B}'$ is

$$B = \begin{bmatrix} t_1 & 0 & \cdots & 0 \\ 0 & t_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & t_r \end{bmatrix}$$

The characteristic polynomial of B (i.e., of Tw) is

$$g = (x - c_1)^{e_1} \ldots (x - c_k)^{e_k}$$

where $e_i = \dim W_i$. Furthermore, g divides f, the characteristic polynomial for T. Therefore, the multiplicity of c_i as a root of f is at least $\dim W_i$.

All of this should make Theorem 2 of unit 12 transparent. It merely says that T is diagonalizable if and only if $r = n$, if and only if $e_1 + \ldots + e_k = n$. It does not help us too much with the non-diagonalizable case, since we don't know the matrices C and D of (3).

Lemma: If W is an invariant subspace for T, then W is invariant under every polynomial in T. Thus, for each α in V, the conductor $S_T(\alpha; W)$ is an ideal in the polynomial algebra $F[x]$.

Proof: If β is in W, then $T\beta$ is in W. Consequently, $T(T\beta) = T^2\beta$ is in W. By induction, $T^k\beta$ is in W for each k. Take linear combinations to see that $f(T)\beta$ is in W for every polynomial f.

The definition of $S_T(\alpha; W)$ makes sense if W is any subset of V. If W is a subspace, then $S_T(\alpha; W)$ is a subspace of $F[x]$, because

$$(cf + g)(T) = cf(T) + g(T)$$

If W is also invariant under T, let g be a polynomial in $S_T(\alpha; W)$, i.e., let $g(T)\alpha$ be in W. If f is any polynomial, then $f(T)[g(T)\alpha]$ will be in W. Since

$$(fg)(T) = f(T)g(T)$$

fg is in $S_T(\alpha; W)$. Thus the conductor absorbs multiplication by any polynomial.

The unique monic generator of the ideal $S_T(\alpha; W)$ is also called the T-conductor of α into W (the T-annihilator in case $W = \{0\}$). The T-conductor of α into W is the monic polynomial g of least degree such that $g(T)\alpha$ is in W. A polynomial f is in $S_T(\alpha; W)$ if and only if g divides f. Note that the conductor $S_T(\alpha; W)$ always contains the minimal polynomial for T; hence, every T-conductor divides the minimal polynomial for T.

As the first illustration of how to use the conductor $S_T(\alpha; W)$, we shall characterize triangulable operators. The linear operator T is called triangulable if there is an ordered basis in which T is represented by a triangular matrix.

Lemma. Let V be a finite-dimensional vector space over the field F. Let T be a linear operator on V such that the minimal polynomial for T is a product of linear factors

$$p = (x - c_1)^{r_1} \ldots (x - c_k)^{r_k}, \quad c_i \text{ in } F$$

Let W be a proper ($W \neq V$) subspace of V which is invariant under T. There exists a vector α in V such that

(a) α is not in W;

(b) $(T - cI)\alpha$ is in W, for some characteristic value c of the operator T.

Notes

Proof: What (a) and (b) say is that the T-conductor of α into W is a linear polynomial. Let β be any vector in V which is not in W. Let g be the T-conductor of β into W. Then g divides p, the minimal polynomial for T. Since β is not in W, the polynomial g is not constant. Therefore,

$$g = (x - c_1)^{e_1} \dots (x - c_k)^{e_k}$$

where at least one of the integers e_i is positive. Choose j so that $e_j > 0$.

Then $(x - c_j)$ divides g:

$$g = (x - c_j)h$$

By the definition of g, the vector $\alpha = h(T)\beta$ cannot be in W. But

$$\begin{aligned}(T - c_jI)\alpha &= (T - c_jI)h(T)\beta \\ &= g(T)\beta\end{aligned}$$

is in W.

Theorem 1: Let V be a finite-dimensional vector space over the field F and let T be a linear operator on V. Then T is triangulable if and only if the minimal polynomial for T is a product of linear polynomials over F.

Proof: Suppose that the minimal polynomial factors

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

By repeated application of the lemma above, we shall arrive at an ordered basis $\mathcal{B} = \{\alpha_1,\dots,\alpha_n\}$ in which the matrix representing T is upper triangular:

$$[T]_{\mathcal{B}} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & a_{22} & a_{23} & \cdots & a_{2n} \\ 0 & 0 & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & a_{nn} \end{bmatrix} \qquad \dots(4)$$

Now (4) merely says that

$$T\alpha_j = \alpha_{1j}\alpha_1 + \dots + \alpha_{jj}\alpha_j, \qquad 1 \le j \le n \qquad \dots(5)$$

that is, $T\alpha_j$ is in the subspace spanned by $\alpha_1,\dots,\alpha_j$. To find $\alpha_1,\dots,\alpha_n$, we start by applying the lemma to the subspace $W = \{0\}$, to obtain the vector α_1. Then apply the lemma to W_1, the space spanned by α_1, and we obtain α_2. Next apply the lemma to W_2, the space spanned by α_1 and α_2. Continue in that way. One point deserves comment. After $\alpha_1,\dots, \alpha_i$ have been found, it is the triangular-type relations (5) for $j = 1,\dots, i$ which ensure that the subspace spanned by $\alpha_1,\dots, \alpha_i$ is invariant under T.

If T is triangulable, it is evident that the characteristic polynomial for T has the form

$$f = (x - c_1)^{d_1} \dots (x - c_k)^{d_k}, \qquad c_i \text{ in } F$$

Just look at the triangular matrix (4). The diagonal entries $a_{11},\dots, a_{1n}$ are the characteristic values, with c_i repeated d_i times. But, if f can be so factored, so can the minimal polynomial p, because it divides f.

Corollary: Let F be an algebraically closed field, e.g., the complex number field. Every $n \times n$ matrix over F is similar over F to a triangular matrix.

Theorem 2: Let V be a finite-dimensional vector space over the field F and let T be a linear operator on V. Then T is diagonalizable if and only if the minimal polynomial for T has the form

Notes

$$p = (x - c_1) \dots (x - c_k)$$

where $c_1,\dots, c_k$ are distinct elements of F.

Proof: We have noted earlier that, if T is diagonalizable, its minimal polynomial is a product of distinct linear factors. To prove the converse, let W be the subspace spanned by all of the characteristic vectors of T, and suppose $W \neq V$. By the lemma used in the proof of Theorem 1, there is a vector α not in W and a characteristic value c_j of T such that the vector

$$\beta = (T - c_jI)\alpha$$

lies in W. Since β is in W,

$$\beta = \beta_1 + \dots + \beta_k$$

where $T\beta_i = c_i\beta_i$, $1 \leq i \leq k$, and therefore the vector

$$h(T)\beta = h(c_1)\beta_1 + \dots + h(c_k)\beta_k$$

is in W, for every polynomial h.

Now $p = (x - c_j)q$, for some polynomial q. Also

$$q - q(c_j) = (x - c_j)h$$

We have

$$q(T)\alpha - q(c_j)\alpha = h(T)(T - c_jI)\alpha = h(T')\beta$$

But $h(T)\beta$ is in W and, since

$$0 = p(T)\alpha = (T - c_jI)q(T)\alpha$$

the vector $q(T)\alpha$ is in W. Therefore, $q(c_j)\alpha$ is in W. Since α is not in W, we have $q(c_j) = 0$. That contradicts the fact that p has distinct roots.

In addition to being an elegant result, Theorem 2 is useful in a computational way. Suppose we have a linear operator T, represented by the matrix A in some ordered basis, and we wish to know if T is diagonalizable. We compute the characteristic polynomial f. If we can factor f:

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

we have two different methods for determining whether or not T is diagonalizable. One method is to see whether (for each i) we can find d_i independent characteristic vectors associated with the characteristic value c_i. The other method is to check whether or not $(T - c_1I) \cdots (T - c_kI)$ is the zero operator.

Theorem 1 provides a different proof of the Cayley-Hamilton theorem. That theorem is easy for a triangular matrix. Hence, via Theorem 1, we obtain the result for any matrix over an algebraically closed field. Any field is a subfield of an algebraically closed field. If one knows that result, one obtains a proof of the Cayley-Hamilton theorem for matrices over any field. If we at least admit into our discussion the Fundamental Theorem of Algebra (the complex number field is algebraically closed), then Theorem 1 provides a proof of the Cayley-Hamilton theorem for complex matrices, and that proof is independent of the one which we gave earlier.

Self Assessment

1. Let T be the linear operator on R^2, the matrix of which in the standard ordered basis is

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

Notes

(a) Prove that the only subspaces of R^2 invariant under T are R^2 and the zero subspace.

(b) If U is the linear operator on C^2, the matrix of which in the standard ordered basis is A, show that U has 1-dimensional invariant subspaces.

2. Let W be an invariant subspace for T. Prove that the minimal polynomial for the restriction operator T_W divides the minimal polynomial for T, without referring to matrices.

14.3 Summary

- In this unit the idea of invariant subspace of a linear operator T on the n dimension space helps in introducing a restriction operator Tw as well as a conductor of a vector $\alpha \in V$ into the subspace W.
- These concepts generally help us in the diagonalizing of the matrix of the linear operator T.
- These concepts also lead to triangular form of the matrix A of the linear operator T if A is diagonalizable.

14.4 Keywords

Invariant: If T is any linear operator on V, then V is invariant under T, as is the zero subspace. The range of T and the null space of T are also invariant under T.

Restriction Operator: By introducing the concepts of the restriction operator T_w and the conductor of a vector into the invariant sub-space the characteristic polynomial of the linear operator is cast into a form where the matrix of T can be seen to be diagonalizable or not.

Restriction: T induces a linear operator on W, called restriction to W.

14.5 Review Questions

1. Show that for the matrix A

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

$A^2 = A$.

Find the characteristic values of A.

2. Show that every matrix A such that $A^2 = A$ is similar to a diagonal matrix.

14.6 Further Readings

Books

Kenneth Hoffman and Ray Kunze, *Linear Algebra*

Michael Artin, *Algebra*

Notes

Unit 15: Simultaneous Triangulation and Simultaneous Diagonalization

CONTENTS

Objectives

After studying this unit, you will be able to:

- Know the structure of the triangular form of a matrix of a linear operator T on a space V over the field F.
- Understand that we can diagonalize two or more commuting matrices simultaneously.
- Know that the matrix of a linear operator T commutes with that of a polynomial of a linear operator T.

Introduction

In this unit we are again exploring the properties of a linear operator on the space V over the field F.

In an upper triangular or lower triangular matrix the elements in the diagonal are the characteristic values.

15.1 Simultaneous Triangulation and Simultaneous Diagonalization

Let V be a finite-dimensional space and let $\mathcal{F}$ be a family of linear operators on V. We ask when we can simultaneously triangulate or diagonalize the operators in $\mathcal{F}$, i.e., find one basis $\mathcal{B}$ such that all of the matrices $[T]_{\mathcal{B}}$, T in $\mathcal{F}$, are triangular (or diagonal). In the case of diagonalization, it is necessary that $\mathcal{F}$ be a commuting family of operators: $UT = TU$ for all T, U in $\mathcal{F}$. That follows from the fact that all diagonal matrices commute. Of course, it is also necessary that each operator in $\mathcal{F}$ be a diagonalizable operator. In order to simultaneously triangulate, each operator in $\mathcal{F}$ must be triangulable. It is not necessary that $\mathcal{F}$ be a commuting family; however that condition is sufficient for simultaneous triangulation (if each T can be individually triangulated). These results follow from minor variations of the proofs of Theorems 1 and 2 of unit 14.

The subspace W is invariant under (the family of operators) $\mathcal{F}$ if W is invariant under each operator in $\mathcal{F}$.

Lemma: Let $\mathcal{F}$ be a commuting family of triangulable linear operator on V. Let W be a proper subspace of V which is invariant under $\mathcal{F}$. There exists a vector α in V such that

(a) α is not in W;

(b) for each T in $\mathcal{F}$, the vector $T\alpha$ is in the subspace spanned by α and W.

Notes

Proof: It is no loss of generality to assume that $\mathcal{F}$ contains only a finite number of operators, because of this observation. Let $\{T_1,...,T_n\}$ be a maximal linearly independent subset of $\mathcal{F}$, i.e., a basis for the subspace spanned by $\mathcal{F}$. If α is a vector such that (b) holds for each T_i, then (b) will hold for every operator which is a linear combination of $T_1,..., T_r$.

By the lemma before Theorem 1 of unit 14 (this lemma for a single operator), we can find a vector β_1 (not in W) and a scalar c_1 such that $(T_1 - c_1I)\beta_1$ is in W. Let V_1 be the collection of all vectors β in V such that $(T_1 - c_1I)\beta$ is in W. Then V_1 is a subspace of V which is properly larger than W. Furthermore, V_1 is invariant under $\mathcal{F}$, for this reason. If T commutes with T_1, then

$$(T_1 - c_1I)(T\beta) = T(T_1 - c_1I)\beta$$

If β is in V_1, then $(T_1 - c_1I)\beta$ is in W. Since W is invariant under each T in $\mathcal{F}$, we have $T(T_1 - c_1I)\beta$ in W, i.e., $T\beta$ in V_1, for all β in V_1 and all T in $\mathcal{F}$.

Now W is a proper subspace of V_1. Let U_2 be the linear operator on V_1 obtained by restricting T_2 to the subspace V_1. The minimal polynomial for U_2 divides the minimal polynomial for T_2. Therefore, we may apply the lemma before Theorem 1 of unit 14 to that operator and the invariant subspace W. We obtain a vector β_2 in V_1 (not in W) and a scalar c_2 such that $(T_2 - c_2I)\ \beta_2$ is in W. Note that

(a) β_2 is not in W;

(b) $(T_1 - c_1I)\beta_2$ is in W;

(c) $(T_2 - c_2I)\beta_2$ is in W.

Let V_2 be the set of all vectors β in V_1 such that $(T_2 - c_2I)\beta$ is in W. Then V_2 is invariant under $\mathcal{F}$. Apply the lemma before Theorem 1 of unit 14 to U_3, the restriction of T_3 to V_2. If we continue in this way, we shall reach a vector $\alpha = \beta_r$ (not in W) such that $(T_j - c_jI)\alpha$ is in W, $j = 1,..., r$.

Theorem 1: Let V be a finite-dimensional vector space over the field F. Let $\mathcal{F}$ be a commuting family of triangulable linear operators on V. There exists an ordered basis for V such that every operator in $\mathcal{F}$ is represented by a triangular matrix in that basis.

Proof: Given the lemma which we just proved, this theorem has the same proof as does Theorem 1 of unit 14, if one replaces T by $\mathcal{F}$.

Corollary: Let $\mathcal{F}$ be a commuting family of $n \times n$ matrices over an algebraically closed field F. There exists a non-singular $n \times n$ matrix P with entries in F such that $P^{-1}AP$ is upper-triangular, for every matrix A in $\mathcal{F}$.

Theorem 2: Let F be a commuting family of diagonalizable linear operators on the finite-dimensional vector space V. There exists an ordered basis for V such that every operator in $\mathcal{F}$ is represented in that basis by a diagonal matrix.

Proof: We could prove this theorem by adapting the lemma before Theorem 1 to the diagonalizable case, just as we adapted the lemma before Theorem 1 of unit 14 to the diagonalizable case in order to prove Theorem 2 of unit 14. However, at this point it is easier to proceed by induction on the dimension of V.

If dim $V = 1$, there is nothing to prove. Assume the theorem for vector spaces of dimension less than n, and let V be an n-dimensional space. Choose any T in $\mathcal{F}$ which is not a scalar multiple of the identity. Let $c_1,..., c_k$ be the distinct characteristic values of T, and (for each i) let W_i be the null space of $T - c_iI$. Fix an index i. Then W_i is invariant under every operator which commutes with T. Let $\mathcal{F}_i$ be the family of linear operators on W_i obtained by restricting the operators in $\mathcal{F}$ to the (invariant) subspace W_i. Each operator in $\mathcal{F}_i$ is diagonalizable, because its minimal polynomial divides the minimal polynomial for the corresponding operator in $\mathcal{F}$. Since dim $W_i <$ dim V, the operators in $\mathcal{F}_i$ can be simultaneously diagonalized. In other words, W_i has a

Notes

basis $\mathcal{B}_i$ which consists of vectors which are simultaneously characteristic vectors for every operator in $\mathcal{F}_i$.

Since T is diagonalizable, the lemma before Theorem 2 of unit 12 tells us that $\mathcal{B} = (\mathcal{B}_1,..., \mathcal{B}_k)$ is a basis for V. That is the basis we seek.

If we consider finite dimensional vector space V over a complex field F, then there is a basis such that the matrix of the linear operator T is diagonal. This is due to the key fact that every complex polynomial of positive degree has a root. This tells us that every linear operator has at least one eigenvector.

From the theorem above we now have that every complex $n \times n$ matrix A is similar to an upper triangular matrix i.e. there is a matrix P, such that $P^{-1} AP$ is upper triangular.

Equally we also state that for a linear operator T on a finite dimensional complex vector space V, there is a basis β of V such that the matrix of T with respect to that basis is upper triangular.

