Advanced Abstract Algebra II

DEMTH529

Edited by:
Dr. Kulwinder Singh

LOVELY PROFESSIONAL UNIVERSITY

Advanced Abstract Algebra II

Edited By

Dr. Kulwinder Singh

CONTENTS

Unit 01: Integral Domains

CONTENTS

Objectives

After studying this unit, you will be able to

- define rings and integral domains,
- understand the concept of divisibility in any integral domain,
- understand Unique Factorization Domain, Principal Integral Domain, and Euclidean Domain with the help of examples,
- relate Euclidean Domain with Principal Ideal Domain and Unique Factorization Domain.

Introduction

In this unit, you will be introduced to rings, and then to special rings whose specialty lay in the properties of their multiplication. In this unit, we will introduce you to yet another type of ring, namely, an integral domain. You will see that an integral domain is a ring with identity in which the product of two non-zero elements is again a non-zero element. We will discuss the various properties of such rings. Next, we will look at special classes of integral domains namely Unique Factorization Domain, Principal Integral Domain, and Euclidean Domain. The examples, properties and their relation will be discussed.

1.1 Ring and Integral Domain

Ring: A system $(R, +, \cdot)$ where R is a non-empty set, + and · are two binary operations defined on set R, is called a ring if it satisfies the following properties:

a) $(R, +)$ is an abelian group.
   - (i) **Closure under addition:** $a + b \in R\ \forall\ a, b \in R$
   - (ii) **Associative:** $(a + b) + c = a + (b + c)\ \forall\ a, b, c \in R$
   - (iii) **Identity:** $\forall\ a \in R$, there exists an element $0 \in R$ such that $a + 0 = a = 0 + a$. The element 0 is called zero or additive identity of the ring.
   - (iv) **Inverse:** For each $a \in R$, there exists $b \in R$ such that $a + b = 0 = b + a$. Then b is called $-a$ or additive inverse of a.
   - (v) **Abelian:** $a + b = b + a\ \forall\ a, b \in R$

b) $(R, \cdot)$ is a semi-group.
   - (i) **Closure under multiplication:** $a \cdot b \in R\ \forall\ a, b \in R$
   - (ii) **Associative:** $(a \cdot b) \cdot c = a \cdot (b \cdot c)\ \forall\ a, b, c \in R$

c) Distributive laws hold in $(R, +, \cdot)$

(i) **Left Distributive Law:** $a \cdot (b + c) = a \cdot b + a \cdot c \; \forall \; a, b, c \in R$
(ii) **Right Distributive Law:** $(a + b) \cdot c = a \cdot c + b \cdot c \; \forall \; a, b, c \in R$

Ring with unity: An element $u \in R$ is called a unity if

$$a \cdot u = u \cdot a = a \; \forall \; a \in R.$$

We generally denote unity by 1. A ring that contains a unity element is called a ring with unity.

Note:

A ring may or may not with unity. For example, the ring of integers $\mathbb{Z}$ has unity 1 and the ring of even integers $2\mathbb{Z}$ contains no such element u satisfying the condition $a \cdot u = u \cdot a = a \; \forall \; a \in 2\mathbb{Z}$.

Units of a ring: Let R be a ring with unity 1. Then an element $a \in R$ is called a unit if there exists an element $b \in R$ such that $a \cdot b = 1 = b \cdot a$.

Note:

Let R be a ring with unity 1. Then 1 is always a unit.

(i) Except for unity, the ring may have some elements are units, but some are not. For example, in the ring of integers, only 1 and -1 are units and all integers except 1 and -1 are not units.
(ii) It may also happen that all the non-zero elements of the ring are units. For example, in the ring of rational numbers, all the non-zero elements of the ring are units.

Ring with/without zero divisors: Let R be a ring

- An element $a \in R$ is called a left zero-divisor if $a \cdot b = 0$ for some non-zero $b \in R$.
- An element $a \in R$ is called a right zero-divisor if $b \cdot a = 0$ for some non-zero $b \in R$.
- A non-zero element $a \in R$ which is either left or right zero divisor is called a proper zero divisor.

Note:

In a ring R, 0 (The additive identity of a ring) is always a zero divisor, called improper or trivial zero divisor.

(i) There are rings without any proper zero divisor. For example, the ring of integers ($\mathbb{Z}$) as for two integers a, b we know that $a \cdot b = 0$ implies at least one of a and b is zero.
(ii) Some rings are with proper zero divisors. For example, $\mathbb{Z}_6$ under the compositions of addition and multiplication modulo 6. Then $\bar{2}, \bar{3} \in \mathbb{Z}_6$ are both non-zero but $\bar{2} \cdot \bar{3} = \bar{0}$.

For the sake of convenience, we will write ab in place of $a \cdot b$.

Commutative Ring: A ring R is called commutative if $a \cdot b = b \cdot a$ for all $a, b \in R$.

Note: A ring may or may not be commutative. For example, the ring of integers ($\mathbb{Z}$) is commutative and the ring of square matrices of order 2 over the field of real numbers $M_{2\times 2}(\mathbb{R})$ is not commutative. For example,

$$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 6 & 8 \end{bmatrix}$$

and

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 4 \\ 3 & 8 \end{bmatrix}$$

This implies, $M_{2\times2}(\mathbb{R})$ is not commutative.

Integral Domain:A commutative ring R without proper zero divisors is called an Integral Domain. For example, $\mathbb{Z}$, $M_{2\times2}(\mathbb{R})$ are both integral domains and $\mathbb{Z}_6$is not an integral domain.

Left Ideal of a ring: Let $I \neq \phi$ be a subset of a ring R. Then I is called a left ideal of R if

(i) $a - b \in I \ \forall \ a, b \in I$
(ii) $ra \in I \ \forall \ r \in R, a \in I$

Right Ideal of a ring: Let $I \neq \phi$ be a subset of a ring R. Then I is called a right ideal of R if

(i) $a - b \in I \ \forall \ a, b \in I$
(ii) $ar \in I \ \forall \ r \in R, a \in I$

Ideal of a ring: A non-empty subset I of a ring R is called an ideal of R if it is both left as well as right ideal of R.

Divisibility in a commutative ring with unity: Let R be a commutative ring with unity. Let a, b be two elements in R, b is said to divide a, symbolically we write $b|a$, if $a = bc$ for some $c \in R$.

b is called a factor of a.

b is said to be a proper factor of a if both b and c are non-units.

For example, in the ring of integers, 3 divides 6 as there exists integer 2 such that $6 = 3 \cdot 2$.

Associates: Let R be a commutative ring with unity. An element a of R is said to be an associate of $b \in R$ if $a = bu$ for some unit $u \in R$. It is denoted as $a{\sim}b$. For example,

In the ring of integers, for any element a, there are two associates of a given by $a, -a$.

In the ring $\mathbb{Z}_8$, associates of $\bar{2}$ are given by $\bar{2}$ and $\bar{6}$.

Theorem 1.1.1: Let R be a commutative ring with unity.The relation ~ of associates is an equivalence relation.

Proof: Let 1 is the unity of ring R.

Reflexive: For all $a \in R, a = a \cdot 1$. Hence, this relation is reflexive.

Symmetric: For $a, b \in R$. Let $a{\sim}b$. This implies,$a = bu$ where u is a unit.

Since u is a unit, therefore, u^{-1} exists in R.

Post-multiply $a = bu$ with u^{-1}, we get,

$$au^{-1} = b$$

This implies, $b{\sim}a$. Hence, the relation is symmetric.

Transitive: For $a, b, c \in R$. Let $a{\sim}b$ and $b{\sim}c$

There exist units $u, v \in R$ such that $a = bu$ and $b = cv$

Consider $a = bu = (cv)u = c(vu)$

Since u and v both are units so uv is also a unit.

This implies $a{\sim}c$.

Hence, the relation is transitive.

Therefore, the relation is an equivalence relation.

Theorem 1.1.2: In a domain R, for $a, b \neq 0$, $a{\sim}b$ implies $a|b$ and $b|a$.

Proof: Given that $0 \neq a, b \in R$

Let $a{\sim}b$

Then there exists a unit $u \in R$ such that $a = bu$

By the definition of divisibility, $b|a$

Again, the relation of associates is symmetric implies $b \sim a$, and then with the same logic, we can say, $a|b$.

This implies, $a|b$ and $b|a$.

Conversely, Let $a|b$ and $b|a$

Then there exist $c, d \in R$ such that $a = bc$ and $b = ad$

Now $b = ad$

$= bcd$

$\Rightarrow b(1 - cd) = 0$

Given that $b \neq 0$ and R is an integral domain.

This implies, $1 - cd = 0$

That is, $cd = 1$

This implies c is a unit. Then $a = bc$ implies $a \sim b$.

Prime element: Let R be a commutative ring with unity. $p \in R$ is called a prime element of R if

(i) $p \neq 0$, non-unit
(ii) For $a, b \in R$, whenever $p|ab, p|a$ or $p|b$.

Irreducible element: Let R be a commutative ring with unity. $p \in R$ is called an irreducible element of R if

(i) $p \neq 0$, non-unit
(ii) If $p = ab$ for some $a, b \in R$ then a or b is a unit.

Example 1.1.3: Example of an element of a ring which is a prime element as well as irreducible.

Every prime number in the ring of integers is a prime as well as an irreducible element.

Example 1.1.4: An element in a commutative ring R with unity which is a prime but not irreducible element.

Consider $\mathbb{Z}_6$; $\bar{2} \in \mathbb{Z}_6$ is prime but not irreducible.

Proof: Let $\bar{2}|\overline{ab}$ for $\bar{a}, \bar{b} \in \mathbb{Z}_6$

This implies, $ab - 2 = 6k; k \in \mathbb{Z}$
So, $ab = 6k + 2$
This implies $2|ab$ in $\mathbb{Z}$
2 is a prime element in $\mathbb{Z}$.
This implies, $2|a$ or $2|b$
Hence, $\bar{2}|\bar{a}$ or $\bar{2}|\bar{b}$.
That proves that $\bar{2}$ is a prime element in $\mathbb{Z}_6$.
But $\bar{2} = \bar{2} \cdot \bar{4}$ where both $\bar{2}$ and $\bar{4}$ both are non-units in $\mathbb{Z}_6$.
Hence, $\bar{2} \in \mathbb{Z}_6$ is not irreducible.

Example 1.1.5: An element in an integral domain R with unity which is an irreducible but not prime element.

Proof: Consider $3 \in \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$. Then 3 is an irreducible but not prime element.
Let $3 = (a + b\sqrt{-5})(c + d\sqrt{-5}); a, b, c, d \in \mathbb{Z}$
Taking conjugate on both sides, we get,

$$3 = (a - b\sqrt{-5})(c - d\sqrt{-5})$$

Multiplying the two equations we get,

$$9 = (a^2 + 5b^2)(c^2 + 5d^2)$$

This implies $a^2 + 5b^2$ and $c^2 + 5d^2$ are both positive divisors of 9.