Let V contain an eigenvector of A, call it v_1. Let λ be its eigenvalue. We extend (v_1) to a Basis $\beta = (v_1, v_2, \ldots, v_n)$ for V. There will be a matrix P for which the new matrix $A' = P^{-1} A P$ has the block form

$$A' = \left[\begin{array}{c|c} \lambda & * \\ \hline O & D \end{array}\right]$$

where D is an $(n - 1) \times (n - 1)$ matrix, λ is a 1×1 matrix of the restriction of T to $W(v_1)$. Here O denotes $n - 1$ zeros below λ in the first column. By induction on n, we may assume that there exists a matrix Q such that $Q^{-1} D Q$ is upper triangular. If we denote Q_1 by the relation

$$Q_1 = \left[\begin{array}{c|c} 1 & O \\ \hline O & Q \end{array}\right]$$

then

$$A'' = Q_1^{-1} A' Q_1 = \left[\begin{array}{c|c} \lambda & * \\ \hline O & Q^{-1} D Q \end{array}\right]$$

is the upper triangular and thus

$$A'' = (P\, Q_1)^{-1} A\, (P\, Q_1).$$

Knowing one vector v corresponding to the characteristic value λ we can find a linear operator P and then Q_1 to find A''.

Self Assessment

1. Find an invertible real matrix P such that $P^{-1}AP$ and $P^{-1}BP$ are both diagonal, where A and B are the real matrices

   (a) $A = \begin{bmatrix} 1 & 2 \\ 0 & 2 \end{bmatrix}$, $\quad B = \begin{bmatrix} 3 & -8 \\ 0 & -1 \end{bmatrix}$

   (b) $A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$, $\quad B = \begin{bmatrix} 1 & a \\ a & 1 \end{bmatrix}$

Notes

2. Let $\mathcal{F}$ be a commuting family of 3 × 3 complex matrices. How many linearly independent matrices can $\mathcal{F}$ contain? What about the $n \times n$ case?

15.2 Summary

- In this unit we are dealing with matrices that commute with each other.
- In a triangular matrix the main diagonal has the entries of the characteristic values and it has not zero entries in the upper part of the diagonal only or non-zero entries in the lower of the main diagonal.
- If two or more matrices commute then we can diagonalize them simultaneously.

15.3 Keywords

Diagonalizable: Each operator in $\mathcal{F}_i$ is diagonalizable, because its minimal polynomial divides the minimal polynomial for the corresponding operator in $\mathcal{F}$.

Ordered Basis: There exists an ordered basis for V such that every operator in $\mathcal{F}$ is represented by a triangular matrix in that basis.

15.4 Review Question

1. Let T be a linear operator on a n-dimension space and suppose that T has n distinct characteristic values. Prove that any linear operator which commutes with T is a polynomial in T.

Answers: Self Assessment

1. (a) $P = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$, (b) $P = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$

2. 3, n

15.5 Further Readings

Books

Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I.N. Herstein, *Topics in Algebra*

Notes

Unit 16: Direct Sum Decompositions of Elementary Canonical Forms

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand the meanings of invariant subspaces as well as decomposition of a vector space into the invariant direct sums of the independent subspaces.
- Know the projection operators and their properties
- See that there is less emphasis is on matrices and more attention is given to subspaces.

Introduction

This unit and the next units are slightly more complicated than the other previous units. The ideas of invariant subspaces and their relations with the vector space V is obtained.

The ideas of projection operators and their properties are introduced. These ideas will help in expressing the given linear operator T in terms of the direct sums of the operators T_{1j} T_K as seen in the next unit.

16.1 Overview

We are again going to analyse a single linear operator on a finite dimensional space V over the field F. In the next three units we shall stress less in terms of matrices and stress more on the subspaces, in order to find an ordered basis in which the matrix of T assumes an especially a simple form. Our aim in three units will be as follows: To decompose the underlying space V into a sum of invariant subspaces for T such that the restriction operators on these subspaces are simple. These subspaces will be taken as independent subspaces of the vector space V and after finding the independent basis of each independent subspace the ordered basis of the whole space will be constructed. Given such a decomposition of the vector space we then see that T induces a linear operator T_i on each subspace W_i, by restriction. We shall describe this situation by saying that the linear operator is the invariant direct sum of the operators T_1, T_2,..., T_k. Once the space is decomposed in terms of invariant subspaces, we shall introduce the concepts of projection operators on V.

16.2 Direct-sum Decompositions

Notes

Definition: Let $W_1,..., W_k$ be subspaces of the vector space V. We say that $W_1,..., W_k$ are independent if

$$\alpha_1 + ... + \alpha_k = 0, \qquad \alpha_i \text{ in } W_i$$

implies that each α_i is 0.

For $k = 2$, the meaning of independence is {0} intersection, i.e., W_1 and W_2 are independent if and only if $W_1 \cap W_2 = \{0\}$. If $k > 2$, the independence of $W_1,..., W_k$ says much more than $W_1 \cap ... \cap W_k = \{0\}$. It says that each W_j intersects the sum of the other subspaces W_i only in the zero vector.

The significance of independence is this. Let $W = W_1 + ... + W_k$ be the subspace spanned by $W_1,..., W_k$. Each vector α in W can be expressed as a sum

$$\alpha = \alpha_1 + ... + \alpha_k, \qquad \alpha_i \text{ in } W_i.$$

If $W_1,..., W_k$ are independent, then that expression for α is unique; for if

$$\alpha = \beta_1 + ... + \beta_k, \qquad \beta_i \text{ in } W_i$$

then $0 = (\alpha_1 - \beta_1) + ... + (\alpha_k - \beta_k)$, hence $\alpha_i - \beta_i = 0$, $i = 1,..., k$. Thus, when $W_1,..., W_k$ are independent, we can operate with the vectors in W as k-tuples $(\alpha_1,..., \alpha_k)$, α_i in W_i, in the same way as we operate with vectors in R^k as k-tuples of numbers.

Lemma: Let V be a finite-dimensional vector space. Let $W_1,..., W_k$ be subspaces of V and let $W = W_1 + ... + W_k$. The following are equivalent.

(a) $W_1,..., W_k$ are independent.

(b) For each j, $2 \le j \le k$, we have

$$W_j \cap (W_1 + ... + W_{j-1}) = \{0\}$$

(c) If $\mathcal{B}_i$ is an ordered basis for W_i, $1 \le i \le k$, then the sequence $\mathcal{B} = (\mathcal{B}_1,..., \mathcal{B}_k)$ is an ordered basis for W.

Proof: Assume (a). Let α be a vector in the intersection $W_j \cap (W_1 + ... + W_{j-1})$. Then there are vectors $\alpha_1,..., \alpha_{j-1}$ with α_i in W_i such that $\alpha = \alpha_1 + ... + \alpha_{j-1}$. Since

$$\alpha_1 + ... + \alpha_{j-1} + (-\alpha) + 0 + ... + 0 = 0$$

and since $W_1, ..., W_k$ are independent, it must be that $\alpha_1 = \alpha_2 = ... = \alpha_{j-1} = \alpha = 0$.

Now, let us observe that (b) implies (a). Suppose

$$0 = \alpha_1 + ... + \alpha_k, \qquad \alpha_i \text{ in } W_i$$

Let j be the largest integer i such that $\alpha_i \neq 0$. Then

$$0 = \alpha_1 + ... + \alpha_j, \qquad \alpha_j \neq 0.$$

Thus $\alpha_j = -\alpha_1 - ... - \alpha_{j-1}$ is a non-zero vector in $W_j \cap (W_1 + ... + W_{j-1})$.

Now that we know (a) and (b) are the same, let us see why (a) is equivalent to (c). Assume (a). Let $\mathcal{B}_i$ be basis for W_i, $1 \le i \le k$, and let $\mathcal{B} = (\mathcal{B}_1,..., \mathcal{B}_k)$. Any linear relation between the vectors in $\mathcal{B}$ will have the form

$$\beta_1 + ... + \beta_k = 0$$

where β_i is some linear combination of the vectors in $\mathcal{B}_i$. Since $W_1,.., W_k$ are independent, each β_i is 0. Since each $\mathcal{B}_i$ is independent, the relation we have between the vectors in $\mathcal{B}$ is the trivial relation.

Notes

If any (and hence all) of the conditions of the last lemma hold, we say that the sum $W = W_1 + ... + W_k$ is direct or that W is the direct sum of $W_1,..., W_k$ and we write

$$W = W_1 \oplus \cdots \oplus W_k$$

In the literature, the reader may find this direct sum referred to as an independent sum or the interior direct sum of $W_1,..., W_k$.

Example 1: Let V be a finite-dimensional vector space over the field F and let $\{\alpha_1,..., \alpha_n\}$ be any basis for V. If W_i is the one-dimensional subspace spanned by α_i, then $V = W_1 \oplus \cdots \oplus W_n$.

Example 2: Let n be a positive integer and F a subfield of the complex numbers, and let V be the space of all $n \times n$ matrices over F. Let W_1 be the subspace of all symmetric matrices, i.e., matrices A such that $A^t = A$. Let W_2 be the subspace of all skew-symmetric matrices, i.e., matrices A such that $A^t = -A$. Then $V = W_1 \oplus W_2$. If A is any matrix in V, the unique expression for A as a sum of matrices, one in W_1 and the other in W_2, is

$$A = A_1 + A_2$$

$$A_1 = \frac{1}{2}(A + A^t)$$

$$A_2 = \frac{1}{2}(A - A^t)$$

Example 3: Let T be any linear operator on a finite-dimensional space V. Let $c_1,.., c_k$ be the distinct characteristic values of T, and let W_i be the space of characteristic vectors associated with the characteristic value c_i. Then $W_1,..., W_k$ are independent. In particular, if T is diagonalizable, then $V = W_1 \oplus \cdots \oplus W_k$.

Definition: If V is a vector space, a projection of V is a linear operator E on V such that $E^2 = E$.

Suppose that E is a projection. Let R be the range of E and let N be the null space of E.

1. The vector β is in the range R if and only if $E\beta = \beta$. If $\beta = E\alpha$, then $E\beta = E^2\alpha = E\alpha = \beta$. Conversely, if $\beta = E\beta$, then (of course) β is in the range of E.
2. $V = R \oplus N$.
3. The unique expression for α as a sum of vectors in R and N is $\alpha = E\alpha + (\alpha - E\alpha)$.

From (1), (2), (3) it is easy to see the following. If R and N are subspaces of V such that $V = R \oplus N$, there is one and only one projection operator E which has range R and null space N. That operator is called the projection on R along N.

Any projection E is (trivially) diagonalizable. If $\{\alpha_1,..., \alpha_r\}$ is a basis for R and $\{\alpha_{r+1},..., \alpha_n\}$ a basis for N, then the basis $\mathcal{B} = \{\alpha_1,..., \alpha_n\}$ diagonalizes E.

$$[E]_{\mathcal{B}} = \begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix}$$

where I is the $r \times r$ identity matrix. That should help explain some of the terminology connected with projections. The reader should look at various cases in the plane R^2 (or 3-space, R^3), to convince himself that the projection on R along N sends each vector into R by projecting it parallel to N.

Notes

Projections can be used to describe direct-sum decompositions of the space V. For, suppose $V = W_1 \oplus \cdots \oplus W_k$. For each j we shall define an operator E_j on V. Let α be in V, say $\alpha = \alpha_1 + \cdots + \alpha_k$ with α_i in W_i. Define $E_j\alpha = \alpha_j$. Then E_j is a well-defined rule. It is easy to see that E_j is linear, that the range of E_j is W_j, and that $E_j^2 = E_j$. The null space of E_j is the subspace

$$(W_1 + \cdots + W_{j-1} + W_{j+1} + \cdots + W_k)$$

for, the statement that $E_j\alpha = 0$ simply means $\alpha_j = 0$, i.e., that α is actually a sum of vectors from the spaces W_i with $i \neq j$. In terms of the projection E_j we have

$$\alpha = E_1\alpha + \cdots + E_k\alpha$$

for each α in V. What (1) says is that

$$I = E_1 + \cdots + E_k$$

Note also that if $i \neq j$, then $E_iE_j = 0$, because the range of E_j is the subspace W_j which is contained in the null space of E_i. We shall now summarize our findings and state and prove a converse.

Theorem 1: If $V = W_1 \oplus \cdots \oplus W_k$, then there exist k linear operators $E_1,..., E_k$ on V such that

(i) each E_i is a projection $(E_1^2 = E_i)$;

(ii) $E_iE_j = 0$, if $i \neq j$;

(iii) $I = E_1 + \cdots + E_k$;

(iv) the range of E_i is W_i.

Conversely, if $E_1,..., E_k$ are k linear operators on V which satisfy conditions (i), (ii) and (iii), and if we let W_i be the range of E_i, then $V = W_i \oplus \cdots \oplus W_k$.

Proof: We have only to prove the converse statement. Suppose $E_1,..., E_k$ are linear operators on V which satisfy the first three conditions, and let W_i be the range of E_i. Then certainly

$$V = W_1 + \cdots + W_k;$$

for, by condition (iii) we have

$$\alpha = E_1\alpha + \cdots + E_k\alpha$$

for each α in V, and $E_i\alpha$ is in W_i. This expression for α is unique, because if

$$\alpha = \alpha_1 + \cdots + \alpha_k$$

with α_i in W_i, say $\alpha_i = E_i\beta_i$, then using (i) and (ii) we have

$$\begin{aligned} E_j\alpha &= \sum_{i=1}^{k} E_j\alpha_i \\ &= \sum_{i=1}^{k} E_jE_i\beta_i \\ &= E_j^2\beta_j \\ &= E_j\beta_j \\ &= \alpha_j \end{aligned}$$

This shows that V is the direct sum of the W_i.

Notes

Self Assessment

1. Let V be a finite dimensional vector space and W_1 is any subspace of V. Prove that there is a subspace W_2 of V such that $V = W_1 \oplus W_2$.
2. True or false? If a diagonalizable operator has only the characteristic values 0 and 1, it is a projection.
3. Let $E_1, E_2, \ldots E_K$ be linear operators on the space V such that $E_1 + E_2 + \ldots + E_K = I$. Prove that if $E_iE_j = 0$ for $i \neq j$, then $E_i^2 = E_i$ for each i.
4. Let V be a finite dimensional vector space and let $W_1,\ldots W_K$ be subspaces of V such that

$$V = W_1 + W_2 + \ldots + W_K \text{ and } \dim V = \dim W_1 + \ldots + W_K$$

Prove that $V = W_1 \oplus W_2 \oplus \ldots \oplus W_K$.

16.3 Summary

- In this unit the importance is given to the ideas of invariant subspaces of a vector space V for a linear operator T.
- The vector space V is decomposed into a set of linear invariant subspaces.
- The sum of the bases vectors of the invariant subspaces defines the basis vectors of the vector space V.

16.4 Keywords

Skew-symmetric Matrices: Skew-symmetric matrices, i.e., matrices A such that $A^t = -A$.

Subspaces: These subspaces will be taken as independent subspaces of the vector space V and after finding the independent basis of each independent subspace the ordered basis of the whole space will be constructed.

16.5 Review Questions

1. If E_1, E_2 are projections onto independent subspaces, then $E_1 + E_2$ is a projection. True or false?
2. Let E_1, E_2 be linear operators on the space V such that $E_1 + E_2 = I$, and $E_1^2 = E_1$ and $E_2^2 = E_2$, then prove that $E_1E_2 = 0$.

Answer: Self Assessment

2. Yes, true

16.6 Further Readings

Books

Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I.N. Herstein, *Topics in Algebra*

Unit 17: Invariant Direct Sums

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- See that the vector space V is decomposed as a direct sum of the invariant subspaces under some linear operator T.
- Understand that the linear operator induces a linear operator T_i on each invariant subspaces W_i by restriction.
- Know that if α_i is the vector in the invariant subspace W_i then the vector α in the finite vector space V is obtained as a linear combinations of its projections α_i in the subspace W_i.

Introduction

In this unit we again consider a linear transformation T on the finite vector space. Here the vector space is decomposed as the direct sum of the invariant subspaces W_i. The linear operator induces a linear operator T_i for each invariant subspaces W_i.

The method of finding the projection operators and their properties is discussed.

17.1 Overview

In this unit we are primarily interested in the direct sum decomposition $V = W_1 \oplus W_2 \oplus + ... + W_K$, where each of the subspaces W_i is invariant under some linear operator T. Given such a decomposition of V, T induces a linear operator T_i on each W_i by restriction. If α_i is the vector in W_i then the vector α in V can be given as a linear combinations of its projection α_i in the invariant subspace W_i. Thus the action of T is then understood as follows:

If α is a vector in V, we have unique vectors $\alpha_1,..., \alpha_k$ with α_i in W_i such that

$$\alpha = \alpha_1 + ... + \alpha_k$$

and then

$$T\alpha = T_1\alpha_1 + ... + T_k\alpha_k$$

We shall describe this situation by saying that T is the direct sum of the operators $T_1,..., T_k$. It must be remembered in using this terminology that the T_i are not linear operators on the space V but on the various subspaces W_i. The fact that $V = W_1 \oplus ... \oplus W_k$ enables us to associate with each α in

Notes

V a unique k-tuple $(\alpha_1,..., \alpha_k)$ of vectors α_i in W_i (by $\alpha = \alpha_1 + ... + \alpha_k$) in such a way that we can carry out the linear operations in V by working in the individual subspaces W_i. The fact that each W_i is invariant under T enables us to view the action of T as the independent action of the operators T_i on the subspaces W_i. Our purpose is to study T by finding invariant direct-sum decompositions in which the T_i are operators of an elementary nature.