That is, $a^2 + 5b^2 = 1, 3$ or 9

Case 1: If $a^2 + 5b^2 = 1$

This is possible only if $a = \pm 1, b = 0$

So that, $a + b\sqrt{-5} = \pm 1$, that is, a unit.

Case 2: If $a^2 + 5b^2 = 3$

Note that there do not exist integers a, b such that $a^2 + 5b^2 = 3$.

Therefore, this case is not possible.

Case 3: If $a^2 + 5b^2 = 9$, then $c^2 + 5d^2 = 1$

Then as done in Case 1, $c + d\sqrt{-5} = \pm 1$ is a unit.

Hence, either $a + b\sqrt{-5}$ or $c + d\sqrt{-5}$ is a unit.

Therefore, 3 is an irreducible element in $Z[\sqrt{-5}]$.

Now, we prove that 3 is not a prime element.

Note that $3|9$, that is, $3|(2 + \sqrt{-5})(2 - \sqrt{-5})$

If possible, let $3|2 + \sqrt{-5}$

Then there exists $a + b\sqrt{-5} \in Z[\sqrt{-5}]$ such that

$$2 + \sqrt{-5} = 3(a + b\sqrt{-5})$$

Comparing the real parts, we get,

$$2 = 3a$$

which is not possible for any integer a.

So, our supposition was wrong.

Similarly, we can see that 3 does not divide $2 - \sqrt{-5}$.

This proves that 3 is not a prime element.

Example 1.1.6: An element in a commutative integral domain R with unity which is neither prime nor irreducible element.

In the ring of integers, every composite number is neither prime nor an irreducible element.

Theorem 1.1.7: Every prime element in an integral domain is irreducible.

Proof: Let R be an integral domain.

Let p be a prime element in R.

Then by definition of a prime element, $p \neq 0$, non-unit.

Let $p = ab$ for some $a, b \in R$

Then $p|p$ implies $p|ab$

Since p is a prime element, therefore, $p|a$ or $p|b$.

If $p|a$, then there exist $x \in R$ such that $a = px$

That is, $a = abx$

This implies, $a(1 - px) = 0$

Since $a \neq 0$ and R is an integral domain, we get,

$$1 - bx = 0$$

That is, $bx = 1$, hence b is a unit.

Similarly, if $p|b$ then a is a unit.

This implies, p is an irreducible element.

Task:

1) Consider the set $S = \left\{\begin{bmatrix} x & x \\ x & x \end{bmatrix} \mid x \in \mathbb{R}\right\}$.

   Then check whether S is a ring under the usual addition and multiplication of matrices or not.

   If yes, check whether S is a ring with unity or not.

2) Show that in an integral domain R, if $a^2 = a$ for some $a \in R$, then $a = 0$ or 1.
3) Determine if $\mathbb{Z}_4$ is integral domain or not.

1.2 Unique Factorization Domain

Definition 1.2.1: A commutative integral domain R with unity is called a Unique Factorization Domain (UFD) if it satisfies the following conditions.

- Every non-zero non-unit element of R is a finite product of irreducible factors.
- If $a = p_1 p_2 \dots p_r$ and $a = q_1 q_2 \dots q_s$ are two expressions of a as a product of irreducible elements, then $r = s$ and there exists a 1-1 correspondence between $p_i's$ and $q_j's$ such that the corresponding elements are associates.

Example 1.2.2: The ring of integers is a Unique Factorization Domain.

Proof: In $\mathbb{Z}$, there are only two units given by 1 and -1.

We know that except 1 and -1, all integers can be written as a product of finite number of prime numbers.

Also, every prime number is an irreducible element in the ring of integers.

Therefore, except 1 and -1, all integers can be written as a product of finite number of irreducible elements.

Hence, $\mathbb{Z}$ is a Unique Factorization Domain.

Example 1.2.3: Every field is a Unique Factorization Domain.

Proof: Since there does not exist any element in a field that is non-zero and non-unit, therefore trivially every field is a Unique Factorization Domain.

Theorem 1.2.4: In a Unique Factorization Domain, every irreducible element is a prime element.

Proof: Let R be a Unique Factorization Domain and p be an irreducible element of R.

Then p is non-zero and non-unit.

Let $p|ab$ for some $a, b \in R$

Then there exist $c \in R$ such that $ab = pc$ ... (1)

Three cases arise:

Case 1: If a and b are both units.

This implies p is a unit that is not so.

Hence, a and b are not both units.

Case 2: Let a or b is a unit.

If a is a unit.

Then from (1), $b = a^{-1}pc$

Since R is commutative, this implies, $p|b$

Similarly, if b is a unit then $p|a$

Case 3: Let a and b both are non-units.

Since a and b both are non-zero, non-unit elements of a Unique Factorization Domain R, there exist irreducible elements $p_1, p_2, \dots p_n, q_1, q_2, \dots, q_m$ in R such that

$a = p_1 p_2 \dots p_n$ and $b = q_1 q_2 \dots q_m$

Claim: c is not a unit.

If c is a unit then (1) implies that p is associate of ab.

Since p is irreducible, a or b is a unit which is not so in this case.

Therefore, c is not a unit. So, there exist irreducible elements $r_1, r_2, \dots, r_t$ in R such that

$$c = r_1 r_2 \dots r_t$$

Then from (1)

$$p_1 p_2 \dots p_n q_1 q_2 \dots q_m = p r_1 r_2 \dots r_t$$

By uniqueness of expression in a Unique Factorization Domain,

$p \sim p_i$ for some i or $p \sim q_j$ for some j

That is, $p|p_i$ for some i or $p|q_j$ for some j

Also, $p_i|a\ \forall\ i$ and $q_j|b\ \forall\ j$

This implies, $p|a$ or $p|b$.

Hence, p is a prime element.

1.3 Principal Ideal Domain

For a non-empty subset S of a commutative ring R, the ideal generated by S is the smallest ideal containing S.

Definition 1.3.1: Let R be a commutative ring and $a \in R$ then the ideal generated by a single element is called the principal ideal of R. If I is the principal ideal of R generated by a then we denote it as $I = \ < a >$.

Theorem 1.3.2: In a commutative ring R with unity, $< a > \ = \{ar | r \in R\}$

Proof: Let R be a commutative ring with unity 1. To prove that ideal I of R generated by a is same as set $S = \{ar | r \in R\}$, we need to prove that

i. $a \in S$
ii. S is an ideal of R
iii. If there is any other ideal J of R containing a then $S \subseteq J$.

$$S = \{ar | r \in R\} = aR$$

Since R is a ring with unity 1. Therefore, $a1 = a \in S$, which proves i.
Now, we prove, S is an ideal of R.
Since $a \in S, S \neq \phi$
Let $ar_1, ar_2 \in S; r \in R$
Now, $r_1, r_2 \in R$ and R is a ring. Then $r_1 - r_2, r_1 r \in R$.
Then $ar_1 - ar_2 = a(r_1 - r_2) \in S$
and $(ar_1)r = a(r_1 r) \in S$
This implies, S is an ideal of R which proves ii.
Let J be an ideal of R containing a, then by the definition of ideal, $ar \in J\ \forall\ r \in R$
This implies, $S \subseteq J$
Hence, $< a > \ = \{ar | r \in R\}$.

Definition 1.3.3: An integral domain R with unity is called a Principal Integral Domain (Principal Ideal Domain) if every ideal of R is generated by a single element of R.

In other words, an integral domain R with unity is called a Principal Ideal Domain if, for every ideal I of R, there exists some element $a \in R$ such that $I = < a >$.

Example 1.3.4: Every field is a Principal Ideal Domain.

Proof: Let F be a field.
Let I be a non-zero ideal of F.
Then there exists at least one non-zero element $a \in I$
a being a non-zero element of I is a non-zero element of field F. Hence, $a^{-1} \in F$.
Then $a \in I, a^{-1} \in F$ implies, $aa^{-1} = 1 \in I$
For all $b \in I, b = b1$
This implies $I = < 1 >$
Hence, every ideal of F is generated by a single element.
So, F is a Principal Ideal Domain.

Example 1.3.5: The ring of integers (Z) is a Principal Ideal Domain.

Proof: The ring of integers is an integral domain.
Let I be a non-zero ideal of Z.
Then there exists at least one non-zero element in I. Let a be a non-zero element in I.
If $a \in I$ since I is an ideal, therefore, $-a \in I$ and one of the $a, -a$ is a positive integer.
Choose the smallest positive integer in I.
Let $a \in I$ is the smallest positive integer in I.
Claim: $I = < a >$
Since $a \in I, < a > \subseteq I$
Let $b \in I$
Divide b by a, then by divisibility theory of integers there exist $q, r \in Z$ such that
$b = aq + r; r = 0$ or $0 < r < b$

If $r \neq 0$

$$r = b - aq$$

Now, $a \in I, q \in Z$, by the definition of ideal, $aq \in I$.
Also, $b \in I$, this implies, $b - aq \in I$
That is, $r \in I$
Since a is the least positive integer in I and $r > 0$
Therefore, $r \in I$
So, we arrive at a contradiction.
This implies, $r = 0$
That is, $b = aq \in < a >$
So, $I \subseteq < a >$ and hence, $I = < a >$.
Hence, every ideal of Z is generated by a single element. So, Z is a Principal Ideal Domain.

Example 1.3.6: Let F be a field. Then $F[x]$ is a Principal Ideal Domain.

Proof: Let I be a non-zero ideal of $F[x]$.
Then there exists at least one non-zero polynomial in I.
Choose the polynomial with the least degree.
Let $f(x) \in I$ is the polynomial with the smallest degree.
Claim: $I = < f(x) >$
Since $f(x) \in I, < f(x) > \subseteq I$
Let $g(x) \in I$
Divide $g(x)$ by $f(x)$, then by divisibility theory of polynomials there exist $q(x), r(x) \in F[x]$ such that
$g(x) = q(x)f(x) + r(x); r(x) = 0$ or $0 < \deg r(x) < \deg f(x)$

If $r(x) \neq 0$

$$r(x) = g(x) - q(x)f(x)$$

Now, $f(x) \in I, q(x) \in F[x]$, by the definition of ideal, $q(x)f(x) \in I$.
Also, $g(x) \in I$, this implies, $g(x) - q(x)f(x) \in I$
That is, $r(x) \in I$
Since $f(x)$ is the polynomial with least degree in I and $\deg r(x) < \deg f(x)$
Therefore, $r(x) \notin I$
So, we arrive at a contradiction.
This implies, $r(x) = 0$
That is, $g(x) = f(x)q(x) \in < f(x) >$
So, $I \subseteq < f(x) >$ and hence, $I = < f(x) >$.
Hence, every ideal of $F[x]$ is generated by a single element. So, $F[x]$ is a Principal Ideal Domain.

Theorem 1.3.7: In a Principal Ideal Domain, every irreducible element is a prime element.
Proof: Let R be a Principal Ideal Domain.
Let $p \in R$ be an irreducible element of R.
Then p is non-zero and non-unit.
Let $a, b \in R$ such that $p|ab$
If possible, let p does not divide a.
$< p >$ and $< b >$ are both ideals of R, hence $< p > + < b >$ is an ideal of R.
Since R is Principal Ideal Domain, there exist $d \in R$ such that $< p > + < b > = < d >$

$$< p > \subseteq < p > + < b > = < d >$$

So, $p \in < d >, d|p$

Therefore, there exists $x \in R$, such that $p = dx$
But p is irreducible, hence, d or x is a unit.
Case 1: If d is a unit.
$< p > + < b > = < d > = < 1 >$ (d is a unit)
So, there exist $x, y \in R$ such that

$$px + by = 1$$

Pre-multiply both sides by a, we get,

$$apx + aby = a$$

Since $p|ab$, we get, $p|apx + aby = a$
That is, $p|a$ but p does not divide a.
Case 2: x is a unit.
Then x^{-1} exists.

$$px^{-1} = d, d \in < p >$$

That is,

$$< p > + < b > = < p >$$

This implies,

$$< b > \subseteq < p >$$

So,

$$p|b$$

Therefore, p is a prime element in R.

Lemma 1.3.8: In any ring R, the union of an ascending chain of ideals $A_1 \subseteq A_2 \subseteq \cdots \subseteq A_n \subseteq \cdots$ is an ideal of R.

Proof: Let

$$A = \bigcup_i A_i$$

Consider $a, b \in A = \cup_i A_i$
There exist positive integers t, r such that $a \in A_t, b \in A_r$
Without loss of generality, let $t \leq r$
Since the chain $\{A_i\}$ is ascending chain of ideals, $A_t \subseteq A_r$ so that $a, b \in A_r$
Also, A_r is an ideal of R, so $a - b \in A_r$
For $a \in A_r, r \in R, ar, ra \in A_r$
But $A_r \subseteq A$
Therefore, we get, $a - b, ar, ra \in A$
Hence, A is an ideal of R.

Lemma 1.3.9: In a Principal Ideal Domain R, for every ascending chain of ideals $A_1 \subseteq A_2 \subseteq \cdots \subseteq A_n \subseteq \cdots$, there exists an integer t such that $A_m = A_t \; \forall \; m \geq t$

Proof: From Lemma 1.3.8, we get that,

$$A = \bigcup_i A_i$$

is an ideal of R.
Given that R is Principal Ideal Domain. Therefore, there exists $a \in A$ such that $A = < a >$

$$a \in A = \bigcup_i A_i$$

There exists a positive integer t such that $a \in A_t$
Now consider $m \geq t, A_t \subseteq A_m$ ... (1)
Further, $a \in A_t$ implies, $< a > \subseteq A_t$ so that $A \subseteq A_t$ ... (2)
From (1) and (2), $A \subseteq A_t \subseteq A_m \subseteq A$
That is, $A_t = A_m \; \forall \; m \geq t$

Definition 1.3.10: Let R be a Principal Ideal Domain. An ideal I of R is called a maximal ideal of R if there does not exist any ideal J of R such that

$$I \subset J \subset R$$

where $A \subset B$ means $A \neq B$ that is, A is properly contained in B.

In other words, if there exists any ideal J such that $I \subset J \subset R$ then $J = I$ or $J = R$.

Remark 1.3.11: A maximal ideal in a Principal Ideal Domain is always generated by an irreducible element.

Proof: Let I be a maximal ideal of a Principal Ideal Domain R. Therefore, there exists $a \in R$ such that $I = < a >$

Let $a = bc; b, c \in R$

Now $b|a$ this implies, $< a > \subset < b > \subset R$

$I = < a >$ is a maximal ideal of R. This implies, $< b > = < a >$ or $< b > = R$

If $< b > = < a >$

This implies, $b = ax; x \in R$

Then $bc = axc$

$\Rightarrow (a - axc) = 0$

$\Rightarrow a(1 - xc) = 0$

Since $a \neq 0, cx = 1$

This implies c is a unit.

If $< b > = R$ then b is a unit.

Therefore, either b or c is a unit.

Hence, a is an irreducible element of R.

Lemma 1.3.12: For every non-zero non-unit element a in a Principal Ideal Domain there exists an irreducible element p such that $p|a$.

Proof: Let a be a non-zero, non-unit element of Principal Ideal Domain R.

Let $I_1 = < a >$

If I_1 is maximal ideal this implies, a is an irreducible element of R. Then there is nothing to prove.

If I_1 is not maximal ideal, then there exists an ideal I_2 of R such that $I_1 \subset I_2 \subset R$.

There exists some element $a_1 \in R$ such that $I_2 = < a_1 >$, that is, $< a > \subset < a_1 >$

If I_2 is a maximal ideal, then a_1 is irreducible then we can choose $a_1 = p$, hence $p|a$

If I_2 is not maximal ideal, then there exists I_3 such that $I_2 \subset I_3 \subset R$

Continuing so on, we get,

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

By Lemma 1.3.11, there exists some natural number n such that I_n is a maximal ideal.

Hence, $I_n = < p >; p$ is an irreducible element of R.

Also, $I_1 \subset I_n \Rightarrow < a > \subset < p > \Rightarrow p|a$

Theorem 1.3.13: Every Principal Ideal Domain is Unique Factorization Domain.

Proof: Let a be a non-zero, non-unit element of a Principal Ideal Domain R.

By Lemma 3, there exists an irreducible element p_1 such that $p_1|a$.

Since $p_1|a$, there exists some $a_1 \in R$ such that $a = a_1 p_1$

This implies, $< a > \subset < a_1 >$

If $< a > = < a_1 >$

$\Rightarrow a_1 \in < a >$, so, there exists some $r \in R$ such that $a_1 = ar$

That is, $a_1 = a_1 p_1 r$

$\Rightarrow a_1(1 - p_1 r) = 0$

As $a_1 \neq 0, 1 - p_1 r = 0$

$\Rightarrow p_1 r = 1 \Rightarrow p_1$ is a unit.

Therefore, we arrive at a contradiction.

Hence, $< a > \subset < a_1 >$.

If a_1 is a unit $a = a_1 p_1$

This implies, a is associate of p_1, hence a is an irreducible element.

If a_1 is not a unit, then there exists some irreducible element p_2 such that $p_2|a_1 \Rightarrow a_1 = a_2 p_2$ for some $a_2 \in R$, so that $a = a_1 p_1 = a_2 p_2 p_1$

That is $< a_1 > \subset < a_2 >$

If a_2 is a unit, we see that a is associate of $p_2 p_1$ that is a finite product of irreducible elements.

If a_2 is not a unit then continuing so on, we will get a_3 such that

$$< a_1 > \subset < a_2 > \subset < a_3 > \subset \cdots$$

By Lemma 1.3.12, there exists some natural number n such that a_n is a unit.

Then $a_{n-1} = a_n q_n; q_n$ is an irreducible element and hence a_{n-1} is an irreducible element.

$a = a_1 p_1 = a_2 p_2 p_1 \ldots \ldots = p_1 p_2 \cdots p_n$ where $p_n = a_{n-1}$.

Now we prove uniqueness.

$a = p_1 p_2 \ldots p_n$ and $a = q_1 q_2 \ldots q_r$ be two expressions of a as a product of irreducible elements of R.

For $n = 1$ there is nothing to prove.

Let the result is true for all those a which can be expressed as a product of m number of irreducible elements where $m < n$.
Now $a = p_1 p_2 \dots p_n = q_1 q_2 \dots q_r$
This implies, $q_1 | a$, that is, $q_1 | p_1 p_2 \dots p_n$
⇒ there exists some p_i such that $q_1 | p_i$
Since q_1 and p_i are both irreducible so, there exists some unit u_i such that $p_i = q_1 u_i$
Without loss of generality, let $i = 1, p_1 = q_1 u_1$
So that, $p_1 p_2 \dots p_n = q_1 q_2 \dots q_r$
That is, $q_1 u_1 p_2 \dots p_n = q_1 q_2 \dots q_r$
⇒ $p_2' \dots p_n' = q_2 \dots q_r$ where $p_2' = u p_2, p_i' = p_i \ \forall \ i \geq 2$
So, p_i' is an associate of $p_i \ \forall i$
Let $b = p_2' \dots p_n' = q_2 \dots q_r$
Thus, b has two expressions with $n - 1$ number of irreducible elements.
By the induction hypothesis, there exists a one-one correspondence between p_i' and q_j such that p_i' is an associate of q_j. Also, $n - 1 = r - 1$
So, $n = r$
Also, $p_i \sim p_i' \sim q_j$
Therefore, $p_i \sim q_j \ \forall \ i, j > 2$
Also, $p_1 \sim q_1$
Therefore, p_i is associate to a unique q_j.
Hence, every Principal Ideal Domain is a Unique Factorization Domain.

Task:
1) Let F be a field. Then prove or disprove:
a) $F[x]$ is a Principal Integral Domain.
b) $F[x]$ is a Unique Factorization Domain.
2) Prove that $\mathbb{Z}[x]$ is a Unique Factorization Domain but not a Principal Ideal Domain.

1.4 Euclidean Domain

Definition 1.4.1: A non-zero integral domain R is called a Euclidean Domain (ED) if there exists a function $\delta: R - \{0\} \to \mathbb{Z}$ such that

i. $\delta(a) \geq 0 \ \forall \ a \in R - \{0\}$
ii. $\delta(ab) \geq \delta(a) \ \forall \ a, b \in R - \{0\}$
iii. $\forall \ a \in R, b \in R - \{0\}$, there exist unique $q, r \in R$ such that $a = bq + r, r = 0$ or $\delta(r) < \delta(b)$.

Property i. is called non-negativity and iii. is called Euclidean algorithm. The function δ is called Euclidean evaluation.

Example 1.4.2: $\mathbb{Z}$ is Euclidean Domain.

Proof: Consider $\delta: \mathbb{Z} - \{0\} \to \mathbb{Z}$ as $\delta(a) = |a| \ \forall \ a \in \mathbb{Z} - \{0\}$
Clearly, $\delta(a) = |a| \geq 0 \ \forall \ a \in \mathbb{Z} - \{0\}$
$\delta(ab) = |ab| = |a||b| \geq |a| \ (b \in \mathbb{Z} - \{0\}, |b| \geq 1)$
By division of integers, there exist $q, r \in \mathbb{Z}$ such that $a = bq + r, r = 0$ or $|r| < |b|$
That is, $a = bq + r, r = 0$ or $\delta(r) < \delta(b)$
Hence, $\mathbb{Z}$ is Euclidean Domain.

Example 1.4.3: Every field is Euclidean Domain.