Before looking at an example, let us note the matrix analogue of this situation. Suppose we select an ordered basis $\mathcal{B}_i$ for each W_i, and let it be the ordered basis for V consisting of the union of the $\mathcal{B}_i$ arranged in the order $\mathcal{B}_1,..., \mathcal{B}_k$, so that $\mathcal{B}$ is a basis for V. From our discussion concerning the matrix analogue for a single invariant subspace, it is easy to see that if $A = [T]_{\mathcal{B}}$ and $A_i = [T_i]_{\mathcal{B}}$, then A has the block form

$$A = \begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & A_k \end{bmatrix} \qquad ...(1)$$

In (1), A_i is a $d_i \times d_i$ matrix ($d_i = \dim W_i$), and the 0's are symbols for rectangular blocks of scalar 0's of various sizes. It also seems appropriate to describe (1) by saying that A is the direct sum of the matrices $A_1,..., A_k$.

Most often, we shall describe the subspace W_i by means of the associated projections E_i (Theorem 1 of unit 16). Therefore, we need to be able to phrase the invariance of the subspaces W_i in terms of the E_i.

17.2 Some Theorems

Theorem 1: Let T be a linear operator on the space V, and $W_1,..., W_k$ and $E_1,..., E_k$ be as in Theorem 1 of unit 16. Then a necessary and sufficient condition that each subspace W_i be invariant under T is that T commutes with each of the projections E_i, i.e.,

$$TE_i = E_iT, \qquad i = 1,..., k$$

Proof: Suppose T commutes with each E_i. Let α be in W_j. Then $E_j\alpha = \alpha$, and

$$\begin{aligned} T\alpha &= T(E_j\alpha) \\ &= E_j(T\alpha) \end{aligned}$$

which shows that $T\alpha$ is in the range of E_j, i.e., that W_j is invariant under T.

Assume now that each W_i is invariant under T. We shall show that $TE_j = E_jT$. Let α be any vector in V. Then

$$\begin{aligned} \alpha &= E_1\alpha + ... + E_k\alpha \\ T\alpha &= TE_1\alpha + ... + TE_k\alpha \end{aligned}$$

Since $E_i\alpha$ is in W_i, which is invariant under T, we must have $T(E_i\alpha) = E_i\beta_i$ for some vector β_i. Then

$$\begin{aligned} E_jTE_i\alpha &= E_jE_i\beta_i \\ &= \begin{cases} 0, & \text{if } i \neq j \\ E_j\beta_j, & \text{if } i = j \end{cases} \end{aligned}$$

Thus

$$\begin{aligned} E_jT\alpha &= E_jTE_1\alpha + ... + E_jTE_k\alpha \\ &= E_j\beta_j \end{aligned}$$

Notes

$$= TE_j\alpha$$

This holds for each α in V, so $E_jT = TE_j$.

We shall now describe a diagonalizable operator T in the language of invariant direct sum decompositions (projections which commute with T). This will be a great help to us in understanding some deeper decomposition theorems later. The description which we are about to give is rather complicated, in comparison to the matrix formulation or to the simple statement that the characteristic vectors of T span the underlying space. But, we should bear in mind that this is our first glimpse at a very effective method, by means of which various problems concerned with subspaces, bases, matrices, and the like can be reduced to algebraic calculations with linear operators. With a little experience, the efficiency and elegance of this method of reasoning should become apparent.

Theorem 2: Let T be a linear operator on a finite-dimensional space V. If T is diagonalizable and if $c_1,..., c_k$ are the distinct characteristic values of T, then there exist linear operators $E_1,..., E_k$ on V such that

(i) $T = c_1E_1 + ... + c_kE_k$;

(ii) $I = 'E_1 + ... + E_k$;

(iii) $E_iE_j = 0, i \neq j$;

(iv) $E_1^2 = E_i$ (E_i is a projection);

(v) the range of E_i is the characteristic space for T associated with c_i.

Conversely, if there exist k distinct scalars $c_1,..., c_k$ and k non-zero linear operators $E_1,..., E_k$ which satisfy conditions (i), (ii), and (iii), then T is diagonalizable, $c_1,..., c_k$ are the distinct characteristic values of T, and conditions (iv) and (v) are satisfied also.

Proof: Suppose that T is diagonalizable, with distinct characteristic values $c_1,..., c_k$. Let W_i be the space of characteristic vectors associated with the characteristic value c_i. As we have seen,

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

Let $E_1,...,E_k$ be the projections associated with this decomposition, as in Theorem 1 of unit 16. Then (ii), (iii), (iv) and (v) are satisfied. To verify (i), proceed as follows. For each α in V,

$$\alpha = E_1\alpha + ... + E_k\alpha$$

and so

$$T\alpha = TE_1\alpha + ... + TE_k\alpha$$
$$= c_1E_1\alpha + ... + c_kE_k\alpha$$

In other words, $T = c_1E_1 + ... + c_kE_k$.

Now suppose that we are given a linear operator T along with distinct scalars c_i and non-zero operators E_i which satisfy (i), (ii) and (iii). Since $E_iE_j = 0$ when $i \neq j$, we multiply both sides of $I = E_1 + ... + E_k$ by E_i and obtain immediately $E_i^2 = E_i$. Multiplying $T = c_1E_1 + ... + c_kE_k$ by E_i, we then have $TE_i = c_iE_i$, which shows that any vector in the range of E_i is in the null space of $(T - c_iI)$. Since we have assumed that $E_i \neq 0$, this proves that there is a non-zero vector in the null space of $(T - c_iI)$, i.e., that c_i is a characteristic value of T. Furthermore, the c_i are all of the characteristic values of T; for, if c is any scalar, then

$$T - cI = (c_1 - c)E_1 + ... + (c_k - c)E_k$$

so if $(T - cI)\alpha = 0$, we must have $(c_i - c)E_i\alpha = 0$. If α is not the zero vector, then $E_i\alpha \neq 0$ for some i, so that for this i we have $c_i - c = 0$.

Notes

Certainly T is diagonalizable, since we have shown that every non-zero vector in the range of E_i is a characteristic vector of T, and the fact that $I = E_1 + ... + E_k$ shows that these characteristic vectors span V. All that remains to be demonstrated is that the null space of $(T - c_iI)$ is exactly the range of E_i. But this is clear, because if $T\alpha = c_i\alpha$, then

$$\sum_{j=1}^{k}(c_j - c_i)E_j\alpha = 0$$

hence

$$(c_j - c_i)E_j\alpha = 0 \qquad \text{for each } j$$

and then

$$E_j\alpha = 0 \qquad j \neq i$$

Since $\alpha = E_1\alpha + ... + E_k\alpha$, and $E_j\alpha = 0$ for $j \neq i$, we have $\alpha = E_i\alpha$, which proves that α is in the range of E_i.

One part of Theorem 1 of unit 16 says that for a diagonalizable operator T, the scalars $c_1,..., c_k$ and the operators $E_1,..., E_k$ are uniquely determined by conditions (i), (ii), (iii), the fact that the c_i are distinct, and the fact that the E_i are non-zero. One of the pleasant features of the decomposition $T = c_1E_1 + ... + c_kE_k$ is that if g is any polynomial over the field F, then

$$g(T) = g(c_1)E_1 + ... + g(c_k)E_k.$$

To see how it is proved one need only compute T^r for each positive integer r. For example,

$$T^2 = \sum_{i=1}^{k}c_iE_i\sum_{j=1}^{k}c_jE_j$$

$$= \sum_{i=1}^{k}\sum_{j=1}^{k}c_ic_jE_iE_j$$

$$= \sum_{i=1}^{k}c_i^2E_i^2$$

$$= \sum_{i=1}^{k}c_i^2E_i$$

The reader should compare this with $g(A)$ where A is a diagonal matrix; for then $g(A)$ is simply the diagonal matrix with diagonal entries $g(A_{11}), ..., g(A_{nn})$.

We should like in particular to note what happens when one applies the Lagrange polynomials corresponding to the scalars $c_1,..., c_k$:

$$p_j = \prod_{i \neq j}\frac{(x - c_i)}{(c_j - c_i)}$$

We have $p_j(c_i) = \delta_{ij}$, which means that

$$p_j(T) = \sum_{i=1}^{k}\delta_{ij}E_i$$

$$= E_j$$

Thus the projections E_j not only commute with T but are polynomials in T.

Such calculations with polynomials in T can be used to give an alternative proof of Theorem 2 of unit 14, which characterized diagonalizable operators in terms of their minimal polynomials. The proof is entirely independent of our earlier proof.

Notes

If T is diagonalizable, $T = c_1E_1 + ... + c_kE_k$, then

$$g(T) = g(c_1)E_1 + ... + g(c_k)E_k$$

for every polynomial g. Thus $g(T) = 0$ if and only if $g(c_i) = 0$ for each i. In particular, the minimal polynomial for T is

$$p = (x - c_1) ... (x - c_k)$$

Now suppose T is a linear operator with minimal polynomial $p = (x - c_1) ... (x - c_k)$, where $c_1,..., c_k$ are distinct elements of the scalar field. We form the Lagrange polynomials

$$p_j = \prod_{i \neq j} \frac{(x - c_i)}{(c_j - c_i)}$$

So that $p_j(c_i) = \delta_{ij}$ and for any polynomial g of degree less than or equal to $(k - 1)$ we have

$$g = g(c_1)p_1 + ... + g(c_k)p_k$$

Taking g to be the scalar polynomial 1 and then the polynomial x, we have

$$\left.\begin{aligned} 1 &= p_1 + \cdots + p_k \\ x &= c_1p_1 + \cdots + c_kp_k \end{aligned}\right\} \quad ...(2)$$

You will note that the application to x may not be valid because k may be 1. But if $k = 1$, T is a scalar multiple of the identity and hence diagonalizable). Now let $E_j = p_j(T)$. From (2) we have

$$\left.\begin{aligned} I &= E_1 + \cdots + E_k \\ T &= c_1E_1 + \cdots + c_kE_k \end{aligned}\right\} \quad ...(3)$$

Observe that if $i \neq j$, then $p_i p_j$ is divisible by the minimal polynomial p, because $p_i p_j$ contains every $(x - c_r)$ as a factor. Thus

$$E_iE_j = 0, \qquad i \neq j \quad ...(4)$$

We must note one further thing, namely, that $E_i \neq 0$ for each i. This is because p is the minimal polynomial for T and so we cannot have $p_i(T) = 0$ since p_i has degree less than the degree of p. This last comment, together with (3), (4), and the fact that the c_i are distinct enables us to apply Theorem 2 to conclude that T is diagonalizable.

Self Assessment

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

$$A = \begin{bmatrix} 5 & -6 & -6 \\ -1 & 4 & 2 \\ 3 & -6 & -4 \end{bmatrix}$$

use the Lagrange polynomials to write the representing matrix A in the form $A = E_1 + 2E_2$, $E_1 + E_2 = I$, $E_1E_2 = 0$. Where I is a unit matrix and 0 is zero matrix.

2. Let T be the linear operator on R^4 which is represented by the 4 × 4 matrix

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

Find the matrices E_1, E_2, E_3 such that

$A = C_1E_1 + C_2E_2 + C_3E_3$, $E_1 + E_2 + E_3 = I$ and $E_iE_j = 0$ for $i \neq j$

Notes

17.3 Summary

- In this unit the finite dimensional vector space is decomposed into a direct sum of the invariant subspaces.
- The linear operator induces a linear operator T_i on each invariant subspace W_i by restriction.
- The projection operators can be obtained from the Lagrange polynomials once we know the characteristic values.

17.4 Keywords

Projection Operator: The projection operator E has the property that $E^2 = E$ so its characteristic values can be equal to 0 and unit.

Restriction: When the finite space V is decomposed into the direct sum of the invariant subspaces the linear operator induces a linear operator by the process known as restriction.

The Lagrange Polynomials: Help us to find the projection operators for any linear operator T in terms of the matrix representing T and its characteristic values.

17.5 Review Questions

1. Let T be a linear operator on V. Suppose $V = W_1 \oplus ... \oplus W_k$, where each W_i is invariant under T. Let T_i be the induced (restriction) operator on W_i. Prove that the characteristic polynomial for f is the product of the characteristic polynomials $f_1, f_2,..., f_k$.
2. Let T be a linear operator on three dimensional space which is represented by the matrix

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

Find the matrices E_1, E_2, E_3 such that $A = C_1E_1 + C_2E_2 + C_3E_3$

$E_1 + E_2 + E_3 = I$, $E_iE_j = 0$ for $i \neq j$

Answers: Self Assessment

1. $E_1 = 2I - A$, $E_2 = A - I$, Here $E_1 + E_2 = I$, $A = E_1 + 2E_2$ and $E_1E_2 = 0$
2. Here $c_1 = 0$, $c_2 = -2$, $c_3 = 2$

$E_1 = I - A^2/4$

$$E^2 = \frac{1}{8}(A - 2I)A$$

$$E^3 = \frac{A}{8}(A - 2I)$$

17.6 Further Readings

Books

Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I.N. Herstein, *Topics in Algebra*

Michael Artin, *Algebra*

Unit 18: The Primary Decomposition Theorem

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- See that in considering a linear operator T on a finite dimensional space the minimal polynomial for the linear operator is a product of a number of irreducible monic polynomials $p_i^{r_i}$ over the field F where r_i are positive integers.
- Know that this structure of the minimal polynomial helps in decomposing the space V as the direct sum of the invariant subspaces W_i.
- Understand that the general linear operator T induces a linear operator T_i on W_i by restriction and the minimal polynomial for T_i is the irreducible $p_i^{r_i}$.

Introduction

In this unit the idea of the direct sum decomposition of the vector space V for a linear operator T in terms of invariant subspaces.

The general linear operator T induces a linear operator T_i on the invariant subspace, the minimal polynomial of T_i is the $p_i^{r_i}$.

This structure of the induced linear operator helps in introducing the projection operators E_i.

These projections associated with the primary decomposition of T, then are polynomials in T, and they commute each will an operator that commutes with T.

18.1 Overview

We continue our study of a linear operator T on the finite dimension space. In this unit we are interested in decomposing T into a direct sum of operators which are in some sense elementary. We had already found the characteristic values of the operator and also studied invariant subspaces. The vector space V was shown to be direct sum of the invariant subspaces. We can decompose T into a direct sum of operators through the characteristic values and vectors of T in certain special cases i.e., when the minimal polynomial for T factors over the scalar field F into a product of distinct monic polynomials of degree 1. In dealing with the general T we come

Notes

across with two problems. First, T may not have a single characteristic value due to the limitation of the scalar field. Second, even if the characteristic polynomial factors completely over F into a product of polynomials of degree 1, there may not be enough characteristic vectors for T to span the space V; which is clearly a deficiency in T. The second situation is illustrated by the operator T on F^3 (F any field) represented in the standard basis by

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

The characteristic polynomial for A is $(x-2)^2(x+1)$ and this is plainly also the minimal polynomial for A (or for T). Thus T is not diagonalizable. One sees that this happens because the null space of $(T-2I)$ has dimension 1 only. On the other hand, the null space of $(T+\mathrm{I})$ and the null space of $(T-2I)^2$ together span V, the former being the subspace spanned by $\in_3$ and the latter the subspace spanned by $\in_1$ and $\in_2$.

This will be more or less our general method for the second problem. If (remember this is an assumption) the minimal polynomial for T decomposes

$$p = (x-c_1)^{r_1} \ldots (x-c_k)^{r_2}$$

where $c_1,\ldots, c_k$ are distinct elements of F, then we shall show that the space V is the direct sum of the null spaces of $(T-c_iI)^{r_i}$, $i = 1,\ldots, k$. The hypothesis about p is equivalent to the fact that T is triangulable (Theorem 1 of unit 14); however, that knowledge will not help us.

The theorem which we prove is more general than what we have described, since it works with the primary decomposition of the minimal polynomial, whether or not the primes which enter are all of first degree. The reader will find it helpful to think of the special case when the primes are of degree 1, and even more particularly, to think of the projection-type proof of Theorem 2 of unit 14, a special case of this theorem.

18.2 Primary Decomposition Theorem

Theorem 1 (Primary Decomposition Theorem): Let T be a linear operator on the finite-dimensional vector space V over the field F. Let p be the minimal polynomial for T,

$$p = p_1^{r_1} \cdots p_k^{r}$$

where the p_i are distinct irreducible monic polynomials over F and the r_i are positive integers. Let W_i be the null space of $p_i(T)^{r_i}$, $i = 1,\ldots, k$. Then

(i) $V = W_1 \oplus \cdots \oplus W_k$;

(ii) each W_i is invariant under T;

(iii) if T_i is the operator induced on W_i by T, then the minimal polynomial for T_i is $p_1^{r_1}$.

Proof: The idea of the proof is this. If the direct-sum decomposition (i) is valid, how can we get hold of the projections $E_1,\ldots, E_k$ associated with the decomposition? The projection E_i will be the identity on W_i and zero on the other W_j. We shall find a polynomial h_i such that $h_i(T)$ is the identity on W_i and is zero on the other W_j, and so that $h_1(T) + \cdots + h_k(T) = I$, etc.

For each i, let

$$f_i = \frac{p}{p_i^{r_i}} = \prod_{j \neq i} p_j^{r_i}.$$

Notes

Since $p_1,..., p_k$ are distinct prime polynomials, the polynomials $f_1,..., f_k$ are relatively prime. Thus there are polynomials $g_1,..., g_k$ such that

$$\sum_{i=1}^{n} f_i g_i = 1$$

Note also that if $i \neq j$, then $f_i f_j$ is divisible by the polynomial p, because $f_i f_j$ contains each $p_m^{r_m}$ as a factor. We shall show that the polynomials $h_i = f_i g_i$ behave in the manner described in the first paragraph of the proof.

Let $E_i = h_i(T) = f_i(T)g_i(T)$. Since $h_1 + \cdots + h_k = 1$ and p divides $f_i f_j$ for $i \neq j$, we have

$$E_1 + ... + E_k = I$$

$$E_i E_j = 0, \quad \text{if } i \neq j$$

Thus the E_i are projections which correspond to some direct sum decomposition of the space V. We wish to show that the range of E_i is exactly the subspace W_i. It is clear that each vector in the range of E_i is in W_i, for if α is in the range of E_i, then $\alpha = E_i\alpha$ and so

$$\begin{aligned} p_i(T)^{r_i}\alpha &= p_i(T)^{r_i}E_i\alpha \\ &= p_i(T)^{r_i}f_i(T)g_i(T)\alpha \\ &= 0 \end{aligned}$$

because $p^{r_i}f_i g_i$ is divisible by the minimal polynomial p. Conversely, suppose that α is in the null space of $p_i(T)^{r_i}$. If $j \neq i$, then $f_j g_j$ is divisible by $p_i^{r_i}$ and so $f_j(T)g_j(T)\alpha = 0$, i.e., $E_j\alpha = 0$ for $j \neq$ i. But then it is immediate that $E_i\alpha = \alpha$, i.e., that α is in the range of E_i. This completes the proof of statement (i).

It is certainly clear that the subspaces W_i are invariant under T. If T_i is the operator induced on W_i by T, then evidently $p_i(T_i)^{r_i} = 0$, because by definition $p_i(T)^{r_i}$ is 0 on the subspace W_i. This shows that the minimal polynomial for T_i divides $p_i^{r_i}$. Conversely, let g be any polynomial such that $g(T_i) = 0$. Then $g(T)f_i(T) = 0$. Thus gf_i is divisible by the minimal polynomial p of T, i.e., $p_i^{r_i} f_i$ divides gf_i. It is easily seen that $p_i^{r_i}$ divides g. Hence the minimal polynomial for T_i is $p_i^{r_i}$.

Corollary: If $E_1,..., E_k$ are the projections associated with the primary decomposition of T, then each E_i is a polynomial in T, and accordingly if a linear operator U commutes with T then U commutes with each of the E_i, i.e., each subspace W_i is invariant under U.

In the notation of the proof of Theorem 1, let us take a look at the special case in which the minimal polynomial for T is a product of first degree polynomials, i.e., the case in which each p_i is of the form $p_i = x - c_i$. Now the range of E_i is the null space W_i of $(T - c_i I)^{r_i}$. Let us put $D = c_1E_1 + \cdots + c_kE_k$. By Theorem 2 of unit 17, D is a diagonalizable operator which we shall call the diagonalizable part of T. Let us look at the operator $N = T - D$. Now

$$\begin{aligned} T &= TE_1 + ... + TE_k \\ D &= c_1E_1 + ... + c_kE_k \end{aligned}$$

so

$$N = (T - c_1I)E_1 + ... + (T - c_kI)E_k$$

The reader should be familiar enough with projections by now so that he sees that

$$N^2 = (T - c_1I)^2E_1 + ... + (T - c_kI)^2E_k$$

Notes

and in general that

$$N^r = (T - c_1 I)^r E_1 + \ldots + (T - c_k I)^r E_k .$$

When $r \geq r_i$ for each i, we shall have $N^r = 0$, because the operator $(T - c_i I)^r$ will then be 0 on the range of E_i.

Definition: Let N be a linear operator on the vector space V. We say that N is nilpotent if there is some positive integer r such that $N^r = 0$.

Theorem 2: Let T be a linear operator on the finite-dimensional vector space V over the field F. Suppose that the minimal polynomial for T decomposes over F into a product of linear polynomials. Then there is a diagonalizable operator D on V and a nilpotent operator N on V such that

(i) $T = D + N$,

(ii) $DN = ND$

The diagonalizable operator D and the nilpotent operator N are uniquely determined by (i) and (ii) and each of them is a polynomial in T.

Proof: We have just observed that we can write $T = D + N$ where D is diagonalizable and N is nilpotent, and where D and N not only commute but are polynomials in T. Now suppose that we also have $T = D' + N'$ where D' is diagonalizable, N' is nilpotent, and $D'N' = N'D'$. We shall prove that $D = D'$ and $N = N'$.

Since D' and N' commute with one another and $T = D' + N'$, we see that D' and N' commute with T. Thus D' and N' commute with any polynomial in T; hence they commute with D and with N. Now we have

$$D + N = D' + N'$$

or

$$D - D' = N' - N$$

and all four of these operators commute with one another. Since D and D′ are both diagonalizable and they commute, they are simultaneously diagonalizable, and $D - D'$ is diagonalizable. Since N and N' are both nilpotent and they commute, the operator $(N' - N)$ is nilpotent; for, using the fact that N and N' commute

$$(N' - N)^r = \sum_{j=0}^{r} \binom{r}{j} (N')^{r-j} (-N)^j$$

and so when r is sufficiently large every term in this expression for $(N' - N)^r$ will be 0. (Actually, a nilpotent operator on an n-dimensional space must have its nth power 0; if we take $r = 2n$ above, that will be large enough. It then follows that $r = n$ is large enough, but this is not obvious from the above expression.) Now $D - D'$ is a diagonalizable operator which is also nilpotent. Such an operator is obviously the zero operator; for since it is nilpotent, the minimal polynomial for this operator is of the form x^r for some $r \leq m$; but then since the operator is diagonalizable, the minimal polynomial cannot have a repeated root; hence $r = 1$ and the minimal polynomial is simply x, which says the operator is 0. Thus we see that $D = D'$ and $N = N'$.

Corollary: Let V be a finite-dimensional vector space over an algebraically closed field F, e.g., the field of complex numbers. Then every linear operator T on V can be written as the sum of a diagonalizable operator D and a nilpotent operator N which commute. These operators D and N' are unique and each is a polynomial in T.

From these results, one sees that the study of linear operators on vector spaces over an algebraically closed field is essentially reduced to the study of nilpotent operators. For vector

Notes

spaces over non-algebraically closed fields, we still need to find some substitute for characteristic values and vectors. It is a very interesting fact that these two problems can be handled simultaneously and this is what we shall do in the next units.

In concluding this section, we should like to give examples, which illustrate some of the ideas of the primary decomposition theorem. We have chosen to give it at the end of the section since it deals with differential equations and thus is not purely linear algebra.

Example 1: In the primary decomposition theorem, it is not necessary that the vector space V be finite dimensional, nor is it necessary for parts (i) and (ii) that p be the minimal polynomial for T. If T is a linear operator on an arbitrary vector space and if there is a monic polynomial p such that $p(T) = 0$, then parts (i) and (ii) of Theorem 1 are valid for T with the proof which we gave.

Let n be a positive integer and let V be the space of all n times continuously differentiable functions f on the real line which satisfy the differential equation.

$$\frac{d^n f}{dt^n} + a_{n-1}\frac{d^{n-1} f}{dt^{n-1}} + \cdots + a_1\frac{d_j}{dt} + a_0 f = 0 \qquad ...(1)$$

where $a_0,..., a_{n-1}$ are some fixed constants. If C_n denotes the space of n times continuously differentiable functions, then the space V of solutions of this differential equation is a subspace of C_n. If D denotes the differentiation operator and p is the polynomial

$$p = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$$

then V is the null space of the operator $p(D)$, because (1) simply says $p(D)f = 0$. Therefore, V is invariant under D. Let us now regard D as a linear operator on the subspace V. Then $p(D) = 0$.

If we are discussing differentiable complex-valued functions, then C_n and V are complex vector spaces, and $a_0,..., a_{n-1}$ may be any complex numbers. We now write

$$p = (x - c_1)^{r1} ... (x - c_k)^{rk}$$

where $c_1,..., c_k$ are distinct complex numbers. If W_j is the null space of $(*D - c_j I)^{ri}$, then Theorem 1 says that

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

In other words, if f satisfies the differential equation (1), then f is uniquely expressible in the form

$$f = f_1 + ... + f_k$$

where f_j satisfies the differential equation $(D - c_j I)^{rj} f_j = 0$. Thus, the study of the solutions to the equation (1) is reduced to the study of the space of solutions of a differential equation of the form

$$(D - cI)^r f = 0 \qquad ...(2)$$

This reduction has been accomplished by the general methods of linear algebra, i.e., by the primary decomposition theorem.

To describe the space of solutions to (2), one must know something about differential equations, that is, one must know something about D other than the fact that it is a linear operator. However, one does not need to know very much. It is very easy to establish by induction on r that if f is in C_r then

$$(D - cI)^r f = e^{ct} D^r (e^{-ct} f)$$

Notes

that is,

$$\frac{df}{dt} - cf(t) = e^{ct}\frac{d}{dt}(e^{-ct}f), \quad \text{etc.}$$

Thus $(D - cI)^r f = 0$ if and only if $D^r(e^{-ct}f) = 0$. A function g such that $D^r g = 0$, i.e., $d^r g/dt^r = 0$, must be a polynomial function of degree $(r - 1)$ or less:

$$g(t) = b_0 + b_1 t + \cdots + b_{r-1}t^{r-1}$$

Thus f satisfies (2) if and only if f has the form

$$f(t) = e^{ct}(b_0 + b_1 t + \ldots + b_{r-1}t^{r-1})$$

Accordingly, 'the functions' e^{ct}, te^{ct}, ..., $t^{r-1}e^{ct}$ span the space of solutions of (2). Since 1, t,..., t^{r-1} are linearly independent functions and the exponential function has no zeros, these r functions $t^j e^{ct}$, $0 \le j \le r - 1$, form a basis for the space of solutions.

Returning to the differential equation (1), which is

$$p(D)f = 0$$

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

we see that the n functions $t^m e^{c_j t}$, $0 \le m \le r_j - 1$, $1 \le j \le k$, form a basis for the space of solutions to (1). In particular, the space of solutions is finite-dimensional and has dimension equal to the degree of the polynomial p.

Example 2: Prove that the matrix A

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

is nilpotent. Find its index of nilpotency.

Proof:

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

$$A^3 = \begin{bmatrix} 1 & 1 & 0 \\ -1 & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

So $A^3 = 0$. Hence A is nilpotent of the index of nilpotence 3. Notice that $A^2 \neq 0$. (matrix)

Also the characteristic polynomial of A is $p(x) = x^3$.

Self Assessment

1. If V is the space of all polynomials of degree less than or equal to n over a field F, prove that the differentiation operator on V is nilpotent. Show that its characteristic polynomial is x^n.

Notes

2. If N is a nilpotent operator on an n-dimensional vector space V, show that the characteristic polynomial for N is x^n.

18.3 Summary

- The primary decomposition theorem is based on the fact that the minimal polynomial of the linear operator is the product of the irreducible.
- This helps in finding the projection operates which are polynomials in T.
- The direct decomposition of the vector space V in terms of the invariant subspaces helps in inducing linear operators T_i on these subspaces W_i.
- The induced operator T_i on W_i by T has the minimal polynomial as well as due to the factorisation of the minimal polynomial of T.

18.4 Keywords

Invariant Sub-spaces: If a vector α in V is such that α and $T\alpha$ are in the subspace W of V then W is invariant subspace of V over the field F.

Nilpotent Transformation: A nilpotent transformation N on the vector space V represented by a matrix A is such that $A^K = 0$ for some integer K and $A^{K-1} \neq 0$. Here K is the index of nilpotency.

Projection Operators: The projection operator E_i acting on the vector α_i gives $E\alpha_i = \alpha_i$ for the subspace W_i and gives zero for other. Also $E_i^2 = E_i$ and $E_iE_j = 0$ for $i \neq j$

18.5 Review Questions

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

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

in the standard ordered basis. Show that $T = D + N$ where D is a diagonalizable operator and N a nilpotent vector.

2. Show that the linear operator T on R^3 represented by the matrix

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

is nilpotent.

18.6 Further Readings

Books

Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I.N. Herstein, *Topics in Algebra*

Notes

Unit 19: Cyclic Subspaces and Annihilators

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand clearly the meaning of cyclic vector, cyclic-vector subspace and T-annihilator of α.
- See that in the case of a nilpotent linear operator one finds out the basis of the vectors α, $T\alpha$, $T^2\alpha$,... as the basis that spans the space of the linear transformation T.
- Know that closely related to the idea of cyclic vector α one understands the T-annihilator of α i.e., finds a polynomial g in F such that $g(T)\alpha = 0$
- See that with the help of these ideas one can understand the rational forms as well as the Jordan forms.

Introduction

The cyclic subspaces, the cyclic vector α and the T annihilators of α help us in the factoring of a linear operator T on the finite dimensional space to give a simple and elementary form.

In this unit the nilpotent transformation helps us in finding the basis vectors α, $T\alpha$, $T^2\alpha$,... that spans the space and this will help us in introducing the rational and the Jordan forms.

19.1 Cyclic Subspaces

We are considering an arbitrary but fixed linear operator on V, a finite-dimension vector space over the field F. If α is any vector in V, there is a smallest subspace of V which is invariant under T and contains α. This subspace can be defined as the intersection of all, T-invariant subspaces which contains α, if W is any subspace of V which is invariant under T and contains α, then W must also contain the vector $T\alpha$; hence W must contain $T^2\alpha$, $T^3\alpha$, etc. In other words, W must contain $g(T)\alpha$ for every polynomial g over F. The set of all vectors of the form $g(T)\alpha$, with g in $F(x)$, is clearly invariant under T, and is thus the smallest T-invariant subspace which contains α.

Notes

T-cyclic Subspace

If α is any vector in V, the T-cyclic subspace generated by α is the subspace $Z(\alpha; T)$ of all vectors of the form $g(T)\alpha$, g in $F[x]$. If $Z(\alpha; T) = V$, then α is called a cyclic vector for T.

In other words, the subspace $Z(\alpha; T)$ is the subspace spanned by the vectors $T^K\alpha$, $K \geq 0$ and thus α is a cyclic vector for T if and only if these vectors span V.

Example 1: For any T, the T-cyclic subspace generated by the zero vector is the zero space.

If the vector α is a characteristic vector for T the space $Z(\alpha; T)$ is one dimensional.

For the identity operator, every non-zero vector generates a one dimension cyclic subspace, thus, if dim $V > 1$, the identity operator has no cyclic vector.

Example 2: Consider the linear operator T on F^2 which is represented in the standard basis by the matrix

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

Here the cyclic vector is $\in_1 = (1, 0)$; for

$$A\in_1 = \in_2$$

So that for any vector β given by

$$\beta(a, b)$$

We have $\beta(a, b) = a\in_1 + b\in_2$,

so $= a\in_1 + bA\in_1$

$= (a + bA)\in_1$

Thus the polynomial g in $F^2(x)$ can be taken as

$$g = a + bx$$

For the same operator T, the cyclic subspace generated by $\in_2 = (0, 1)$ is the one dimensional space spanned by $\in_2$, because $\in_2$ is a characteristic vector of T.

Example 3: Consider the linear operator T on F^3, which is represented by A;

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

Here $A^3 = 0$, but $A^2 \neq 0$. So if α is a vector such that $A^2\nu \neq 0$ i.e., $\nu = \in_1 = (1,0,0)$, then the basic vectors will be $(\nu, T\nu, T^2\nu)$ and space generated by $\in_1$ is a cyclic subspace.

19.2 Annihilators

For any T and α, we shall be interested in linear relations

$$c_0\alpha + c_1T\alpha + ... + c_kT^k\alpha = 0$$

Notes

between the vectors $T^j\alpha$, that is, we shall be interested in the polynomials $g = c_0 + c_1x + ... + c_kx^k$ which have the property that $g(T)\alpha = 0$. The set of all g in $F[x]$ such that $g(T)\alpha = 0$ is clearly an ideal in $F[x]$. It is also a non-zero ideal, because it contains the minimal polynomial p of the operator $T(p)(T)\alpha = 0$ for every α in V).

Definition: If α is any vector in V, the T-annihilator of α is the ideal $M(\alpha; T)$ in $F[x]$ consisting of all polynomials g over F such that $g(T)\alpha = 0$. The unique monic polynomial p_α which generates this ideal will also be called the T-annihilator of α.

As we pointed out above, the T-annihilator p_α divides the minimal polynomial of the operator T. Please note that $\deg(p_\alpha) > 0$ unless α is the zero vector.

Theorem 1: Let α be any non-zero vector in V and let p_α be the T-annihilator of α.

(i) The degree of p_α is equal to the dimension of the cyclic subspace $Z(\alpha; T)$.

(ii) If the degree of p_α is k, then the vectors $\alpha, T\alpha, T^2\alpha, ..., T^{k-1}\alpha$ form a basis for $Z(\alpha; T)$.

(iii) If U is the linear operator on $Z(\alpha; T)$ induced by T, then the minimal polynomial for U is p_α.

Proof: Let g be any polynomial over the field F. Write

$$g = p_\alpha q + r$$

where either $r = 0$ or $\deg(r) < \deg(p_\alpha) = k$. The polynomial $p_\alpha q$ is in the T-annihilator of α, and so

$$g(T)\alpha = r(T)\alpha$$

Since $r = 0$ or $\deg(r) < k$, the vector $r(T)\alpha$ is a linear combination of the vectors $\alpha, T\alpha, ..., T^{k-1}\alpha$, and since $g(T)\alpha$ is a typical vector in $Z(\alpha; T)$, this shows that these k vectors span $Z(\alpha; T)$. These vectors are certainly linearly independent, because any non-trivial linear relation between them would give us a non-zero polynomial g such that $g(T)\alpha = 0$ and $\deg(g) < \deg(p_\alpha)$, which is absurd. This proves (i) and (ii).