Proof: Let F be a field.
Define a function $\delta: F - \{0\} \to \mathbb{Z}$ as $\delta(a) = 1 \ \forall \ a \in F - \{0\}$
$\delta(a) = 1 \geq 0 \ \forall \ a \in F - \{0\}$
$\delta(ab) = 1 = \delta(a)\delta(b) \ \forall \ a, b \in F - \{0\}$
Also, for $a \in F, b \in F - \{0\}$
Since $b \neq 0$ and $b \in F$, $b^{-1} \in F$
$a = (ab^{-1})b + 0; q = ab^{-1}, r = 0$
Hence, every field is a Euclidean Domain.

Example 1.4.4: $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is Euclidean Domain.

Proof: Define map $\delta: \mathbb{Z}[i] - \{0\} \to \mathbb{Z}$ as $\delta(a + bi) = a^2 + b^2$
The sum of the square of two integers is always non-negative. Hence,

$$\delta(a + bi) = a^2 + b^2 \geq 0 \ \forall \ a + bi \in \mathbb{Z}[i] - \{0\}$$

Let $a + bi, c + di \in \mathbb{Z}[i] - \{0\}$. Then

$$\begin{aligned}\delta((a+bi)(c+di)) &= \delta((ac - bd) + i(ad + bc)) \\ &= (ac - bd)^2 + (ad + bc)^2 \\ &= a^2c^2 + b^2d^2 - 2abcd + a^2d^2 + b^2c^2 + 2abcd \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\ &= a^2(c^2 + d^2) + b^2(c^2 + d^2) \\ &= (a^2 + b^2)(c^2 + d^2)\end{aligned}$$

Since $c + di \neq 0, c, d \in \mathbb{Z}$, this implies, $c^2 + d^2 \neq 0$ that is, $c^2 + d^2 \geq 1$
That is $\delta\big((a + bi)(c + di)\big) = (a^2 + b^2)(c^2 + d^2) \geq a^2 + b^2 = \delta(a + bi)$
For $a + bi \in \mathbb{Z}[i], c + di \in \mathbb{Z}[i] - \{0\}$
Then

$$\frac{a + bi}{c + di} = p + qi,$$

where,

$$p = \frac{ac + bd}{c^2 + d^2} \in \mathbb{Q}, q = \frac{bc - ad}{c^2 + d^2} \in \mathbb{Q}$$

Therefore, there exist integers m, n such that $|p - m| \leq \frac{1}{2}, |q - n| \leq \frac{1}{2}$
Let $p - m = \alpha, q - n = \beta$
Then

$$\begin{aligned}a + bi &= (p + qi)(c + di) \\ &= ((m + \alpha) + (n + \beta)i)(c + di) \\ &= (m + ni)(c + di) + (\alpha + \beta i)(c + di)\end{aligned}$$

Let $r' = (\alpha + \beta i)(c + di)$
If $r' \neq 0$

$$\begin{aligned}\delta(r') &= (\alpha^2 + \beta^2)(c^2 + d^2) \\ &\leq \left(\frac{1}{4} + \frac{1}{4}\right)(c^2 + d^2) \\ &= \frac{1}{2}(c^2 + d^2) \\ &< c^2 + d^2 \\ &= \delta(c + di)\end{aligned}$$

So, $r' = 0$ or $\delta(r') < \delta(c + di)$
Hence, $\mathbb{Z}[i]$ is Euclidean Domain.

Theorem 1.4.5 Every Euclidean Domain is Principal Ideal Domain.

Proof: Let R be a Euclidean Domain with Euclidean evaluation δ.
Let A be a non-zero ideal of R.
Therefore, there exists $0 \neq x \in A$
Consider $M = \{\delta(x) \mid 0 \neq x \in A\}$
$\delta(x)$ is a non-negative integer for all $x \in A$
Let $\delta(b)$ is the least non-negative integer in M, so that $b \in A, b \neq 0$.
Claim: $A = \langle b \rangle$
Now, $b \in A$ implies $\langle b \rangle \subseteq A$
For $a \in A, b \neq 0$
By property iii of the definition of Euclidean Domain, we get $q, r \in R$ such that
$a = bq + r; r = 0$ or $\delta(r) < \delta(b)$
Let $r \neq 0, r = a - bq$
Since $a, b \in A, r \in R$, then by definition of ideal, $a - bq = r \in A$
By choice of b, since $\delta(r) < \delta(b)$, we get $r \notin A$

So, we arrive at a contradiction.
Therefore, $r = 0$ and hence, $a = bq \in < b >$
That is, $A \subseteq < b >$
So, $A = < b >$
Hence, every ideal of R is a principal ideal.
So, every Euclidean Domain is Principal Ideal Domain.

Summary

- Rings and integral domains are defined.
- The concept of divisibility in any integral domain is elaborated.
- Unique Factorization Domain, Principal Integral Domain, and Euclidean Domainare explained with the help of examples.
- Relation betweenEuclidean Domain,Principal Ideal Domain, and Unique Factorization Domain is established. That is, every Euclidean Domain is Principal Ideal Domain as well as Unique Factorization Domain. Every Principal Ideal Domain is a Unique Factorization Domain but may not be a Euclidean Domain.

Keywords

- Rings and Integral Domain
- Divisibility in Rings
- Principal Integral Domain
- Euclidean Domain
- Unique Factorization Domain

Self Assessment

1. The number of proper zero divisors in the ring of integers is

A. 0
B. 1
C. 2
D. Infinite

2. An Integral Domain is always

A. With zero divisors
B. With infinitely many units
C. With finitely many units
D. Commutative

3. Let R be a ring. Let I and J are two ideals of R. Which of the following is not true?

A. $I + J$ is an ideal of R
B. $I \cap J$ is an ideal of R
C. $I \cup J$ is an ideal of R
D. IJ is an ideal of R

4. In the ring of integers, associates of 2 are

A. 2
B. -2
C. $2, -2$
D. All integers

5. In the ring Z_6, which of the following is not a zero divisor?

A. 1
B. 2
C. 4
D. 3

6. Which of the following is a prime ideal of Z
A. 6Z
B. 4Z
C. 3Z
D. 8Z

7. Which of the following is true in a PID R?
A. Every element of R is prime as well as irreducible
B. Every prime element of R is irreducible and vice versa
C. A prime element may not be irreducible
D. An irreducible element may not be prime

8. In a PID R, an ideal $< a >$ is maximal ideal then
A. a is a prime element but not irreducible
B. a is irreducible but not prime
C. a is irreducible as well as prime
D. a is neither irreducible nor prime

9. Which of the following is not a PID?
A. Ring of integers
B. Ring of real numbers
C. Ring of square matrices of order 2 over the set of real numbers
D. Ring of rational numbers

10. A PID is always
A. A ring with zero divisors
B. A field
C. With zero divisors
D. A Unique Factorization Domain

11. Let Z denote the ring of integers. Then Z is
A. A PID but not ED
B. An ED but not UFD
C. A UFD but not PID
D. A PID, ED as well as a UFD

12. All the units of $R = \{a + b\sqrt{-5} | a, b \in Z\}$ are
A. 1
B. -1
C. $1, -1$
D. $0, 1, -1$

13. Let R be a Euclidean Domain with unity 1 and Euclidean evaluation δ. Then $\delta(a) = \delta(1)$ implies
A. $a = 1$
B. a is the unity of R
C. $a = 0$
D. a is a unit in R

14. Every ideal of an ED is generated by …… number of elements.
A. 1
B. 2
C. n; where $n \in N$

D. Infinitely many

15. Let R be a Euclidean Domain with unity 1 and Euclidean evaluation δ. Then for $a, b \in R$, $\delta(ab)$

A. $= \delta(a)$

B. $> \delta(a)$

C. $< \delta(a)$

D. $\geq \delta(a)$

Answers for Self Assessment

1.	A	2.	D	3.	C	4.	C	5.	A
6.	C	7.	B	8.	C	9.	C	10.	D
11.	D	12.	C	13.	D	14.	A	15.	D

Review Questions

1. Let n be a positive integer and m is a divisor of n such that $1 < m < n$. Then show that m is a zero divisor in $\mathbb{Z}_n$.
2. List all the zero divisors in $\mathbb{Z}$.
3. For which rings with unity will unity be a zero divisor?
4. Let R be a ring and $a \in R$ be a zero divisor. Then show that every element of the principal ideal Ra is a zero divisor.
5. Show that a subring of a PID need not be PID.

Further Readings

- Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress
- Topics in algebra by I.N. Hartstein, Wiley
- Abstract algebra by David S Dummit and Richard M Foote, Wiley

Weblinks

- https://nptel.ac.in/courses/111/102/111102009/
- https://nptel.ac.in/courses/111/105/111105112/#

Unit 02: Polynomial Ring Over a UFD

CONTENTS

Objectives

After studying this unit, you will be able to

- define Highest Common Factor (HCF) and Least Common Multiple (LCM) of two elements of a commutative ring with unity,
- illustrate the concept of existence/non-existence and non-uniqueness of HCF and LCM with examples,
- prove that HCF and LCM of two elements of a PID and UFD always exist,
- define content of a polynomial and primitive polynomial over a UFD,
- prove results about primitive polynomials,
- illustrate with the help of example that a UFD need not be a PID.

Introduction

In this unit, you will be able to generalize the notion of Highest Common Factor (HCF) and Least Common Multiple (LCM) of two non-zero integers to that of two non-zero elements of a ring. You will see that unlike in the set of integers, it may happen that HCF and LCM of two non-zero elements does not even exist. Moreover, if they exist, then they may not be unique. Further you will understand the characteristics of polynomial rings over a UFD.

2.1 Polynomial Rings Over a UFD

Definition 2.1.1: Let R be a commutative ring. Given two non-zero elements a and b of R, a non-zero element c of R is said to be a HCF of a and b in R if

i. $c|a$ and $c|b$ in R; and

ii. For any $d \neq 0$, $d \in R$ if $d|a$ and $d|b$ in R then $d|c$ in R

HCF of a and b is denoted as (a, b).

Definition 2.1.2: Let R be a commutative ring. Given two non-zero elements a and b of R, a non-zero element d of R is said to be a LCM of a and b in R if

i. $a|d$ and $b|d$ in R; and

ii. For any $c \neq 0$, $c \in R$ if $a|c$ and $b|c$ in R, then $d|c$ in R

LCM of a and b is denoted as $[a, b]$.

Example 2.1.3: HCF and LCM of two elements in a ring may not be unique.

Solution: Consider the ring Z_{12}.

Consider $\bar{6}, \bar{8} \in Z_{12}$

Note that $\bar{6} = \bar{2} \cdot \bar{3}$ and $\bar{8} = \bar{2} \cdot \bar{4}$

This implies, $\bar{2} | \bar{6}$ and $\bar{2} | \bar{8}$

Also, if there is any $\bar{x} \in Z_{12}$ such that $\bar{x} | \bar{6}$ and $\bar{x} | \bar{8}$

This implies, $\bar{x} | \bar{8} - \bar{6} = \bar{2}$

So, $HCF\ (\bar{6}, \bar{8}) = \bar{2}$

Also, $\bar{6} = \overline{10} \cdot \bar{3}$ and $\bar{8} = \bar{2} \cdot \overline{10}$

This implies, $\overline{10} | \bar{6}$ and $\overline{10} | \bar{8}$

Also, if there is any $\bar{x} \in Z_{12}$ such that $\bar{x} | \bar{6}$ and $\bar{x} | \bar{8}$

This implies, $\bar{x} | \bar{2} \cdot \bar{8} - \bar{6} = \overline{10}$

So, $HCF\ (\bar{6}, \bar{8}) = \overline{10}$

Therefore, HCF is not unique.

Note: If c and d are both HCF of a and b in a commutative ring R with unity then c and d are associates.

Proof: Consider $c = HCF\ (a, b)$.

Since $d = HCF(a, b)$, d is a common factor of a and b.

So, $d | c$.

Consider c as a common factor and d as HCF, we get, $c | d$

Therefore, $c | d$ and $d | c$

Thus, c and d are associates.

Example 2.1.4: A pair of non-zero elements a and b in a ring with unity such that LCM of a, b does not exist.

Solution: Consider the ring Z_{12}.

Consider $\bar{6}, \bar{8} \in Z_{12}$

If possible, let $LCM\ [\bar{6}, \bar{8}] = \bar{x}$

This implies, $\bar{6} | \bar{x}$ and $\bar{8} | \bar{x}$

So, $\bar{x} = \bar{6}\bar{n};\ \bar{n} \in Z_{12}$

So, $\bar{x} = \bar{0}, \bar{6}$

Also, $\bar{8} | \bar{x}$

So, $\bar{x} = \bar{8}\bar{m};\ \bar{m} \in Z_{12}$

$\bar{x} = \bar{0}, \bar{8}, \bar{4}$

The only common value is $\bar{0}$. Since LCM is always non-zero.

Therefore, LCM does not exist.

<u>**Theorem 2.1.5:**</u> In a PID R, HCF and LCM always exist.

Proof: We claim that every pair of non-zero elements a and b of R has an HCF and LCM. Further if $d = GCD\ (a,\ b)$ then $d = ax + by$ for some $x,\ y \in R$.

Consider $< a > + < b > = < d >; d \in R$

$$< a > \subseteq < d > \Rightarrow d|a$$

$$< b > \subseteq < d > \Rightarrow d|b$$

If there exist $x \in R$ such that $x|a$ and $x|b$

Then
$< a > \subseteq < x >$ and $< b > \subseteq < x >$

This implies, $< a > + < b > = < d > \subseteq < x >$

$\Rightarrow x|d \Rightarrow d = HCF\ (a, b)$

$< d > = < a > + < b > = d = ax + by$ for some $x, y \in R$

Again, $< a > \cap < b >$ is also an ideal.

Then there exists $c \in R, < a > \cap < b > = < c >$

$$< c > \subset < a > \Rightarrow a|c$$

$$< c > \subset < b > \Rightarrow b|c$$

Let $d \in R$ such that $a|d$ and $b|d$

So, $< d > \subset < a > \cap < b > = < c >$

$\Rightarrow c|d$, hence $c = LCM\ [a, b]$

Theorem 2.1.6: In a UFD R, HCF and LCM of two non- zero elements always exist.

Proof: Let $a, b \neq 0$ elements of a UFD R.

If a is a unit, then

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

Then $HCF\ (a, b) = a$ and $LCM\ [a, b] = b$.

If a and b are both non-units.

Then $a = u$ ·finite product of irreducible elements in R

$a \neq 0$, non-unit in R, there exists some irreducible element $p \in R$ such that $p|a$

If p does not divide b, then $p^0|b$.

$a = up_1^{\alpha_1}p_2^{\alpha_2} \dots p_k^{\alpha_k}$; u is a unit and $\alpha_i \geq 0$

$b = vp_1^{\beta_1}p_2^{\beta_2} \dots p_k^{\beta_k}$; v is a unit and $\beta_i \geq 0$

Let $c = p_1^{\gamma_1}p_2^{\gamma_2} \dots p_k^{\gamma_k}; \gamma_i = \min(\alpha_i, \beta_i)$ and $d = p_1^{\mu_1}p_2^{\mu_2} \dots p_k^{\mu_k}; \mu_i = \max(\alpha_i, \beta_i)$

Then $c = HCF\ (a, b)$ and $d = LCM\ (a, b)$

Corollary 2.1.7: Any finite number of non-zero elements of a UFD have an HCF and LCM

Proof: Let $a_1, a_2, \dots, a_n \in R$; R is a UFD.

If $n = 2$,

By theorem, $HCF\ (a, b)$ always exists.

Let the result is true for $n - 1$, therefore, $HCF\ (a_1, a_2, \dots, a_{n-1})$ exists.

Let $d = HCF\ (a_1, a_2, \dots, a_{n-1})$

Consider $HCF\ (d, a_n) = c$

$\Rightarrow c|d$ and $c|a_n$

$\Rightarrow d|a_i\ \forall\ 1 \leq i \leq n - 1$

So, $c|a_i\ \forall\ 1 \leq i \leq n$

Also, if there exists $d' \in R$ such that $d'|a_i\ \forall\ i$, then $d'|d$ and $d'|a_n$

Therefore, $c'|c$

That is, $c = HCF\ (a_1, a_2, \dots, a_n)$.

Definition 2.1.8: Let R be a UFD. Then a polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n; a_n \neq 0$ is a polynomial of degree n.

$C(f)$ =Content of $f(x) = HCF\ (a_0, a_1, \dots, a_n)$

A polynomial $f(x) \in R[x]$ is called primitive polynomial if its content is a unit. For example, $2 + 3x + x^2$ is a primitive polynomial over the ring of integers.

Lemma 2.1.9: If R is a UFD then every non-zero polynomial in $R[x]$ is a product of a primitive polynomial over R and an element of R.

Proof: Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$

Let $d = C(f) = HCF\ (a_0, a_1, \dots, a_n)$

$$d | a_i\ \forall\ 0 \leq i \leq n$$

Let $a_i = db_i; b_i \in R$

$$\begin{aligned} f(x) &= a_0 + a_1x + \cdots + a_nx^n \\ &= db_0 + db_1x + \cdots + db_nx^n \\ &= d(b_0 + b_1x + \cdots + b_nx^n) \\ &= C(f)\, g(x) \end{aligned}$$

where $C(f) \in R; g(x) = b_0 + b_1x + \cdots + b_nx^n$

$$\begin{aligned} C(g) &= HCF\ (b_0, b_1, \dots, b_n) \\ &= \left(\frac{a_0}{d}, \frac{a_1}{d}, \dots, \frac{a_n}{d}\right) \\ &= \frac{1}{d}(a_0, a_1, \dots, a_n) \\ &= \frac{d}{d} = u;\ unit \end{aligned}$$

Result 2.1.10: The product of two primitive polynomials over a UFD is a primitive polynomial

Proof: Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_mx^m$ be two polynomials over a $UFD\,R$ with degree n and m respectively.

Let

$$\begin{aligned} h(x) &= f(x)g(x) \\ &= \sum_{i+j=k} a_ib_jx^{j+i} \\ &= \sum_{k=0}^{n+m} c_kx^k \end{aligned}$$

Let $d = HCF\ (c_0, c_1, \dots, c_{n+m})$

If d is not a unit then there exists an irreducible element $p \in R$ such that $p|d$

$\Rightarrow p|c_i\ \forall\ 0 \leq c_i \leq n + m$

Also, $HCF\ (a_0, a_1, \dots, a_n)$ and $HCF\ (b_0, b_1, \dots, b_m)$ are both units.

There exists a least positive integer t such that p does not divide a_t and a least positive integer u such that p does not divide b_u.

$$c_{t+u} = (a_0b_{t+u} + a_1b_{t+u-1} + \cdots + a_{t-1}b_{u+1}) + a_tb_u + (a_{t+1}b_{u-1} + \cdots + a_{t+u}b_0)$$

Since $p|a_0b_{t+u} + a_1b_{t+u-1} + \cdots + a_{t-1}b_{u+1}$ and $p|a_{t+1}b_{u-1} + \cdots + a_{t+u}b_0$.

Also, $p|c_{t+u}$.

This implies, $p|a_tb_u$

p is irreducible and hence prime element of R.

Therefore, $p|a_t$ or $p|b_u$

So, we arrive at a contradiction to the choices of a_t and b_u.

This implies, $d = HCF\ (c_0, c_1, \dots, c_{n+m})$ is a unit and hence fg is a primitive polynomial.

Theorem 2.1.11: For two polynomials f and g over a UFD, $C(fg) = C(f)C(g)$.

Proof:

Let $f(x) = C(f)f_1(x)$ and $g(x) = C(g)g_1(x)$ where $f_1(x)$ and $g_1(x)$ are primitive polynomials.

Then $f(x)g(x) = C(f)\ C(g)f_1(x)g_1(x)$

By the theorem, being product of primitive polynomials $f_1(x)g_1(x)$ is a primitive polynomial.

So, $fg(x) = C(f)C(g)f_1(x)g_1(x)$ implies, $C(fg) = C(f)C(g)$

Remark: If fg is primitive polynomial then f and g both are primitive polynomials.

Proof: Suppose f is not primitive polynomial.

There exists $d \in R$ such that $d|\ C(f)$, d is not a unit.

This implies, $d|C(fg)$

That is, fg is not a primitive polynomial.

So, we arrive at a contradiction. Our supposition was wrong.

Therefore, f and g are both primitive polynomials.

Lemma 2.1.12: Let $R[x]$ be a polynomial ring over a commutative ID R. Let $f(x)$ and $0 \neq g(x)$ be polynomials in $R[x]$ of degrees m and n respectively. Let $k = \max(m - n + 1,\ 0)$, and a be the leading coefficient of $g(x)$. Then there exist unique polynomials $q(x)$ and $r(x) \in R[x]$ such that $a^kf(x) = q(x)g(x) + r(x)$, where $r(x) = 0$ or $r(x)$ has degree less than that of $g(x)$.

Proof: Suppose $m < n$

We take $q(x) = 0$ and $r(x) = f(x)$

Here the result holds trivially.

Let $m > n$ and $k = m - n + 1$

We use PMI on m to prove this result.

We assume that result is true for all polynomials of degree $< m$.

Let $\deg f(x) = m$ and leading coefficient of $f(x) = b$.

Consider the polynomial $af(x) - bx^{m-n}g(x)$.

$af(x)$ has leading coefficient ab and is of degree m and $bx^{m-n}\,g(x)$ has leading coefficient ba, and is of degree m.

Therefore,$af(x) - bx^{m-n}g(x)$ is a polynomial of degree $< m$.