Let U be the linear operator on $Z(\alpha; T)$ obtained by restricting T to that subspace. If g is any polynomial over F, then

$$\begin{aligned} p_\alpha(U)g(T)\alpha &= p_\alpha(U)g(T)\alpha \\ &= g(T)p_\alpha(U)\alpha \\ &= g(T)0 \\ &= 0 \end{aligned}$$

Thus the operator $p_\alpha(U)$ sends every vector in $Z(\alpha; T)$ into 0 and is the zero operator on $Z(\alpha, T)$. Furthermore, if h is a polynomial of degree less than k, we cannot have $h(U) = 0$, for then $h(U)\alpha = h(T)\alpha = 0$, contradicting the definition of p_α. This shows that p_α is the minimal polynomial for U.

A particular consequence of this theorem is the following: If α happens to be a cyclic vector for T, then the minimal polynomial for T must have degree equal to the dimension of the space V; hence, the Cayley-Hamilton theorem tells us that the minimal polynomial for T is the characteristic polynomial for T. We shall prove later that for any T there is a vector α in V which has the minimal polynomial of T for its annihilator. It will then follow that T has a cyclic vector if and only if the minimal and characteristic polynomials for T are identical. But it will take a little work for us to see this.

Our plan is to study the general T by using operators which have a cyclic vector. So, let us take a look at a linear operator U on a space W of dimension k which has a cyclic vector α. By Theorem 1, the vectors $\alpha, ..., U^{k-1}\alpha$ form a basis for the space W, and the annihilator p_α of α is the minimal

Notes

polynomial for U (and hence also the characteristic polynomial for U). If we let $\alpha_i = U^{i-1}\alpha$, $i = 1,..., k$, then the action of U on the ordered basis $\mathcal{B} = \{\alpha_1,..., \alpha_k\}$ is

$$\left.\begin{aligned} U\alpha_i &= \alpha_{i+1}, \qquad i = 1,...,k-1 \\ U\alpha_k &= -c_0\alpha_1 - c_1\alpha_2 - ... - c_{k-1}\alpha_k \end{aligned}\right\} \quad ... (1)$$

where $p_\alpha = c_0 + c_1x + \cdots + c_{k-1}x^{k-1} + x^k$. The expression for $U\alpha_k$ follows from the fact that $p_\alpha(U)\alpha = 0$, i.e.,

$$U^k\alpha + c_{k-1}U^{k-1}\alpha + \cdots + c_1U\alpha + c_0\alpha = 0$$

This says that the matrix of U in the ordered basis $\mathcal{B}$ is

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & 0 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -c_{k-1} \end{bmatrix}$$

The matrix (2) is called the companion matrix of the monic polynomial p_α.

Theorem 2: If U is a linear operator on the finite-dimensional space W, then U has a cyclic vector if and only if there is some ordered basis for W in which U is represented by the companion matrix of the minimal polynomial for U.

Proof: We have just observed that if U has a cyclic vector, then there is such an ordered basis for W. Conversely, if we have some ordered basis $\{\alpha_1,..., \alpha_k\}$ for W in which U is represented by the companion matrix of its minimal polynomial, it is obvious that α_1 is a cyclic vector for U.

Corollary: If A is the companion matrix of a monic polynomial p, then p is both the minimal and the characteristic polynomial of A.

Proof: One way to see this is to let U be the linear operator on F^k which is represented by A in the standard ordered basis, and to apply Theorem 1 together with the Cayley-Hamilton theorem. Another method is to use Theorem 1 to see that p is the minimal polynomial for A and to verify by a direct calculation that p is the characteristic polynomial for A.

One last comment—if T is any linear operator on the space V and α is any vector in V, then the operator U which T induces on the cyclic subspace $Z(\alpha; T)$ has a cyclic vector, namely, α. Thus $Z(\alpha; T)$ has an ordered basis in which U is represented by the companion matrix of p_α, the T-annihilator of α.

Self Assessment

1. Consider the linear operator T represented by the matrix

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

   Show that A is nilpotent. Find the basis vectors that will span the space of the linear operator T.

2. Let T be a linear operator on the finite dimensional vector space V. Suppose T has a cyclic vector. Prove that if U is any linear operator which commutes with T, then U is a polynomial in T.

Notes

19.3 Summary

- Know what is a cyclic vector, cyclic subspaces of a linear operator T acting on a finite dimension vector space.
- See that if the cyclic vector is found then the basis vectors of the sub-space of the linear transformation can be found that span the space of the linear operator.
- Understand how to find the T-annihilator of a vector and also find out that the monic polynomial which generates it has a degree equal to the dimension of the cyclic subspace.

19.4 Keywords

A Cyclic Vector: If the T-cyclic subspace generated by the vector α spans the whole finite dimensional space V then α is called a cyclic vector for the linear T.

Cyclic Subspace: If α is a vector in a finite dimensional space V of a linear operator T, then the invariant subspace W which contains all $g(T)\alpha$ for every polynomial g over F is called T-cyclic subspace generated by α.

T-annihilator of a Vector: α consisting of all polynomials g over F such that $g(T)\alpha = 0$ is called T-annihilator of α. The unique monic polynomial which generates this set will also be called the T-annihilator of α.

19.5 Review Questions

1. Let T be a linear operator on the finite dimensional space V_n. Suppose that T is diagonalizable. If T has a cyclic vector, then show that T has n-distinct characteristic values.
2. If S and T are nilpotent linear transformation which commute, prove that ST and $S + T$ are nilpotent linear transformations.

19.6 Further Readings

Books

Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I.N. Herstein, *Topics in Algebra*

Michael Artin, *Algebra*

Unit 20: Cyclic Decomposition and the Rational Form

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand that if T is any linear operator on a finite dimensional space V, then there exists vectors $\alpha_1, \alpha_2, \ldots \alpha_n$ in V such that the space V is a direct sum of the T-cyclic subspaces $Z(\alpha_i; T)$ for $i = 1, 2, \ldots n$.
- See that if W is any subspace of V, then there exists a subspace W', called *complementary* to W, such that $V = W \oplus W'$.
- Know that if W is T-invariant and W' complementary to W is also T-invariant then W is also T-admissible.
- Understand that the Cyclic decomposition theorem says that there exist non-zero vectors $\alpha_1, \alpha_2, \ldots \alpha_n$ in V with respective T-annihilators $p_1, p_2, \ldots p_r$ such that, V is a direct sum of T-invariant subspaces along with a proper T-admissible subspace W.

Introduction

In this unit certain concepts like invariant cyclic subspaces, complimentary subspaces and T-admissible proper subspaces are introduced.

The Cyclic decomposition theorem helps us in decomposing the n-dimensional vector space as a direct sum of T-invariant cyclic subspaces.

The matrix analogue of the Cyclic Decomposition theorem is that for the cyclic ordered basis $(\alpha, T\alpha, T^2\alpha, \ldots T^{k-1}\alpha)$ the matrix of induced operator T_i is the companion matrix Ai if the polynomial p_i, the matrix

$$A = \begin{bmatrix} A_1 & 0 & \ldots & 0 \\ 0 & A_2 & \ldots & 0 \\ \vdots & \vdots & \ldots & 0 \\ 0 & 0 & \ldots & A_n \end{bmatrix}$$

having a *rational form*.

Notes

20.1 Overview

In this unit we are interested in dealing with a linear operator T on a finite-dimensional space V, and dealing with the cyclic subspaces $Z(\alpha_1; T)$ where the vectors $\alpha_1, \alpha_2, \ldots \alpha_r$ in V. In this case the finite dimensional space V can be decomposed as the direct sum, i.e.,

$$V = Z(\alpha_1; T) \oplus \ldots. \oplus Z(\alpha_r; T)$$

This will also show that T is the direct sum of a finite number of linear operators each of which has a cyclic vector. The effect of this will be to reduce many questions about the general linear operator.

Let us consider T-invariant subspaces W and W' such that $V = W \oplus W'$. Here for any invariant subspace W, W' is complementary to W. We are interested in those W' which are also T-invariant.

T-admissible invariant subspace W

Let T be a linear operator on a vector space V and let W be a subspace of V. We say that W is *T-admissible* if W is invariant under T and if $f(T)\,\beta$ is in W where f is a polynomial, and there exists a vector γ in W such that

$$f(T)\,\beta = f(T)\,\gamma$$

our method for arriving at a decomposition

$$V = Z(\alpha_i; T) \oplus \ldots \oplus Z(\alpha_r; T)$$

will be to inductively select the vectors $\alpha_1, \alpha_2, \ldots \alpha_r$. Suppose that by some process or another we have selected $\alpha_1, \alpha_2, \ldots. \alpha_j$ and the sub-space

$$W_j = Z(\alpha_i; T) \oplus Z(\alpha_2; T) + \ldots + Z(\alpha_j; T)$$

is proper. We would like to find a non-zero vector α_{j+1} such that

$$W_j \cap Z(\alpha_{j+1}; T) = \{0\}.$$

Thus W will be a *proper T-invariant* subspace if there is a non-zero vector α such that

$$W \cap Z(\alpha\,; T) = \{0\} \qquad \ldots(1)$$

Thus the subspace $Z(\alpha; T)$ and W are independent if (1) is satisfied and the polynomial f is the T-annihilator of α i.e. $f(T)\,\alpha = 0$.

20.2 Cyclic Decomposition

With the above definition we arrive at the following theorem for the cyclic decomposition of the finite vector space.

Theorem 1 (Cyclic Decomposition Theorem). Let T be a linear operator on a finite-dimensional vector space V and let W_0 be a proper T-admissible subspace of V. There exist non-zero vectors $\alpha_1, \ldots., \alpha_r$ in V with respective T- annihilators $p_1, \ldots., p_r$ such that

(i) $V = W_0 \oplus Z(\alpha_1; T) \oplus \ldots \oplus Z(\alpha_r; T)$;

(ii) p_k divides p_{k-1}, $k = 2, \ldots, r$.

Furthermore, the integer r and the annihilators $p_1, \ldots., p_r$ are uniquely determined by (i), (ii), and the fact that no α_k is 0.

Proof: The proof is rather long; hence, we shall divide it into four steps. For the first reading it may seem easier to take $W_0 = \{0\}$, although it does not produce any substantial simplification. Throughout the proof, we shall abbreviate $f(T)\,\beta$ to f^β.

Notes

Step 1: There exist non-zero vectors $\beta_1, ..., \beta_r$ in V such that

(a) $V = W_0 + Z(\beta_1; T) + ... + Z(\beta_r; T)$;

(b) if $1 \le k \le r$ and

$$W_k = W_0 + Z(\beta_1; T) + ... + Z(\beta_k; T)$$

then the conductor $p_k = s(\beta_k; W_{k-1})$ has maximum degree among all T-conductors into the subspace W_{k-1}, i.e., for every k

$$\deg p_k = \max_{\alpha \text{ in } V} \deg s(\alpha; W_{k-1})$$

This step depends only upon the fact that W_0 is an invariant subspace. If W is a proper T-invariant subspace, then

$$0 < \max_{\alpha} \deg s(\alpha; W) \le \dim V$$

and we can choose a vector β so that deg s (β; W) attains that maximum. The subspace $W + Z$ (β; T) is then T-invariant and has dimension larger than dim W. Apply this process to $W = W_0$ to obtain β_1. If $W_1 = W_0 + Z(\beta_1; T)$ is still proper, then apply the process to W_1 to obtain β_2. Continue is that manner. Since dim W_k > dim W_{k-1}, we must reach $W_r = V$ is not more than dim V steps.

Step 2: Let $\beta_1, ... \beta_r$ be non-zero vectors which satisfy conditions (a) and (b) of Step 1. Fix k, $1 \le k \le r$. Let β be any vector in V and let $f = s(\beta; W_{k-1})$. If

$$f\beta = \beta_0 + \sum_{1 \le i < k} g_i\beta_i, \qquad \beta_i \text{ in } W_i$$

then f divides each polynomial g_i and $\beta_0 = f\gamma_0$, where γ_0 is in W_0.

If $k = 1$, this is just the statement that W_0 is T-admissible. In order to prove the assertion for $k > 1$, apply the division algorithm:

$$g_i = fh_i + r_i, \qquad r_i = 0 \quad \text{or} \quad \deg r_i < \deg f. \qquad ...(2)$$

We wish to show that $r_i = 0$ for each i, Let

$$\gamma = \beta - \sum_{1}^{k-1} h_i\beta_i. \qquad ...(3)$$

Since $\gamma - \beta$ is in W_{k-1},

$$s(\gamma; W_{k-1}) = s(\beta; W_{k-1}) = f.$$

Furthermore

$$f\gamma = \beta_0 + \sum_{1}^{k-1} r_i\,\beta_i. \qquad ...(4)$$

Suppose that some r_i is different from 0. We shall deduce a contradiction. Let j be the largest index i for which $r_i \ne 0$. Then

$$f\gamma = \beta_0 + \sum_{1}^{j} r_i\,\beta_i, \qquad r_j \ne 0 \quad \text{and} \quad \deg r_j < \deg f. \qquad ...(5)$$

Let $p = s(\gamma; W_{j-1})$. Since W_{k-1} contains W_{j-1}, the conductor $f = s(\gamma; W_{k-1})$ must divide p:

$$p = fg.$$

Notes

Apply $g(T)$ to both sides of (5):

$$p\gamma = gf\gamma = gr_j\beta_j + g\beta_0 + \sum_{1 \le i < j} gr_i\,\beta_i \qquad ...(6)$$

By definition $p\gamma$ is i W_{j-1}, and the last two terms on the right side of (6) are in W_{j-1}. Therefore, $gr_j\beta_j$ is in W_{j-1}. Now we use condition (b) on Step 1:

$$\begin{aligned} \deg(gr_j) &\ge \deg s(\beta_j; W_{j-1}) \\ &= \deg p_j \\ &= \deg s(\gamma; W_{j-1}) \\ &= \deg p \\ &= \deg(fg). \end{aligned}$$

Thus deg $r_j \ge$ deg f, and that contradicts the choice of j. We now know that f divides each g_i and hence that $\beta_0 = f\gamma$. Since W_0 is T-admissible, $\beta_0 = f\gamma_0$ where γ_0 is in W_0. We remark in passing that Step 2 is a strengthened form of the assertion that each of the subspaces $W_1, W_2, ...W_r$ is T-admissible.

Step 3: There exist non-zero vectors $\alpha_1,....\alpha_r$ in V which satisfy conditions (i) and (ii) of Theorem 1.

Start with vectors $\beta_1,.....,\beta_r$ as in Step 1. Fix $k, 1 \le k \le r$. We apply Step 2 to the vector $\beta = \beta_k$ and the T-conductor $f = p_k$. We obtain

$$p_k\beta_k = p_k\gamma_0 + \sum_{1 \le i < k} p_k h_i \beta_i \qquad ...(7)$$

where γ_0 is in W_0 and $h_i,....,h_{k-1}$ are polynomials. Let

$$\alpha_k = \beta_k - \gamma_0 - \sum_{1 \le i < k} h_i \beta_i. \qquad ...(8)$$

Since $\beta_k - \alpha_k$ is in W_{k-1},

$$s(\alpha_k; W_{k-1}) = s(\beta_k; W_{k-1}) = p_k \qquad ...(9)$$

and since $p_k\alpha_k = 0$, we have

$$W_{k-1} \cap Z(\alpha_k; T) = \{0\}. \qquad ...(10)$$

Because each α_k satisfies (9) and (10), it follows that

$$W_k = W_0 \oplus Z(\alpha_1; T) \oplus ... \oplus Z(\alpha_k; T)$$

and that p_k is the T-annihilator of α_k. In other words, the vectors α_1, ..., α_r define the same sequence of subspaces W_1, W_2, ... as do the vectors β_1, ..., β_r and the T-conductors $p_k = s(\alpha_k, W_{k-1})$ have the same maximality properties (condition (b) of Step 1). The vectors α_1, ..., α_r have the additional property that the subspaces W_0, $Z(\alpha_1; T)$, $Z(\alpha_2; T)$, ... are independent. It is therefore easy to verify condition (ii) in Theorem 1. Since $p_i\alpha_i = 0$ for each i, we have the trivial relation

$$p_k\alpha_k = 0 + p_1\alpha_1 + ... + p_{k-1}\alpha_{k-1}.$$

Notes

Apply Step 2 with $\beta_1,....,\beta_k$ replaced by $\alpha_1,.....,\alpha_k$ and with $\beta = \alpha_k$.

Conclusion: p_k divides each p_i with $i < k$.

Step 4: The number r and the polynomials $p_1, \ldots, p_r$ are uniquely determined by the conditions of Theorem 1.

Suppose that in addition to the vectors $\alpha_1,....,\alpha_r$ in Theorem 1 we have non-zero vectors $\gamma_1,....,\gamma_r$ with respective T-annihilators $g_1,....,g_r$ such that

$$V = W_0 \oplus Z(\gamma_i; T) \oplus ... \oplus Z(\gamma_i; T) \qquad ...(11)$$

g_k divides g_{k-1}, $k = 2, ... , s$.

We shall show that $r = s$ and $p_i = g_i$ for each i.

It is very easy to see that $p_1 = g_1$. The polynomial g_1 is determined from (11) as the T-conductor of V into W_0. Let $S(V; W_0)$ be the collection of polynomials f such that $f\beta$ is in W_0 for each β in V, i.e., polynomials f such that the range of $f(T)$ is contained in W_0. Then $S(V; W_0)$ is a non-zero ideal in the polynomial algebra. The polynomial g_1 is the monic generator of that ideal, for this reason. Each β in V has the form

$$\beta = \beta_0 + f_1\gamma_1 + ... + f_s\gamma_s$$

and so

$$g_1\beta = g_1\beta_0 + \sum_1^s g_1 f_i \ \gamma_i.$$

Since each g_i divides g_1, we have $g_1\gamma_i = 0$ for all i and $g_1\beta = g_1\beta_0$ is in W_0. Thus g_1 is in $S(V; W_0)$. Since g_1 is the monic polynomial of least degree which sends γ_1 into W_0 we see that g_1 is the monic polynomial of least degree in the ideal $S(V; W_0)$. By the same argument, p_1 is the generator of that ideal, so $p_1 = g_1$.