By Induction hypothesis, there exists $q_1(x), r_1(x)$ such that

$$a^{m-1-n+1}\left(af(x) - bx^{m-n}g(x)\right) = q_1(x)g(x) + r_1(x)$$

This implies,

$$a^kf(x) = \left(ba^{m-n}x^{m-n} + q_1(x)\right)g(x) + r_1(x)$$

So, the result is true for m also.

Lemma 2.1.13: Let R is a UFD then every irreducible element of R[x] is a prime element of R[x]

Proof: Let $p(x)$ is an irreducible element of $R[x]$.

This implies, $p(x) \neq 0$, non-unit.

Let $f(x), g(x) \in R[x]$ such that $p(x) | f(x)g(x)$

Case 1: If $p(x)$ is a constant polynomial.

Let $p(x) = c \in R$

$p(x) | f(x)g(x)$ implies there exists $h(x) \in R$ such that $f(x)g(x) = p(x)h(x) = ch(x)$

$$C(f)C(g) = c\,C(h)$$

That is, $c | C(f)C(g)$

$p(x) = c$ is irreducible element of $R[x]$ and hence in R, it is irreducible.

R is UFD implies c is prime element.

This implies, $c|C(f)$ or $c|C(g)$ and hence $c|f(x)$ or $c|g(x)$.

Case 2: Let $\deg p(x) > 0$

$p(x)$ does not divide $f(x)$

Consider $S = < f(x) > + < p(x) >$

Then elements of S are of type

$$A(x)f(x) + B(x)p(x); A(x), B(x) \in R[x]$$

Let $0 \neq \phi(x) \in S$ be of smallest degree and a as a leading coefficient of $\phi(x)$.

By Lemma 2.1.12, there exists $h(x), r(x)$ such that

$a^k f(x) = \phi(x)h(x) + r(x); r(x) = 0$ or $\deg r(x) < \deg \phi(x)$

$\Rightarrow r(x) = a^k f(x) - \phi(x)h(x) \in S$

If $\deg r(x) < \deg \phi(x)$

$\Rightarrow r(x) \notin S$

Therefore, $r(x) = 0$

$$a^k f(x) = \phi(x)h(x) = C(\phi)\phi_1(x)\,h(x),$$

where $\phi_1(x)$ is a primitive polynomial.

$\phi_1(x) | a^k f(x)$

$\Rightarrow a^k f(x) = \phi_1(x)t(x)$

$\Rightarrow C(t) = a^k C(f)$

$\Rightarrow a^k | C(t) \Rightarrow a^k | t(x)$

Also, $\phi_1(x)t(x) = a^k f(x)$ and $R[x]$ is an integral domain.

$\Rightarrow \phi_1(x) | f(x)$

Similarly, $\phi_1(x) | p(x)$, $p(x)$ is irreducible.

$\phi_1(x)$ is a unit or $p(x) | f(x)$

$\Rightarrow \phi_1(x)$ is a unit.

$$\Rightarrow \phi_1(x) \in R$$

Thus, $\phi(x) = C(\phi)\phi_1(x) \in R$

$\phi(x) = a \in R$

$a = A(x)f(x) + B(x)p(x); A(x), B(x) \in R[x]$

$\Rightarrow a\,g(x) = A(x)f(x)\,g(x) + B(x)p(x)\,g(x)\ ; A(x), B(x) \in R[x]$

$\Rightarrow p(x)|g(x)$

Theorem 2.1.14: If R is UFD then $R[x]$ is a UFD.

Proof: Let $f(x)$ be a non-zero, non-unit element of $R[x]$.

Without loss of generality, we may assume that $f(x)$ is a primitive polynomial.

Let $\deg f = 1$

f is either primitive polynomial or irreducible polynomial. So, we are done in this case.

Assume that the result is true for $\deg f < n$

For $\deg f = n$

If $f(x)$ is irreducible then $f(x) = f(x)$.

If $f(x)$ is reducible, $f(x) = f_1(x)f_2(x)$

Therefore, $\deg f_1(x), \deg f_2(x) < n$

$f_1(x) = g_{11}(x)g_{12}(x)g_{13}(x) \dots g_{1n}(x)$; g_{1i} are all irreducible elements in $R[x]$

$f_2(x) = g_{21}(x)g_{22}(x)g_{23}(x) \dots g_{2m}(x)$; g_{2i} are all irreducible elements in $R[x]$

Then $f(x) = g_{11}(x)g_{12}(x)g_{13}(x) \dots g_{1n}(x)g_{21}(x)g_{22}(x)g_{23}(x) \dots g_{2m}(x)$; g_{1i}, g_{2i} are all irreducible elements in $R[x]$

Uniqueness follows from Lemma 2.

Therefore, $R[x]$ is a UFD.

Example 2.1.15: A UFD need not be a PID.

Proof: Z is a UFD.

$\Rightarrow Z[x]$ is also UFD.

If possible, let $Z[x]$ is a PID.

$< 2 > + < x >$ is an ideal of $Z[x]$

This implies, there exists $f(x) \in Z[x]$ such that $< 2 > + < x > = < f >$

Now $2 \in < f >$

There exists $g(x) \in Z[x]$ such that $2 = f(x)g(x)$.

This implies, $\deg f(x)\, g(x) = \deg 2 = 0$

That is, $\deg f(x) = \deg g(x) = 0$

Again $< x > \subset < f >$ implies $f|x$

This implies, there exists $h(x) \in Z[x]$ such that $x = f(x)h(x)$

Comparing degrees, we get, $\deg h(x) = 1$

So, $1 = f(x)(leading\ coeff\ of\ h)$

That is, $f(x) = \pm 1$; a unit in Z.

$< 2 > + < x > = < f > = Z[x]$

But $x + 1 \in Z[x] = < 2 > + < x >$

$$x + 1 = 2f(x) + x\,g(x);\ f(x), g(x) \in Z[x]$$

Comparing constant term on both sides, we get, $1 = \pm 2$ which is absurd.

This implies, $< 2 > + < x >$ is not a principal ideal and hence, $Z[x]$ is not a PID.

Task:

Express f as $gq + r$, where $\deg r < \deg g$, in each of the following cases.

a) $f = x^4 + 1, g = x^3$ in $Q[x]$
b) $f = x^3 + \bar{2}x^2 - x + \bar{1}, g = x + \bar{1}$ in $Z_3[x]$

c) $f = x^3 - 1$, $g = x - 1$ in $R[x]$

Summary

- Highest Common Factor (HCF) and Least Common Multiple (LCM) of two elements of a commutative ring with unity are defined.
- The concept of existence/non-existence and non-uniqueness of HCF and LCM with examples is illustrated.
- Proved that HCF and LCM of two elements of a PID and UFD always exist
- Content of a polynomial and primitive polynomial over a UFD is defined.
- Results about primitive polynomials are proved.
- Example is given to prove that a UFD need not be a PID

Keywords

- Highest Common Factor
- Least Common Multiple
- Content of a polynomial
- Polynomial ring over a UFD
- Primitive Polynomial

Self Assessment

1. Let R be a commutative ring with unity. Let $a, b \in R$. Choose the correct statement.
A. $HCF\ (a, b)$ always exists but $LCM\ (a, b)$ may not
B. $LCM\ (a, b)$ always exists but $HCM\ (a, b)$ may not
C. $HCF\ (a, b)$ and $LCM\ (a, b)$ both always exist, and both are unique
D. $HCF\ (a, b)$ and $LCM\ (a, b)$ may or may not exist

2. Let R be a commutative ring with unity. Let $a, b \in R$. If c and d are both $HCF(a, b)$. Then
A. $c = d$
B. c is an associate of d
C. c is inverse of d
D. c and d both are units

3. Let R be a PID. Then for two elements $a, b \in R$,
A. HCF and LCM always exist and are unique
B. HCF and LCM may not exist
C. HCF and LCM always exist and if there are two or more of them then they are associates
D. HCF and LCF always exist and if there are two of them then they are additive inverse of each other

4. Let Z denotes the ring of integers. Then $HCF\ (8, 12) =$
A. 4
B. -4
C. 4 and -4
D. 1

5. In $Z[x]$, the polynomial ring over the set of integers, consider $x^2 + 2x + 1$ and $x^2 - 1$. Let $c = HCF(x^2 + 2x + 1, x^2 - 1)$ and $d = LCM(x^2 + 2x + 1, x^2 - 1)$. Then
A. $c = x + 1, d = x - 1$
B. $c = x + 1, d = (x + 1)^2(x - 1)$
C. $c = (x + 1)^2, d = x - 1$
D. $c = (x + 1), d = (x - 1)^2$

6. $HCF\ (\bar{6}, \bar{3}) \in Z_{12}$ is/are
A. $\bar{1}$
B. $\bar{2}$
C. $\overline{10}$
D. $\bar{2}, \overline{10}$

7. Which of the following is a primitive polynomial over Z (Ring of integers)?
A. $4x^2 + 2x + 6$
B. $3x^2 + 2x + 1$
C. $9x^2 + 12x + 6$
D. $24x^2 + 2x$

8. Let R be a PID. Then content of the polynomial $a_0 + a_1x + a_2x^2$ over R is
A. $HCF\ (a_0, a_1, a_2)$
B. $LCM(a_0, a_1, a_2)$
C. $\min\ (a_0, a_1, a_2)$
D. $\max\ (a_0, a_1, a_2)$

9. A polynomial $f(x) \in R[x]$, where R is a UFD, is called primitive if
A. Its leading coefficient is 1
B. Its leading coefficient is a unit
C. Its content is 1
D. Its content is a unit

10. True/False Sum of two primitive polynomials is always primitive
A. True
B. False

11. Let R be a UFD. Let $f, g \in R[x]$ be two polynomials of degree 3 each and $c(f) = 3, C(g) = 2$. Then
A. $C(fg) = 5, \deg fg = 6$
B. $C(fg) = 6, \deg fg = 6$
C. $C(fg) = 1, \deg fg = 6$
D. $C(fg) = 6, \deg fg = 3$

12. Let R be a UFD. Let $f, g \in R[x]$ be two polynomials such that $C(fg) = u$

Then u is a unit in R

A. f or g is a primitive polynomial in $R[x]$
B. f and g both are primitive polynomials in $R[x]$
C. Neither f nor g is a primitive polynomial in $R[x]$
D. There is no primitive polynomial in $R[x]$

13. True/False Content of a polynomial over a UFD R always exists
A. True
B. False

14. Which of the following statements is true?
A. If R is a PID then so is $R[x]$
B. If R is a UFD then so is $R[x]$
C. If R is an ED then so is $R[x]$
D. If R is a field then so is $R[x]$

15. $Z[x]$ is a

A. PID
B. ED
C. UFD
D. Field

Answer for Self Assessment

1.	D	2.	B	3.	C	4.	C	5.	B
6.	D	7.	B	8.	A	9.	D	10.	B
11.	C	12.	B	13.	A	14.	B	15.	C

Review Questions

1. Let R be a commutative integral domain with unity that is not a field; show that the polynomial ring $R[x]$ in a variable x is not a PID.
2. Show that the polynomial ring $F[x, y]$ in two variables over a field F is a UFD but not a PID.
3. Let $F[x]$ be polynomial ring over a field F. Show that a non-zero polynomial $f(x) \in F[x]$ is a unit if and only if $f(x) \in F$.
4. Let R be a commutative ring with unity. Show that an element $f(x) \in R[x]$ is a zero divisor if and only if there exists an element $0 \neq b \in R$ such that $bf(x) = 0$.
5. Show that the $n \times n$ matrix ring $(R[x])_n$ over a polynomial ring $R[x]$ is isomorphic to the polynomial ring $R_n[x]$ over the $n \times n$ matrix ring R_n.