If f is a polynomial and W is a subspace of V, we shall employ the shorthand fW for the set of all vectors $f\alpha$ with α in W. We have left to the exercises the proofs of the following three facts.

1. $f\,Z(\alpha; T) = Z(f\alpha; T)$.

2. If $V = V_1 \oplus ... \oplus V_k$, where each V_i is invariant under T, then $fV = fV_1 \oplus ... \oplus fV_k$.

3. If α and γ have the same T-annihilator, then $f\alpha$ and $f\gamma$ have the same T-annihilator and (therefore)

$$\dim Z(f\alpha; T) = \dim Z(f\gamma; T).$$

Now, we proceed by induction to show that $r = s$ and $p_i = g_i$ for $i = 2, ..., r$. The argument consists of counting dimensions in the right way. We shall give the proof that if $r \geq 2$ the $p_2 = g_2$, and from that the induction should be clear. Suppose that $r \geq 2$. Then

$$\dim W_0 + \dim Z(\alpha_1; T) < \dim V.$$

Since we know that $p_1 = g_1$, we know that $Z(\alpha_1; T)$ and $Z(\gamma_1; T)$ have the same dimension. Therefore,

$$\dim W_0 + \dim Z(\gamma_1; T) < \dim V.$$

Notes

which shows that $s \geq 2$. Now it makes sense to ask whether or not $p_2 = g_2$. From the two decompositions of V, we obtain two decompositions of the subspace p_2V:

$$\left.\begin{aligned} p_2V &= p_2W_0 \oplus Z(p_2\alpha_1;T) \\ p_2V &= p_2W_0 \oplus Z(p_2\gamma_1;T) \oplus ... \oplus Z(p_2\gamma_s;T). \end{aligned}\right\} \quad ...(12)$$

We have made use of facts (1) and (2) above and we have used the fact that $p_2\alpha_i = 0, i \geq 2$. Since we know that $p_1 = g_1$, fact (3) above tells us that $Z(p_2\alpha_1;T)$ and $Z(p_2\gamma_1;T)$ have the same dimension. Hence, it is apparent from (12) that

$$\dim Z(p_2\gamma_i;T) = 0, \qquad i \geq 2.$$

We conclude that $p_2\gamma_2 = 0$ and g_2 divides p_2. The argument can be reversed to show that p_2 divides g_2. Therefore $p_2 = g_2$.

Corollary: If T is a linear operator on a finite-dimensional vector space, then every T-admissible subspace has a complementary subspace which is also invariant under T.

Proof: Let W_0 be an admissible subspace of V. If $W_0 = V$, the complement we seek is {0}. If W_0 is proper, apply Theorem 1 and let

$$W_0' = Z(\alpha_1;T) \oplus ... \oplus Z(\alpha_r;T).$$

Then W_0' is invariant under T and $V = W_0 \oplus W_0'$.

Corollary: Let T be a linear operator on a finite-dimensional vector space V.

(a) There exists a vector α in V such that the T-annihilator of α is the minimal polynomial for T.

(b) T has a cyclic vector if and only if the characteristic and minimal polynomials for T are identical.

Proof: If $V = \{0\}$, the results are trivially true. If $V \neq \{0\}$, let

$$V = Z(\alpha_1;T) \oplus ... \oplus Z(\alpha_r;T) \quad ...(13)$$

where the T-annihilators $p_1, ..., p_r$ are such that p_{k+1} divides $p_k, 1 \leq k \leq r-1$. As we noted in the proof of Theorem 1, it follows easily that p_1 is the minimal polynomial for T, i.e., the T-conductor of V into {0}. We have proved (a).

We saw in unit 19 that, if T has a cyclic vector, the minimal polynomial for T coincides with the characteristic polynomial. The content of (b) is in the converse. Choose any α as in (a). If the degree of the minimal polynomial is dim V, then $V = Z(\alpha; T)$.

Theorem 2 (Generalized Cayley-Hamilton Theorem): Let T be a linear operator on a finite-dimensional vector space V. Let p and f be the minimal and characteristic polynomials for T, respectively.

1. p divides f.
2. p and f have the same prime factors, except for multiplication.
3. If

$$p = f_1^{T_1} .... f_1^{T_k} \quad ...(14)$$

is the prime factorization of p, then

$$f = f_1^{d_1} .... f_k^{d_k} \quad ...(15)$$

where d_i is the nullity of $f_i(T)^n$ divided by the degree of f_i.

Notes

Proof: We disregard the trivial case $V = \{0\}$. To prove (i) and (ii), consider a cyclic decomposition (13) of V obtained from Theorem 1. As we noted in the proof of the second corollary, $p_1 = p$. Let U_i be the restriction of T to $Z(\alpha_i; T)$. Then U_i has a cyclic vector and so p_i is both the minimal polynomial and the characteristic polynomial for U_i. Therefore, the characteristic polynomial f is the product $f = p_1 .... p_r$. That is evident from the block form (1) of unit 17 which the matrix of T assumes in a suitable basis. Clearly $p_1 = p$ divides f, and this proves (i). Obviously any prime divisor of p is a prime divisor of f. Conversely, a prime divisor of $f = p_1 .... p_r$ must divide one of the factors p_i, which in turn divides p_1.

Let (14) be the prime factorization of p. We employ the primary decomposition theorem (Theorem 1 of unit 18). It tells us that, if V_1 is the null space of $f_i(T)^{r_i}$, then

$$V = V_1 \oplus ... \oplus V_k \qquad ...(16)$$

and f_1^{ri} is the minimal polynomial of the operator T_i, obtained by restricting T to the (invariant) subspace V_i. Apply part (ii) of the present theorem to the operator T_i. Since its minimal polynomial is a power of the prime f_i, the characteristic polynomial for T_i has the form $f_i^{d_i}$, where $d_i \geq r_i$. Obviously

$$d_i = \frac{\dim V_i}{\deg f_i}$$

and (almost by definition) dim V_i = nullity $f_i(T)^{r_i}$. Since T is the direct sum of the operators T_1, ..., T_k, the characteristic polynomial f is the product

$$f = f_1^{d_1} ..... f_k^{d_k}.$$

Corollary: If T is a nilpotent linear operator on a vector space of dimension n, then the characteristic polynomial for T is x^n.

20.3 The Rational Form

Now let us look at the matrix analogue of the cyclic decomposition theorem. If we have the operator T and the direct-sum decomposition of Theorem 1, let β_i be the 'cyclic ordered basis'

$$\{\alpha_i, T\alpha_i, ..., T^{k_i-1}\alpha_i\}$$

for $Z(\alpha_i; T)$. Hence k_i denotes the dimension of $Z(\alpha_i; T)$, that is, the degree of the annihilator p_i. The matrix of the induced operator T_i in the ordered basis β_i is the companion matrix of the polynomial p_i. Thus, if we let $\mathcal{B}$ be the ordered basis for V which is the union of the β_i arranged in the order β_1, ..., β_r, then the matrix of T in the ordered basis β will be

$$A = \begin{bmatrix} A_1 & 0 & ... & 0 \\ 0 & A_2 & ... & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & ... & A_r \end{bmatrix} \qquad ...(17)$$

where A_i is the $k_i \times k_i$ companion matrix of p_i. An $n \times n$ matrix A, which is the direct sum (17) of companion matrices of non-scalar monic polynomials p_1,....., p_r such that p_{i+1} divides p_i for $i = 1$, ..., $r - 1$, will be said to be in **rational form**. The cyclic decomposition theorem tells us the following concerning matrices.

Theorem 3: Let F be a field and let B be an $n \times n$ matrix over F. The B is similar over the field F to one and only one matrix which is in rational form.

Notes

Proof: Let T be the linear operator on F^n which is represented by B in the standard ordered basis. As we have just observed, there is some ordered basis for F^n in which T is represented by a matrix A in rational form. Then B is similar to this matrix A. Suppose B is similar over F to another matrix C which is in rational form. This means simply that there is some ordered basis for F^n in which the operator T is represented by the matrix C. If C is the direct sum of companion matrices C_i of monic polynomials $g_1, ..., g_s$ such that g_{i+1} divides g_i for i = 1, ..., $s - 1$, then it is apparent that we shall have non-zero vectors $\beta_1, ..., \beta_s$ in V with T-annihilators $g_1, ..., g_s$ such that

$$V = Z(\beta_1; T) \oplus ... \oplus Z(\beta_s; T).$$

But then by the uniqueness statement in the cyclic decomposition theorem, the polynomials g_i, are identical with the polynomials p_i which define the matrix A. Thus $C = A$.

The polynomials $p_1, ..., p_r$ are called the **invariant factors** for the matrix B. We shall describe an algorithm for calculating the invariant factors of a given matrix B. The fact that it is possible to compute these polynomials by means of a finite number of rational operations on the entries of B is what gives the rational form its name.

Example 1: Suppose that V is a two-dimensional vector space over the field F and T is a linear operator on V. The possibilities for the cyclic subspace decomposition for T are very limited. For, if the minimal polynomial for T has degree 2, it is equal to the characteristic polynomial for T and T has a cyclic vector. Thus there is some ordered basis for V in which T is represented by the companion matrix of its characteristic polynomial. If, on the other hand, the minimal polynomial for T has degree 1, then T is a scalar multiple of the identity operator. If $T = cI$, then for any two linear independent vectors α_1 and α_2 in V we have

$$V = Z(\alpha_1; T) \oplus Z(\alpha_2; T)$$

$$p_1 = p_2 = x - c.$$

For matrices, this analysis says that every 2 × 2 matrix over the field F is similar over F to exactly one matrix of the types

$$\begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix}, \quad \begin{bmatrix} 0 & -c_0 \\ 1 & -c_1 \end{bmatrix}$$

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

$$A = \begin{bmatrix} 5 & -6 & -6 \\ -1 & 4 & 2 \\ 3 & -6 & -4 \end{bmatrix}$$

in the standard ordered basis. We have computed earlier that the characteristic polynomial for T is $f = (x-1)(x-2)^2$ and minimal polynomial for T is $p = (x-1)(x-2)$. Thus we know that in the cyclic decomposition for T the first vector α_1 will have p as its T-annihilator.

Since we are operating in a three-dimensional space, there can be only one further vector, α_2. It must generate a cyclic subspace of dimension I, i.e., it must be a characteristic vector for T. T-annihilator p_2 must be $(x - 2)$, because we must have $pp_2 = f$. Notice that this tells us immediately that the matrix A is similar to the matrix

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

Notes

that is, that T is represented by B in some ordered basis. How can we find suitable vectors α_1 and α_2? Well, we know that any vector which generates a T-cyclic subspace of dimension 2 is a suitable α_1. So let's just try ε_1. We have

$$T\varepsilon_1 = (5, -1, 3)$$

which is not a scalar multiple of ε_1; hence $Z(\varepsilon_1; T)$ has dimension 2. This space consists of all vectors $a\varepsilon_1 + b\,(T\varepsilon_1)$:

$$a(1,0,0) + b(5,-1,3) = (a+5b, -b, 3b)$$

or, all vectors (x_1, x_2, x_3) satisfying $x_3 = -3x_2$. Now what we want is a vector α_2 such that $T\alpha_2 = 2\alpha_2$ and $Z(\alpha_2; T)$ is disjoint from $Z(\varepsilon_1; T)$. Since α_2 is to be a characteristic vector for T, the space $Z(\alpha_2; T)$ will simply by the one-dimensional space spanned by α_2, and so what we require is that α_2 not be in $Z(\varepsilon_1; T)$. If $\alpha = (x_1, x_2, x_3)$, one can easily compute that $T\alpha = 2\alpha$ if and only if $x_1 = 2x_2 + 2x_3$. Thus $\alpha_2 = (2, 1, 0)$ satisfies $T\alpha_2 = 2\alpha_2$ and generates a T-cyclic subspace disjoint from $Z(\varepsilon_1; T)$. The reader should verify directly that the matrix of T is the ordered basis.

$$\{(1, 0, 0), (5, -1, 3), (2, 1, 0)\}$$

is the matrix B above.

Example 3: Suppose that T is a diagonalizable linear operator on V. It is interesting to relate a cyclic decomposition for T to a basis which diagonalizes the matrix of T. Let $c_1, \ldots c_k$ be the distinct characteristic values of T and let V_i be the space of characteristic vectors associated with the characteristic value c_i. Then

$$V = V_i \oplus \ldots \oplus V_k$$

and if $d_i = \dim V_i$ then

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

is the characteristic polynomial for T. If α is a vector in V, it is easy to relate the cyclic subspace $Z(\alpha; T)$ to the subspaces $V_1, \ldots, V_k$. There are unique vectors $\beta_1, \ldots, \beta_k$ such that β_i is in V_i and

$$\alpha = \beta_1 + \ldots + \beta_k.$$

Since $T\beta_1 = c_i \beta_i$, we have

$$f(T)\alpha = f(c_1)\beta_1 + \ldots + f(c_k)\beta_k \qquad \ldots(18)$$

for every polynomial f. Given any scalars $t_1, \ldots, t_k$ there exists a polynomial f such that $f(c_i) = t_i$, $1 \le i \le k$. Therefore $Z(\alpha; T)$ is just the subspace spanned by the vectors $\beta_1, \ldots, \beta_k$. What is the annihilator of α? According to (18), we have $f(T)\alpha = 0$ if and only if $f(c_i)\beta_i = 0$ for each i. In other words, $f(T)\alpha = 0$ provided $f(c_i) = 0$ for each i such that $\beta_i \neq 0$. Accordingly, the annihilator of α is the product

$$\prod_{\beta_i \neq 0} (x - c_i). \qquad \ldots(19)$$

Now, let $\beta_i = \{\beta_1^t, \ldots, \beta_{d_i}^t\}$ be an ordered basis for V_i. Let

$$r = \max_u d_i.$$

We define vectors $\alpha_1, \ldots, \alpha_r$ by

$$\alpha_j = \sum_{d_i \ge j} \beta_j^t, \qquad 1 \le j \le r. \qquad \ldots(20)$$

Notes

The cyclic subspace $Z(\alpha_j; T)$ is the subspace spanned by the vectors β_j^t, as i runs over those indices for which $d_i \geq j$. The T-annihilator of α_j is

$$p_j = \prod_{d_i \geq j} (x - c_i). \qquad ...(21)$$

We have

$$V = Z(\alpha_1; T) \oplus ... \oplus Z(\alpha_r; T)$$

because each β_j^t belongs to one and only one of the subspaces $Z(\alpha_1; T)$; ...., $Z(\alpha_r; T)$ and $\beta = (\beta_1, ..., \beta_k)$ is a basis for V. By (21) p_{j+1} divides p_j.

Self Assessment

1. Let T be the linear operator on R^3 which is represented in the standard ordered basis by

$$\begin{bmatrix} 1 & 3 & 3 \\ 3 & 1 & 3 \\ -3 & -3 & -5 \end{bmatrix}$$

   Find the characteristic polynomial for T. What is the minimal polynomial?

2. Show that if T is a diagonalizable linear operator then every T-invariant subspace has a complementary T-invariant subspace.

20.4 Summary

- In this unit the theorem 1 (derived) helps us in finding non-zero vectors $\alpha_1, ..., \alpha_r$ in V with respect to T-annihilators $p_1, p_2, ...p_r$ such that the vector space is a direct sum of T-invariant subspaces along with a proper T-admissible subspace W_0.
- Certain concepts like complementary subspace T-admissible subspace, proper T-invariant subspaces are explained.
- If T is a nilpotent linear operator on a vector space of dimension n, then the characteristic polynomial for T is x^n.
- It is shown that if there is direct sum decomposition theorem 1 the cyclic ordered basis $(\alpha_i, Td_i, ...T^{k-1}\alpha_i)$ for $Z(\alpha_i; T)$ then with the help of companion matrices, A representing T can be put in Jordan Form.

20.5 Keywords

Complementary Subspace: T-invariant subspace W has the property that there exists a subspace W', such that $V = W \oplus W'$, where W' is called a complementary subspace of W. W' can also be T-invariant.

Rational Form: An $n \times n$ matrix A

$$A = \begin{bmatrix} A_1 & 0 & 0 & ... & 0 \\ 0 & A_2 & 0 & ... & 0 \\ 0 & 0 & ... & & 0 \\ \vdots & \vdots & & & 0 \\ 0 & 0 & ... & & A_n \end{bmatrix}$$

which is direct sum of companion matrices A_i has a rational form.

Notes

T-admissible Subspace: An invariant subspace W with another T-invariant subspace W', such that

$$V = W \oplus W$$

is called T-admissible subspace.

20.6 Review Questions

1. Let T be the linear operator on R^3 which is represented in the standard ordered basis by

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

Find non-zero α_1, α_2, α_3 satisfying the conditions of theorem 1.

2. Find the minimal polynomial and the rational forms of the following real matrices

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

Answer: Self Assessment

1. The characteristic polynomial is

$$f = (x-1)(x+2)^2$$

The minimal polynomial is

$$p = (x-1)(x+2)$$

20.7 Further Readings

Books

Kenneth Hoffman and Ray Kunze, *Linear Algebra*

Michael Artin, *Algebra*

Notes

Unit 21: The Jordan Form

CONTENTS

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 $k_1 \geq k_2 \geq ... \geq k_r$. The minimal polynomial also has the form

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

- 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.

21.1 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 $p_1, p_2, ..., p_r$ for r non-zero vectors $\alpha_1, \alpha_2,...,\alpha_r$, V is decomposed as follows:

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

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

$$K_1 = K_1 \geq K_2 \geq ... K_r$$

Notes

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

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

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

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

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.

21.2 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

Notes

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

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

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

of matrices $A_1,..., A_k$. 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 $c_1,..., c_k$) 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

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

This shows that $c_1, ..., c_k$ and $d_1, ..., d_k$ 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 $V = W_1 \oplus ... \oplus W_k$ 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 $(T_i ... c_iI)$.

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 $J_1^{(i)}$ 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 $v_1 = v, v_2 = T\,v, v_3 = T^2v, \ldots v_{n_1} = T^{n_1-1}v$ vectors which are claimed to be linearly independent over the field F.

Let V_1 be the subspace of V spanned by $v_1 = v, v_2 = Tv, \ldots v_{n_1} = T^{n_1-1}v$, 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

Notes

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

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

Notes

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

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 $a_0,..., a_{n-1}$ 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

$$\frac{d^nf}{dx^n}+a_{n-1}\frac{d^{n-1}f}{dx^{n-1}}+\cdots+a_1\frac{df}{dx}+a_0f=0$$

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

$$p = x^n + \cdots + a_1x + a_0$$

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

Let $c_1,..., c_k$ 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 $(D - c_iI)^{r_i}$, that is, the set of solutions to the differential equation

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

Then the primary decomposition theorem tells us that

$$V = V_1 \oplus ... \oplus V_k$$

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

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

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

Notes

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

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

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.

21.3 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 $k \leq n$, 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.

21.4 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 $a^{k-1} \neq 0$.

21.5 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 $A = c_1d_1 + c_2d_2 + ... + c_kd_k$

21.6 Further Readings

Books

Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I.N. Herstein, *Topics in Algebra*

Notes

Unit 22: Computation of Invariant Factors

CONTENTS

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.

22.1 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.

Notes

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

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

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

22.2 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 $F^{m \times n}(x)$, 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.

Notes

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

$$I(M_1) = \min_{f_i \neq 0} \deg f_i$$

$$p(M_1) = \text{g.c.d. } (f_1, \ldots f_m) \qquad \ldots(2)$$

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 $\deg f_i = I(M_1)$. Attempt to divide each f_i by f_j:

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

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

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

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

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

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 $r_i \neq 0$ 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 $f_1, \ldots, f_m$.

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

Notes

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

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

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 $x I - A$ 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 $xI - A$, 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 $xI - A$ 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

Notes

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}, $1 \leq k \leq l - 1$.

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:

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

Notes

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) $$\begin{aligned} D_{I', J}(e(M)) &= D_J(\alpha_{i1}, \ldots, c\alpha_r, \ldots, \alpha_{ik}) \\ &= cD_J(\alpha_{i1}, \ldots, \alpha_r, \ldots, \alpha_{ik}) \\ &= cD_{I, J}(M); \end{aligned}$$

(b) $$\begin{aligned} D_{I, J}(e(M)) &= D_J(\alpha_{i1}, \ldots, \alpha_r + g\alpha_s, \ldots, \alpha_{ik}) \\ &= D_{I, J}(M) + gD_J(\alpha_{i1}, \ldots, \alpha_s, \ldots, \alpha_{ik}) \end{aligned}$$

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

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

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

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.

Notes

22.3 Summary

- 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.

22.4 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.

22.5 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.

Notes

Answer: Self Assessment

1. True

22.6 Further Readings

Books Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I.N. Herstein, *Topics in Algebra*

Unit 23: Semi-simple Operators

Notes

CONTENTS

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 $SN = NS$.

23.1 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.

Notes

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.

23.2 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.

Notes

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 $p = p_1 \ldots p_k$, where $p_1, \ldots, p_k$ 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 $p = p_1 \ldots p_k$, where $p_1, \ldots, p_k$ 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 $V = W_1 \oplus \ldots \oplus W_k$ 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

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

By the first lemma above, $W = (W \cap W_1) \oplus \ldots \oplus (W \cap W_k)$ so that if $W' = V_1 \oplus \ldots \oplus V_k$, 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 $p = (x - c_1) \ldots (x - c_k)$, where $c_1, \ldots, c_k$ 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 $\deg f \leq n$, then

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

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

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

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

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

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 $k \leq n$, the formula says

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

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

$$f' = P_1'f_1 + P_2'f_2 + ... + P_k'f_k$$

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 $j \neq i$, 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' 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 $SN = NS$.

23.3 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 $V = W \oplus W'$.

Notes

- 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 $T = S + N$, $SN = NS$.

23.4 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.

23.5 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.

23.6 Further Readings

Books Kenneth Hoffman and Ray Kunze, *Linear Algebra*

Michael Artin, *Algebra*

Notes

Unit 24: Inner Product and Inner Product Spaces

CONTENTS

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

$$(\alpha / c\beta + \gamma) = \overline{c}\,(\alpha \mid \beta) + (\alpha \mid \gamma)$$

- Know the importance of the construction known as Gram–Schmidt orthogonalization process to convert a set of independent vector $(\beta_1, \beta_2, \ldots \beta_n)$ into an orthogonal set of vectors $(\alpha_1, \alpha_2, \ldots \alpha_n)$.
- 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 $(\alpha_1, \alpha_2, \ldots \alpha_n)$ from a set of independent vectors $(\beta_1, \beta_2, \ldots \beta_n)$ 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 $V = W \oplus W^{\perp}$.

24.1 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

Notes

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 $\beta = (y_1\ y_2 \ldots y_n)$, $(\alpha \mid \beta) = x, \overline{y}_1 + x_2\ \overline{y}_2 + \ldots + x_n \overline{y}_n$ 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

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

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

Notes

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,

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

be an ordered basis for V. Let $\varepsilon_1, ..., \varepsilon_n$ be the standard basis vectors in F^n, and let T be the linear transformation from V into F^n such that $T\alpha_j = \varepsilon_j$, $j = 1, ..., n$. 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, $(Tf)(t) = tf(t)$, $0 \le t \le 1$. It is easy to see that T is linear. Also T is non-singular; for suppose $Tf = 0$. Then $tf(t) = 0$ for $0 \le t \le 1$; 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

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

$$= \int_0^1 f(t)\overline{g(t)}t^2 dt.$$

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

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

Notes

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

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

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

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

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

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

it assumes on pairs of vectors in $\mathfrak{B}$. 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

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

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

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

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

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

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

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

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

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

(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

Notes

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

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

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

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

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

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

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

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

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 $|(\alpha \mid \beta| < \|\alpha\|\|\beta\|$ unless

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

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

(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 $(\alpha \mid \beta) = 0$; 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

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

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

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

Suppose $f_n(x) = \sqrt{2}\cos 2\pi nx$ and that $g_n(x) = \sqrt{2}\sin 2\pi nx$. Then $\{1, f_1, g_1, f_2, g_2, \ldots\}$ 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

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

Notes

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

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

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

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

$$= 0.$$

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

$$\alpha_1 = \beta_1$$

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

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

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

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

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

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

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

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

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

Notes

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

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

in R^3 equipped with the standard inner product. Applying the Gram-Schmidt process to $\beta_1, \beta_2, \beta_3$, we obtain the following vectors.

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

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

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

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

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

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

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 $\alpha_1, \alpha_2, \alpha_3$, 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

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

Finally, note that from $\alpha_1, \alpha_2, \alpha_3$ we get the orthonormal basis

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

Notes

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

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

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

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

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

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

and

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

Thus

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

and normalized α_3 is given by

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

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

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

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

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

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

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

$$> \|\beta - \alpha\|^2.$$

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

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

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

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

Notes

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

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

Then the inequality reduces to the statement

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

This holds if and only if $(\beta - \alpha \mid \alpha - \gamma) = 0$. 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,

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

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

Notes

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

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

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

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

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

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

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

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

Notes

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

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

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

24.3 Summary

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

Notes

- 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.

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

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

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

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.

Notes

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

24.6 Further Readings

Books

Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I N. Herstein, *Topics in Algebra*

Notes

Unit 25: Linear Functional and Adjoints of Inner Product Space

CONTENTS

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 $[T^*]_\beta = [T]_\beta$.

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 $T^*T = TT^*$.

25.1 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

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

Notes

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

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

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 $\overline{y}_i = c_j$ 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

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

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

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

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 $(f \mid g) = L(f)$ 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 $L(f) = (f \mid g)$, 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.

25.2 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

Notes

$\beta \to \beta'$:

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

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,

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

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

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

Notes

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

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

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.

$$(E\alpha|\beta) = (E\alpha|E\beta + (1 - E)\beta)$$

$$= (E\alpha|E\beta)$$

$$= (E\alpha + (1 - E)\alpha|E\beta)$$

$$= (\alpha|E\beta)$$

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

$$\alpha_1 = (154, 0, 0)$$

$$\alpha_2 = (145, -36, 3)$$

$$\alpha_3 = (-36, 10, 12)$$

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

$$E\alpha_1 = (9, 36, -3)$$

$$E\alpha_2 = (0, 0, 0)$$

$$E\alpha_3 = (0, 0, 0)$$

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.

Notes

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

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

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 $\overline{f}$. For

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

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

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.

25.3 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.

25.4 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

Notes

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

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.

25.5 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.

25.6 Further Readings

Books

Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I N. Herstein, *Topics in Algebra*

Michael Artin, *Algebra*

Notes

Unit 26: Unitary Operators and Normal Operators

CONTENTS

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.

26.1 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

Notes

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) $\rightarrow$ (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) $\rightarrow$ (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) $\rightarrow$ (iv) This requires no comment.

(iv) $\rightarrow$ (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 $(X \mid Y) = Y^*X$ 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 $(A \mid B) = \frac{1}{2}\,\mathrm{tr}\,(AB^t)$, 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 $(\alpha \mid \beta) = (T\alpha \mid T\beta)$ 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 $[X \mid Y] = Y^*GX$.

Let W be the same vector space, with the standard inner product $(X \mid Y) = Y^*X$. 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

$$(TX \mid TY) = (PX \mid PY)$$

Notes

$$= (PY)^*(PX)$$

$$= Y^*P^*PX$$

$$= Y^*GX$$

$$= [X \mid Y].$$

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 $\overline{c}c = 1$. The latter condition means (of course) that $|c| = 1$, or $c = e^{i\theta}$, where θ is real.

(b) Let

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Notes

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

$$\begin{bmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{bmatrix} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

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

$$A = \begin{bmatrix} a & b \\ -e^{i\theta}\overline{b} & e^{i\theta}\overline{a} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}\begin{bmatrix} a & b \\ -\overline{b} & \overline{a} \end{bmatrix}$$

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

$$M_{k_j} = \begin{cases} -\frac{1}{\|\alpha_k\|} \cdot C_{k_j}, & \text{if } j < k \\ \frac{1}{\|\alpha_k\|}, & \text{if } j = k \\ 0, & \text{if } j > k \end{cases}$$

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

$$\alpha_1 = (x_1, x_2, 0)$$

$$\alpha_2 = (0, 1, 0) - x_2 (x_1, x_2, 0)$$

$$= x_1 (-x_2, x_1, 0)$$

$$\alpha_3 = (0, 0, 1).$$

Let U be the matrix with rows α_1, (α_2/x_1), α_3. Then U is unitary, and

$$U = \begin{bmatrix} x_1 & x_2 & 0 \\ -x_2 & x_1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ -\frac{x_2}{x_1} & \frac{1}{x_1} & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 & x_2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Now multiplying by the inverse of

$$M = \begin{bmatrix} 1 & 0 & 0 \\ -\frac{x_2}{x_1} & \frac{1}{x_1} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

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

$$[\alpha]_{\beta'} = P^{-1}[\alpha]_{\beta}$$

Notes

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

$$[T]_{\beta'} = P^{-1}[T]_{\beta}P = P^*[T]_{\beta}P.$$

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 $[T]_{\beta'}$ is unitarily equivalent to the matrix $[T]_{\beta}$. 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.

26.2 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

$$TT^* = T^*T. \qquad \ldots (2)$$

Notes

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

$$\begin{aligned} c(\alpha \mid \alpha) &= (c\alpha \mid \alpha) \\ &= (T\alpha \mid \alpha) \\ &= (\alpha \mid T\alpha) \\ &= (\alpha \mid c\alpha) \\ &= \bar{c}(\alpha \mid \alpha) \end{aligned}$$

Since $(\alpha \mid \alpha) \neq 0$, we must have $c = \bar{c}$. Suppose we also have $T\beta = d\beta$ with $\beta \neq 0$. Then

$$\begin{aligned} c(\alpha \mid \beta) &= (T\alpha \mid \beta) \\ &= (\alpha \mid T\beta) \\ &= (\alpha \mid d\beta) \\ &= \bar{d}(\alpha \mid \beta) \\ &= d(\alpha \mid \beta) \end{aligned}$$

If $c \neq d$, then $(\alpha \mid \beta) = 0$.

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 $(X \mid Y) = Y^*X$. 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 $T\alpha = c\alpha$.

Notes

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 $t \neq c$. 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 $(\alpha \mid (T^*\beta) = 0$ for every α in W. If α is in W, then $T\alpha$ is in W, so $(T\alpha \mid \beta) = 0$. But $(T\alpha \mid \beta) = (\alpha \mid T^*\beta)$.

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

Notes

be an ordered orthonormal basis for V, such that $T\alpha_j = c_j \alpha_j$, $j = 1, \ldots, n$. If $D = [T]_{\mathcal{B}}$, 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

$$\| U\alpha \|^2 = (U\alpha \mid U\alpha) = (\alpha \mid U^*U\alpha)$$

$$= (\alpha \mid UU^*\alpha) = (U^*\alpha \mid U^*\alpha) = \| U^*\alpha \|^2.$$

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 $(T - cI)\alpha = 0$ 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,

$$T^*\alpha_1 = \sum_j (A^*)_{j1}\alpha_j$$

$$= \sum_j \bar{A}_{1j}\alpha_j$$

Notes

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 $T = T_1 + iT_2$, where T_1 and T_2 are self-adjoint operators which commute.

26.3 Summary

- In this unit we have studied unitary operators and normal operators.

Notes

- 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.

26.4 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.

26.5 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.

26.6 Further Readings

Books

Michael Artin *Algebra*

I N. Herstein *Topics in Algebra*

Kenneth Hoffman and Ray Kunze *Linear Algebra*

Notes

Unit 27: Introduction and Forms on Inner Product Spaces

CONTENTS

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 $f \to T$ 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.

27.1 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.

27.2 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

$$f(\alpha, \beta) = (T_f\alpha \mid \beta)$$

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

$$f\left(\sum_s x_s\alpha_s \sum_r y_r\alpha_r\right) = \sum_{r,s} \overline{y}_r A_{rs} x_s \qquad ...(1)$$

for all scalars x, and y $(1 \le r, s \le n)$. 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.

Notes

The matrix of f in another basis

$$\alpha'_j = \sum_{i=1}^{n} P_{ij}\alpha_i , \quad (1 \le j \le n)$$

is given by the equation

$$A' = P^*AP. \tag{2}$$

For

$$\begin{aligned} A'_{jk} &= f(\alpha'_k, \alpha'_j) \\ &= f\left(\sum_s P_{sk}\alpha_s, \sum_r P_{rj}\alpha_r\right) \\ &= \sum_{r,s} \overline{P_{rj}} A_{rs} P_{sk} \\ &= (P^*AP)_{jk}. \end{aligned}$$

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

$$\begin{aligned} f(\alpha, \beta) + f(\beta, \alpha) &= \overline{f(\alpha, \beta)} + \overline{f(\beta, \alpha)} \\ -if(\alpha, \beta) + if(\beta, \alpha) &= \overline{if(\alpha, \beta)} - \overline{if(\beta, \alpha)} \end{aligned}$$

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 $(T\alpha \mid \alpha)$ 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 $f(\alpha, \beta) = (T\alpha \mid \beta)$ for all α and β in V. Then, since $f(\alpha, \beta) = \overline{f(\beta, \alpha)}$ and $(\overline{T\beta \mid \alpha}) = (\alpha \mid T\beta)$, it follows that

$$(T\alpha \mid \beta) = \overline{f(\beta, \alpha)} = (\alpha \mid T\beta)$$

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

$$f(\alpha_k, \alpha_j) = (T\alpha_k \mid \alpha_j) = \delta_{kj}c_k$$

and by Theorem 2 of unit 24 each c_k is real.

Corollary: Under the above conditions

$$f(\sum_j x_j\alpha_j, \sum_k y_k\alpha_k) = \sum_j c_j x_j \overline{y}_j$$

Self Assessment

1. Which of the following functions f, defined on vectors $\alpha = (x_1, x_2)$ and $\beta\ (y_1, y_2)$ = 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.

27.3 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}.

27.4 Keywords

Notes

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 $(T\alpha \mid \alpha)$ is real for every α in V.

27.5 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)

27.6 Further Readings

Books Kenneth Hoffman and Ray Kunze, *Linear Algebra*

Michael Artin, *Algebra*

Notes

Unit 28: Positive Forms and More on Forms

CONTENTS

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 $P_{kk} = 1 (1 \leq k \leq n)$ 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 $P_{kk} = 1$ $(1 \leq k \leq n)$ such that $B = AP$ is lower triangular.