Further Readings

- Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress
- Topics in algebra by I.N. Hartstein, Wiley
- Abstract algebra by David S Dummit and Richard M Foote, Wiley

Weblinks

- https://nptel.ac.in/courses/111/102/111102009/
- https://nptel.ac.in/courses/111/105/111105112/#

Unit 03: Vector Spaces and Subspaces

CONTENTS

Objectives

After studying this unit, you will be able to

- generalize the concept of vectors done in vector analysis and geometry in such a way that it is no more restricted to two or three dimensions,
- understand the concept of vector space and study its properties,
- define subspace and understand it with the help of examples,
- define linear dependent and linear independent set of vectors,
- define basis and dimension of a vector space,
- find standard basis and dimension of some vector spaces,
- find the basis and dimension of a subspace generated by a given set of vectors,
- extend an L. I. set to a basis of vector space.

Introduction

In this unit, you will be introduced to vector spaces and subspaces. Several important results related to these structures will be explained. Linear dependence and Independence of vectors are defined and explained with the help of examples. The concept of basis and dimension will be elaborated. Results regarding extension of a linearly independent set to a basis and reduction of a spanning set to a basis are proved.

3.1 Vector Spaces

Definition 3.1.1: Let V be a non-empty set and D is a division ring. Consider a binary operation $\oplus$ on V and a mapping '$\cdot$' from $D \times V \to V$ such that for each element $\alpha \in D$, $v \in V$, there is a unique element $\alpha \cdot v \in V$.

Then V is called a left vector space over D if it satisfies the following axioms

1. $(V, \oplus)$ is an abelian group
2. For all $\alpha, \beta \in D$, $x, y \in V$, we have

i. $\alpha \cdot (x \oplus y) = \alpha \cdot x \oplus \alpha \cdot y$

ii. $(\alpha + \beta) \cdot x = \alpha \cdot x \oplus \beta \cdot x$

iii. $(\alpha\beta) \cdot x = \alpha \cdot (\beta \cdot x)$

iv. $1 \cdot x = x$

Remarks 3.1.2: The map '$\cdot$' is called scalar multiplication.

- Elements of V are called vectors.
- Elements of D are called scalars.
- By defining scalar multiplication as $v \cdot \alpha$, we get the right vector space.
- For the sake of convenience, we will write $+$ in place of $\oplus$ and αv in place of $\alpha \cdot v$
- In case, D is a field then by defining $v \cdot \alpha$ as $\alpha \cdot v$, we get that V is both left as well as right vector space. Then we call V is a vector space over the field D.

$v \cdot \alpha$ as $\alpha \cdot v$, we get that
space over the field D.

Examples 3.1.3: For any field F, let $V = \{(\alpha, \beta) \mid \alpha, \beta \in F\}$

Then V is a vector space over F under vector addition given by

$$(\alpha_1, \beta_1) + (\alpha_2, \beta_2) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2)$$

and scalar multiplication is given by

$$\alpha(\alpha_1, \beta_1) = (\alpha\alpha_1, \alpha\beta_1)$$

where $\alpha, \alpha_1, \alpha_2, \beta_1, \beta_2 \in F$

V is generally denoted as F^2.

Proof: Consider $(\alpha_1, \beta_1), (\alpha_2, \beta_2) \in V$

$\alpha_1, \alpha_2, \beta_1, \beta_2 \in F$

$(F, +)$ is always closed. This implies, $\alpha_1 + \alpha_2, \beta_1 + \beta_2 \in F$ so that $(\alpha_1 + \alpha_2, \beta_1 + \beta_2) \in V$

That is, $(\alpha_1, \beta_1) + (\alpha_2, \beta_2) \in V$

So, $(V, +)$ is **closed.**

Again, consider $(\alpha_1, \beta_1), (\alpha_2, \beta_2), (\alpha_3, \beta_3) \in V$

Then $\big((\alpha_1, \beta_1) + (\alpha_2, \beta_2)\big) + (\alpha_3, \beta_3) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2) + (\alpha_3, \beta_3)$

$$= ((\alpha_1 + \alpha_2) + \alpha_3, (\beta_1 + \beta_2) + \beta_3)$$

$$= \big(\alpha_1 + (\alpha_2 + \alpha_3), \beta_1 + (\beta_2 + \beta_3)\big)$$

$$= (\alpha_1, \beta_1) + (\alpha_2 + \alpha_3, \beta_2 + \beta_3)$$

$$= (\alpha_1, \beta_1) + \big((\alpha_2, \beta_2) + (\alpha_3, \beta_3)\big)$$

So, $(V, +)$ is **associative.**

$0 \in F$ so that $(0, 0) \in V$

For $(\alpha, \beta) \in V, \alpha, \beta \in F$ and thus $\alpha + 0 = \alpha, \beta = \beta + 0$

That is, $(\alpha, \beta) + (0, 0) = (\alpha, \beta) = (0, 0) + (\alpha, \beta)$

Hence $(0, 0)$ is **the additive identity of V.**

For $(\alpha, \beta) \in V, \alpha, \beta \in F$, implies $-\alpha, -\beta \in F$

Also, $(\alpha, \beta) + (-\alpha, -\beta) = \big(\alpha + (-\alpha), \beta + (-\beta)\big) = (0, 0)$

Again, $(-\alpha, -\beta) + (\alpha, \beta) = \big((-\alpha) + \alpha, (-\beta) + \beta\big) = (0, 0)$

That is, $-(\alpha, \beta) = (-\alpha, -\beta)$

Hence every element of V **has an additive inverse in V.**

Consider $(\alpha_1, \beta_1), (\alpha_2, \beta_2) \in V$

Since $\alpha_1, \beta_1, \alpha_2, \beta_2 \in F, \alpha_1 + \alpha_2 = \alpha_2 + \alpha_1$ and $\beta_1 + \beta_2 = \beta_2 + \beta_1$

So that $(\alpha_1, \beta_1) + (\alpha_2, \beta_2) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2) = (\alpha_2 + \alpha_1, \beta_2 + \beta_1) = (\alpha_2, \beta_2) + (\alpha_1, \beta_1)$

V is abelian.

Let $\alpha \in F, (\alpha_1, \beta_1), (\alpha_2, \beta_2) \in V$

Consider

$$\begin{aligned} \alpha((\alpha_1, \beta_1) + (\alpha_2, \beta_2)) &= \alpha(\alpha_1 + \alpha_2, \beta_1 + \beta_2) \\ &= (\alpha(\alpha_1 + \alpha_2), \alpha(\beta_1 + \beta_2)) \\ &= (\alpha\alpha_1 + \alpha\alpha_2, \alpha\beta_1 + \alpha\beta_2) \\ &= (\alpha\alpha_1, \alpha\beta_1) + (\alpha\alpha_2, \alpha\beta_2) \\ &= \alpha(\alpha_1, \beta_1) + \alpha(\alpha_2, \beta_2) \end{aligned}$$

Again, consider

$$\begin{aligned} (\alpha + \beta)(\alpha_1, \beta_1) &= ((\alpha + \beta)\alpha_1, (\alpha + \beta)\beta_1) \\ &= (\alpha\alpha_1 + \beta\alpha_1, \alpha\beta_1 + \beta\beta_1) \\ &= \alpha(\alpha_1, \beta_1) + \beta(\alpha_1, \beta_1) \end{aligned}$$

Consider

$$\begin{aligned} (\alpha\beta)(\alpha_1, \beta_1) &= ((\alpha\beta)\alpha_1, (\alpha\beta)\beta_1) \\ &= (\alpha(\beta\alpha_1), \alpha(\beta\beta_1)) \\ &= \alpha(\beta\alpha_1, \beta\beta_1) \\ &= \alpha(\beta(\alpha_1, \beta_1)) \end{aligned}$$

Now $1 \in F$

$$1(\alpha_1, \beta_1) = (1\alpha_1, 1\beta_1) = (\alpha_1, \beta_1)$$

Thus, $V = F^2$ is a vector space over F.

Example 3.1.4: For any field F and any positive integer n, the set of all n-tuples $(\alpha_1, \alpha_2, \ldots, \alpha_n)$; $\alpha_i \in F$ is a vector space under the addition and scalar multiplication defined by

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) + (\beta_1, \beta_2, \ldots, \beta_n) = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots, \alpha_n + \beta_n)$$

and

$$c(\alpha_1, \alpha_2, \ldots, \alpha_n) = (c\alpha_1, c\alpha_2, \ldots, c\alpha_n)$$

where $c \in F$, $\alpha_i, \beta_i \in F \ \forall \ 1 \leq i \leq n$.

Example 3.1.5: The set V of polynomials in one variable x over a field F is a vector space under usual addition of polynomials and for any

$$\alpha \in F, f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n \in V,$$

scalar multiplication defined as

$$\alpha(f(x)) = \alpha\alpha_0 + \alpha\alpha_1 x + \cdots + \alpha\alpha_n x^n$$

Example 3.1.6: The set V of matrices of order $n \times m$ with entries from the field of real numbers is a vector space under usual addition and scalar multiplication of matrices given by

$$[a_{ij}] + [b_{ij}] = [a_{ij} + b_{ij}]$$

and

$$c[a_{ij}] = [ca_{ij}]$$

where $c \in \mathbb{R}$, $[a_{ij}], [b_{ij}] \in V$

Note: The last property of vector space may not be true even if all other properties are true.

Example 3.1.7: Consider V= $\{(\alpha, \beta, \gamma) | \alpha, \beta, \gamma \in \mathbb{R}\}$

Define

$$(\alpha_1, \beta_1, \gamma_1) + (\alpha_2, \beta_2, \gamma_2) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2, \gamma_1 + \gamma_2)$$

and

$$\lambda(\alpha, \beta, \gamma) = (\lambda\alpha, \lambda\beta, 0)$$

for all $\lambda, \alpha, \beta, \gamma, \alpha_1, \beta_1, \gamma_1, \alpha_2, \beta_2, \gamma_2 \in \mathbb{R}$.