28.1 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 $f(\alpha, \alpha) \geq 0$ for every α in v. The form f is positive if it is Hermitian and $f(\alpha, \alpha) > 0$ for all $\alpha \neq 0$.

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

$$= (\sum_j \sum_k x_j \bar{x}_k f(\alpha_j, \alpha_k)$$

$$= (\sum_j \sum_k A_{kj} x_j \bar{x}_k) \quad ...(1)$$

So we see that f is non-negative if and only if

and

$$A = A^*$$

$$\sum_j \sum_k A_{kj} x_j \bar{x}_k \geq 0 \text{ for all scalars } x_1, x_2, \ldots x_n \quad ..(2)$$

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

$$g(X, Y) = Y^*AX \quad ...(3)$$

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

$$g(X, Y) = Y^*AX \quad ...(4)$$

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

$$g(X, X) = X^*P^*PX$$
$$= (PX)^*PX$$
$$\geq 0.$$

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

$$\delta_{jk} = g(Q_1, Q_k)$$
$$= Q^*_k A Q_j.$$

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

Notes

$$\Delta_k(A) = \det \begin{bmatrix} A_n & \cdots & A_{1k} \\ \vdots & & \vdots \\ A_{k1} & \cdots & A_{kk} \end{bmatrix}, 1 \le k \le n.$$

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

$$\sum_{r=1}^{k-1} A_{jr} P_{rk} = - A_{kk}, \qquad 1 \le j \le k-1$$

$$2 \le k \le n. \qquad ...(5)$$

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}, ..., $P_{k-1,\,k}$. 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 $\Delta_{k-1}(A) \neq 0$, 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,

$$\Delta_k(A) = \Delta_k(B)$$

$$= B_{11} B_{22} \ldots B_{kk}, \; k = 1, \ldots, n. \qquad ...(6)$$

To verify (6), let A_1, ..., A_n and B_1, ... B_n be the columns of A and B, respectively. Then

$$B_1 = A_1$$

$$B_r = \sum_{j=1}^{r-1} P_{jr} A_j + A_r, \quad r > 1. \qquad ...(7)$$

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

Notes

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

$$(X + iY)^*A(X + iY) = (X^t - iY^t)A(X + iY)$$
$$= X^tAX + Y^tAY + i[X^tAY - Y^tAX]$$

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 $A = P^tP$.

28.2 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

$$\begin{aligned} f(\alpha, \beta) &= \sum_{j,k}^{r} \overline{y}, M_{jk} x_k \\ &= \sum_{k} \left(\sum_{j} \overline{y}_j M_{jk} \right) x_k. \end{aligned}$$

It follows from this that $W \cap W' \neq \{0\}$ if and only if the homogeneous system

$$\sum_{j=1}^{r} \overline{y}_j M_{jk} = 0, 1 \leq k \leq r$$

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

$$A = (M^*)^{-1} = (M^{-1})^*$$

$$g_j(\beta) = \sum_{k=1}^{r} A_{jk} \overline{f(\alpha_k, \beta)}$$

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

$$E\beta = \sum_{j=1}^{r} g_j(\beta) \alpha_j$$

Notes

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.

Notes

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 $\alpha_1, \ldots, \alpha_k$ 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 $k = 1, \ldots, n$. 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 $(\beta_1, \ldots \beta_n)$. 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.

28.3 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 ($1 \le k \le n$) such that P^*AP is upper triangular.

28.4 Keywords

Non-negative Form: A form f on real or complex vector space V is non-negative if it is Hermitian and $f(\alpha, \alpha) \ge 0$.

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: $P_{kk} = 1$, $1 \le k \le n$ and $P_{ij} = 0$ for $j > k$.

28.5 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

$$A = P^tP.$$

2. Does

$$\left[(x_1, x_2) | (y_1, y_2)\right] = x_1\overline{y}_1 + 2x_2\overline{y}_1 + 2x_1\overline{y}_2 + x_2\overline{y}_2$$ define an inner product on c^2?

28.6 Further Readings

Books Kenneth Hoffman and Ray Kunze, *Linear Algebra*

I N. Herstein, *Topics in Algebra*

Notes

Unit 29: Spectral Theory and Properties of Normal Operators

CONTENTS

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, ... W_k and $T = C_1E_1 + C_2E_2 + ... + C_k E_k$ 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 ... C_k are the distinct characteristic values of T and E_1, E_2 ... E_k are the orthogonal projections of V on W_1, W_2 ... 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, ... 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.

Notes

29.1 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 $c_i(\alpha \mid \beta) = (T\alpha \mid \beta) = (\alpha \mid T^*\beta) = (\alpha \mid \overline{c}_i \beta)$. 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 $e_j = \prod_{i \neq j} \left(\frac{x - c_i}{c_j - c_i} \right)$, 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

$$f(S) = \{b_1, \ldots, b_r\}$$

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

$$T' = \sum_j c_j E'_j, \qquad E'_j = UE_jU^{-1}$$

is the spectral resolution of T'. Hence

$$f(T') = \sum_j f(c_j)E'_j$$

$$= \sum_j f(c_j)UE_jU^{-1}$$

$$= U\left(\sum_j f(c_j)E_j\right)U^{-1}$$

$$= Uf(T)^{-1}$$

Notes

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

$$S = \{c_1, \ldots, c_k\}$$

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 $\beta = \{\alpha_1, \ldots, \alpha_n\}$ by the diagonal matrix D with entries $d_1, \ldots, d_n$. Then, in the basis β, $f(T)$ is represented by the diagonal matrix $f(D)$ with entries $f(d_1), \ldots, f(d_n)$. If $\beta' = \{\alpha'_1, \ldots, \alpha'_n\}$ 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

$$\begin{aligned} f(T)\alpha'_j &= \sum_j P_{ij} f(T)\alpha_i \\ &= \sum_j d_i P_{ij}\alpha_i \\ &= \sum_j (DP)_{ij}\alpha_i \\ &= \sum_j (DP)_{ij} \sum_k P_{ki}^{-1}\alpha'_k \\ &= \sum_k (P^{-1}DP)_{kj}\alpha'_k. \end{aligned}$$

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 $d_1, \ldots, d_n$; Let f be a complex-valued function which can be applied to $d_1, \ldots d_n$, and let $f(D)$ be the diagonal matrix with entries $f(d_1) \ldots .f(d_n)$. 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 $c_1, \ldots, c_k$, 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 $E_i E_j = 0$ when $i \ne j$, $E_1^2 = E_i$, $E_i^* = E_i$,

and

$$I = E_1 + \ldots + E_k.$$

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.

Notes

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

$$(N\alpha \mid N\alpha) = (N^2\alpha \mid \alpha) = (T^*T\alpha \mid \alpha) = (T\alpha \mid T\alpha).$$

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 $r_1, \ldots, r_k$ are the distinct roots of $\mathcal{F}$, then

(i) $V(r_i)$ is orthogonal to $V(r_j)$ when $i \neq j$, and

(ii) $V = V(r_1) \oplus \ldots \oplus V(r_k)$.

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 $r_1, \ldots, r_k$, be the roots of F. Suppose $\{T_1, \ldots, T_m\}$ is a maximal linearly independent subset of $\mathcal{F}$, and let

$$\{E_{i1}, E_{i2}, \ldots\}$$

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 $T_1, \ldots, T_m$, commute with one another.

Since

Notes

$$I = \left(\sum_{j_1} E_{1ji}\right)\left(\sum_{j_2} E_{2j_2}\right)\left(\sum_{jm} E_{mj_m}\right)$$

each vector α in V may be written in the form

$$\alpha = \sum_{j_1 \ldots, j_m} E_{1j_1}E_{2j_2}\ldots E_{mj_m}\alpha. \qquad \ldots (3)$$

Suppose $j_1, \ldots, j_m$, are indices for which $\beta = E_{1j1}E_{2j2}, \ldots E_{mjm}\,\alpha \neq 0$. Let

$$\beta_i = \left(\prod_{n \neq i} E_{nj_n}\right)\alpha.$$

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 $T \rightarrow \sum_i b_i c_i$, 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 $V(r_1), \ldots, V(r_k)$. It follows that V is the orthogonal direct sum of $V(r_1), \ldots, V(r_k)$.

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 $i \neq j$,

$$I = P_1 + \ldots + P_k,$$

and every T in $\mathcal{F}$ may be written in the form

$$T = \sum_i r_j(T)P_j. \qquad \ldots (4)$$

Definition: The family of orthogonal projections $\{P_1, \ldots, P_k\}$ 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 $P_1, \ldots, P_k$, 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.

Notes

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

$$T = \sum_{j=1}^{k} c_j P_j \qquad \ldots (15)$$

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

$$T^* = \sum_j \overline{c}_j P_j$$

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

$$TU = \sum_{i,\,j} c_i d_j P_i P_j$$

$$= \sum_j c_i d_j P_j$$

$$= UT.$$

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

$$T_{ij}\alpha = r_j(T_{ij})\alpha$$

$$= b_{ij}\alpha$$

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

$$a_{in}^{-1}(T_{in} - b_{in}I)\alpha = a_{in}^{-1}[r_i(T_{in}) - r_n(T_{in})]\alpha = \alpha.$$

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, $U = f(T)$.

29.2 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 $(\alpha \mid N\beta) = 0$ for all β in W. Then $(N^*\alpha \mid \beta) = 0$ 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

$$(N^*\alpha \mid \beta) = (\alpha \mid N\beta) = 0$$

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

$$f(T)^* = \overline{a}_0I + \overline{a}_1T^* + \cdots + \overline{a}_n(T^*)^n.$$

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 $(\alpha \mid \beta) = 0$.

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

$$(\alpha \mid \beta) = (g(T)\,b(T)\,\alpha \mid \beta) = (b(T)\,\alpha \mid g(T)^*\beta)$$

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 $(\alpha \mid \beta) = 0$.

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, …, 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) $V = V_1 \oplus \ldots \oplus V_s$;

Notes

(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

$$\left.\begin{aligned} S^*\alpha &= -\beta \\ S^*\beta &= \alpha \end{aligned}\right\} \quad \ldots (1)$$

$(\alpha \mid \beta) = 0$, 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 $V_1, \ldots, V_s$ be a maximal collection of two-dimensional subspaces satisfying (i) and (ii), and the additional conditions.

$$\begin{aligned} T^*\alpha_j &= a\alpha_j - b\beta_j, \\ 1 &\le j \le s. \qquad \ldots (2) \\ T^*\beta_j &= b\alpha_j - a\beta_j \end{aligned}$$

Let $W' = V_1 + \ldots + V_s$. Then W is the orthogonal direct sum of $V_1, \ldots, V_s$. 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_j 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

$$E_j U E_j = U E_j^2 = U E_j.$$

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 $T_j = c_j I_j$, it is clear that U_j also commutes with $T_j^* = \overline{c}_j I_j$. 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 $U_j T_j = T_j U_j$, it follows that $T_j^{-1} U_j = U_j T_j^{-1}$. 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

Notes

if $T_j = c_j I$. 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

$$T'\alpha'_j = UT\alpha_j$$

Notes

$$= \sum_k A_{kj} U\alpha_k$$

$$= \sum_k A_{kj}\alpha'_k$$

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

$$\det(xI_j - T_j) = (x - c_j)^{s_j}$$

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

$$\det(xI_j - T_j) = p_j^{s_j}$$

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

Notes

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) $\det B = e^{\text{tr } A}$;
   (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.

29.3 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.

29.4 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 $(T\alpha \mid \alpha) \geq 0$ for every α in V.

The Spectral Resolution: The decomposition of the linear operator T as the sum of orthogonal projections, i.e.

$$T = \sum_{i=1}^{k} C_i E_i.$$

Notes

29.5 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. $D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{9-\sqrt{57}}{2} & 0 \\ 0 & 0 & \frac{9+57}{2} \end{bmatrix}$

29.6 Further Readings

Books Kenneth Hoffman and Ray Kunze, *Linear Algebra*

Michael Artin, *Algebra*

Unit 30: Bilinear Forms and Symmetric Bilinear Forms

Notes

CONTENTS

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.

30.1 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

$$f(v) = (v, A, v) = a_{11}x_1^2 + a_{22}x_2^2 + ... + a_{nn}x_n^2 + 2\sum_{iLj} a_{ij}x_j x_j$$

In real n-dimensional Euclidean space such quadratic functions serve to define the quadratic surfaces.

Notes

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

$$\left.\begin{aligned} f(c\alpha_1 + \alpha_2, \beta) &= cf(\alpha_1, \beta) + f(\alpha_2, \beta) \\ f(\alpha_1 + c\beta_1, \beta_2) &= cf(\alpha_1, \beta_1) + f(\alpha_2, \beta_2) \end{aligned}\right\} \quad \ldots(1)$$

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

$$f(\alpha, \beta) = X^tAY. \quad \ldots (2)$$

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).

Notes

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

$$f(\alpha, \beta) = [\alpha]^t_\beta A[\beta]_\beta \qquad \ldots (3)$$

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 $f \to [f]_\beta$ 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

Notes

$$f(\alpha, \beta) = [x_1, x_2] \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$$

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^*.

Notes

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_f).

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

Notes

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) $f(\alpha, \beta) = (x_1 - y_1)^2 + x_2y_2$

   (b) $f(\alpha, \beta) = (x_1 + y_1)^2 + (x_1 - y_1)^2$

   (c) $f(\alpha, \beta) = x_1y_2 - x_2y_1$

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

$$\text{rank } f = \dim V - \dim W.$$

30.2 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

$$f(X, Y) = X^tAY$$

is symmetric.

This happens if and only if $X^tAY = Y^tAX$ for all column matrices X and Y. Since X^tAY is a 1×1 matrix, we have $X^tAY = Y^tA^tX$. Thus f is symmetric if and only if $Y^tA^tX = Y^tAX$ 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

$$f(\alpha, \beta) = \tfrac{1}{4} q(\alpha + \beta) - \tfrac{1}{4} q(\alpha - \beta) \qquad ...(5)$$

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 $f_A(X, Y) = X^tAY$, the associated quadratic form is

$$q_A(X) = X^tAX = \sum_{i,j} A_{ij}x_ix_j$$

Notes

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 $i \neq j$.

Notes

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

$$\dim V^+ + \dim V^- = \text{rank } f.$$

Notes

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

30.3 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.

30.4 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 $f(\alpha, \beta) \neq 0$.

Notes

The polarization Identity helps in determining the symmetric bilinear form by its associated quadratic form.

30.5 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) $f(\alpha, \beta) = \frac{b}{2}(x_1y_2 + y_1x_2)$

   Here $\alpha = (x_1, x_2)$

   $\beta = (y_1, y_2)$

30.6 Further Readings

Books Kenneth Hoffman and Ray Kunze, *Linear Algebra*

Michael Artin, *Algebra*

Unit 31: Skew-symmetric Bilinear Forms

Notes

CONTENTS

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, $A^t = -A$.

31.1 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.

Notes

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

$$f(\delta, \alpha) = f(\varepsilon - f(\varepsilon, \beta)\alpha + f(\varepsilon, \alpha)\beta, \alpha)$$

$$= f(\varepsilon, \alpha) + f(\varepsilon, \alpha)f(\beta, \alpha)$$

$$= 0$$

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,

$$(\alpha_1, \beta_1), (\alpha_2, \beta_2), \ldots, (\alpha_k, \beta_k)$$

with the following properties:

(a) $f(\alpha_j, \beta_j) = 1, j = 1, \ldots, k.$

(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

$$V = W_1 \oplus \ldots \oplus W_k \oplus W_0$$

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.

Notes

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 $\{\gamma_1, \ldots, \gamma_s\}$ 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

31.2 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.

Notes

31.3 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. $n = 2k$.

31.4 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.

31.5 Further Readings

Books Kenneth Hoffman and Ray Kunze, *Linear Algebra*

Michael Artin, *Algebra*

Unit 32: Groups Preserving Bilinear Forms

Notes

CONTENTS

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**.

32.1 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

Notes

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

$$A^{t'} = (P^t A P)^t = P^t A^t P = P^t A P = A'$$

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;

$$X^t X = X^{t'} P^t P X' = X^{t'} X', \text{ if}$$

$$P^t P = I$$

which means that *P* is an orthogonal matrix.

One of the examples of the orthogonal transformation the rotation of co-ordinate system.

Notes

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.

32.2 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

$$q(T\alpha) = f(T\alpha, T\alpha) = f(\alpha, \alpha) = q(\alpha)$$

Notes

for every α in V. Conversely, since f is symmetric, the polarization identity

$$f(\alpha, \beta) = \tfrac{1}{4} q(\alpha + \beta) - \tfrac{1}{4} q(\alpha - \beta)$$

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

$$q(x_1, \ldots, x_n) = x_1^2 + \ldots + x^2 n.$$

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

$$T \rightarrow [T]_\beta$$

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.

Notes

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

$$y_i = \sum_{k=1}^{n} M_{ik} x_k$$

Notes

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 $M_1, M_2, \ldots M_n$. Show that M belongs to $O(n, c)$ if and only if

$$M^+ j\, M_k = \delta_{jk}.$$

32.3 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.

32.4 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**.

32.5 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

   $$\det T = \pm 1.$$

32.6 Further Readings

Books Kenneth Hoffman and Ray Kunze, *Linear Algebra*

Michael, *Artin Algebra*

LOVELY PROFESSIONAL UNIVERSITY
Jalandhar-Delhi G.T. Road (NH-1)
Phagwara, Punjab (India)-144411
For Enquiry: +91-1824-300360
Fax.: +91-1824-506111
Email: odl@lpu.co.in