Note that $1\,(\alpha, \beta, \gamma) = (1\alpha, 1\beta, 0) = (\alpha, \beta, 0) \neq (\alpha, \beta, \gamma)$

Therefore, V is not a vector space over the field of real numbers.

Properties of a Vector Space:

Let V be a vector space over a field F and 0_V and 0_F be the additive identities of V and F respectively. Then for all $\alpha \in F$, $v \in V$

(i) $\alpha 0_V = 0_V$
(ii) $0_F v = 0_V$
(iii) $-v = (-1)v$
(iv) $(-\alpha)v = \alpha(-v) = -(\alpha v)$
(v) If $\alpha v = 0_V$, then $\alpha = 0_F$ or $v = 0_V$

Proof:

(i) $0_V = 0_V + 0_V$

$\alpha 0_V = \alpha\,(0_V + 0_V)$

This implies,

$\alpha 0_V + 0_V = \alpha 0_V + \alpha 0_V$

Using left cancellation law,

$0_V = \alpha 0_V$ or $\alpha 0_V = 0_V$.

(ii) $0_F v = 0_V$

$0_F = 0_F + 0_F$

$0_F v = (0_F + 0_F)v$

$0_F v + 0_V = 0_F v + 0_F v$

$0_V = 0_F v$

Or

$0_F v = 0_V$

(iii) $-v = (-1)v$

$0_F v = (1 + (-1))v$

$= 1v + (-1)v$

$= v + (-1)v$

Similarly,

$0_V = (-1)v + v$

Therefore, $(-1)v = -v$

(iv) $(-\alpha)v = \alpha(-v) = -(\alpha v)$

$0_V = 0_F v$

$= (\alpha + (-\alpha))v$

$= \alpha v + (-1)\alpha v$

So, $(-\alpha)v = -(\alpha v)$ ... (1)

Again, $0_V = \alpha 0_V$

$$= \alpha(v + (-v))$$

$= \alpha v + \alpha(-v)$

From (1),

$$(-\alpha)v = \alpha(-v) = -(\alpha v)$$

(v) If $\alpha v = 0_V$, then $\alpha = 0_F$ or $v = 0_V$

Given that $\alpha v = 0_V$

If $\alpha \neq 0_F$

$\alpha^{-1} \in F$

$\alpha^{-1}(\alpha v) = \alpha^{-1}(0_V)$

$1v = 0_V$

$v = 0_V$

Task:

1. Which is the smallest subspace and how many elements does it contain?
2. Let F be a field. Then prove that F is a vector space over itself.

3.2 Subspaces

Definition 3.2.1: A non-empty subset W of a vector space V_F is called a subspace of V if

1. For any $a, b \in W$, $a + b \in W$
2. For any $a \in W$ and $c \in F$, $ca \in W$

There are at least two subspaces, called trivial subspaces, of a non-zero vector space given by {0} and itself.

Lemma 3.2.2: If W is a subspace of a vector space V_F then W is a subgroup of $< V, + >$ and it is a vector space over the same field F.

Proof: $(W, +)$ is a subgroup of $(V, +)$ if and only if $W \subseteq V$ and $a - b \in W$ for every $a, b \in W$.

$$W \subseteq V$$

For $b \in W$, $-1 \in F$

By property (ii) of definition $(-1)b = -b \in W$

For $a, -b \in W$, by property (i), $a + (-1)b = a - b \in W$

Therefore, W is a subgroup of $(V, +)$.

Also, $(W, +)$ is an abelian group.

Rest all the properties are true by the condition that $W \subseteq V$ and they are defined over the same field.

Therefore, W is a vector space.

Example 3.2.3: Let $V = \{(\alpha, \beta) | \alpha, \beta \in F\}$. Then the subsets $W_1 = \{(\alpha, 0) | \alpha \in F\}$ and $W_2 = \{(0, \alpha) | \alpha \in F\}$ are both subspaces of V.

Solution: $0 \in F \Rightarrow (0,0) \in W_1$

Therefore, $W_1 \neq \phi$

Also, $W_1 \subseteq V$

Let $(\alpha, 0), (\beta, 0) \in W_1$

Then $(\alpha, 0) + (\beta, 0) = (\alpha + \beta, 0) \in W_1$.

Again let $a \in F, (\alpha, 0) \in W_1$

$a(\alpha, 0) = (a\alpha, a0) = (a\alpha, 0) \in W_1$

Hence, W_1 is a subspace of vector space V over F.

Similarly, we can show that W_2 is a subspace of V.

Result 3.2.4: A non-empty subset W of a vector space V_F is a subspace of V if and only if

$$\alpha a + b \in W \ \forall\ a, b \in W \text{ and } \alpha \in F$$

Proof: Let W is a subspace of V.

For all $a \in W, \alpha \in F, \alpha a \in W$

Now $\alpha a, b \in W \Rightarrow \alpha a + b \in W$

Conversely, let $\alpha a + b \in W \ \forall\ \alpha \in F, a, b \in W$

$1 \in F$ so $1a + b = a + b \in W$

Again, $\alpha = -1, b = a$

We get, $(-1)a + a = 0 \in W$

For, $\alpha \in F, a, 0 \in W$

$\alpha a + 0 = \alpha a \in W$

Therefore, W is a subspace of V.

Theorem 3.2.5: Intersection of any family of subspaces of a vector space is again a subspace.

Proof: Let $S = \{W_\alpha | \alpha \in \Lambda\}$ be a family of subspaces of a vector space V over a field F.

Consider

$$W = \bigcap_{\alpha \in \Lambda} W_\alpha$$

W_α is a subspace of $V \ \forall\ \alpha \in \Lambda$,

So, $0 \in W_\alpha \ \forall\ \alpha \in \Lambda$.

$$0 \in \bigcap_{\alpha \in \Lambda} W_\alpha = W$$

Hence $W \neq \phi$

Let $a, b \in W, \alpha \in F$

$a, b \in W = \bigcap_{\alpha \in \Lambda} W_\alpha$

$\Rightarrow a, b \in W_\alpha \ \forall\ \alpha \in \Lambda$

$\Rightarrow \alpha a + b \in W_\alpha \ \forall \alpha \in \wedge$

$\Rightarrow \alpha a + b \in \bigcap_{\alpha \in \wedge} W_\alpha = W$

$\Rightarrow W$ is a subspace of V.

Example 3.2.6: Union of two subspaces of a vector space need not be a subspace

Proof: $V = \{(\alpha, \beta) | \alpha, \beta \in F\}$

$W_1 = \{(\alpha, 0) | \alpha \in F\}$ and $W_2 = \{(0, \alpha) | \alpha \in F\}$ are subspaces of V.

$(1, 0) \in W_1, (0, 1) \in W_2$

$(1, 0), (0, 1) \in W_1 \cup W_2$

$(1, 0) + (0, 1) = (1, 1) \notin W_1 \cup W_2$

This implies, $W_1 \cup W_2$ is not a subspace of V.

Definition 3.2.7: Let $X \subseteq V$; V is a vector space over some field F.

Then a subspace W of V is said to be **spanned by or generated by X** if

1. $X \subseteq W$
2. If W' is a subspace of V containing X then $W \subseteq W'$

We denote $W = \langle X \rangle$.

Elements of spanned subspace: Let V be a vector space and $X = \{x_1, x_2, \ldots, x_n\}$ is a subset of V. Then subspace spanned by X is the set of all vectors of the form $\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n$, $\alpha_i \in F \ \forall 1 \le i \le n$

Proof:

Let W be the set of all elements of the form $\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n$, $\alpha_i \in F \ \forall 1 \le i \le n$

Then we need to prove that $W = \langle X \rangle$

$X = \{x_1, x_2, \ldots, x_n\}$

$W = \{\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n | \alpha_i \in F \ \forall 1 \le i \le n\}$

$0, 1 \in F$

$\alpha_1 = 1, \alpha_i = 0 \ \forall i > 1$

$1x_1 + 0x_2 + \cdots + 0x_n \in W$

That is, $x_1 \in W$

Similarly, we can show that $x_i \in W \ \forall 1 \le i \le n$

That is, $X \subseteq W$

Again, let $\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n, \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n \in W, \alpha \in F$

Consider

$$\alpha(\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n) + (\beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n) = \alpha\alpha_1 x_1 + \alpha\alpha_2 x_2 + \cdots + \alpha\alpha_n x_n + \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n$$

$$= (\alpha\alpha_1 + \beta_1)x_1 + (\alpha\alpha_2 + \beta_2)x_2 + \cdots + (\alpha\alpha_n + \beta_n)x_n$$

Since $\alpha, \alpha_i, \beta_i \in F$

$\alpha\alpha_i + \beta_i \in F \ \forall i$

Hence, $\alpha(\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n) + (\beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n) \in W$

So, W is a subspace of V.

Let W' be a subspace of V containing $\{x_1, x_2, \ldots, x_n\}$

Consider $\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n \in W, \alpha_i \in F \ \forall i$

$x_i \in W' \ \forall i$

$\alpha_i x_i \in W' \ \forall i, \alpha_i \in F$

$$\sum_{i=1}^{n} \alpha_i x_i \in W'$$

That is, $\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n \in W'$

$W \subseteq W'$

Hence, $W = < X >; X = \{x_1, x_2, \ldots, x_n\}$

In case, X is an infinite set then the subspace $W =< X >$ contains elements of the type

$\{\alpha_1 x_1 + \alpha_2 x_2 + \cdots |$all but finitely many α_i's are zero$\}$.

Definition 3.2.8: For any finite number of vectors $x_1, x_2, \ldots, x_n$ in a vector space V_F and scalars $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$, the vector

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n$$

is called a **linear combination** of the vectors $x_1, x_2, \ldots, x_n$.

Definition 3.2.9: For any two subspaces W_1 and W_2 of a vector space V_F, the **sum of two subspaces** W_1 and W_2 is denoted as $W_1 + W_2$ and defined as

$$W_1 + W_2 = \{w_1 + w_2 |\ w_1 \in W_1,\ w_2 \in W_2\}$$

Theorem 3.2.10: For any two subspaces W_1 and W_2 of a vector space V_F, $W_1 + W_2$ is a subspace of V spanned by $W_1 \cup W_2$.

Proof: To prove this result, we need to prove

1. $W_1 \cup W_2 \subseteq W_1 + W_2$
2. $W_1 + W_2$ is a subspace of V
3. If W' is a subspace of V containing $W_1 \cup W_2$, then $W_1 + W_2 \subseteq W'$

let $x \in W_1 \cup W_2$

This implies, $x \in W_1$ or $x \in W_2$

If $x \in W_1, 0 \in W_2$

So that $x = x + 0 \in W_1 + W_2$

Similarly, if $x \in W_2, x \in W_1 + W_2$

This implies, $W_1 \cup W_2 \subseteq W_1 + W_2$

Let $a, b \in W_1 + W_2, \alpha \in F$

$a = a_1 + a_2$ and $b = b_1 + b_2; a_1, b_1 \in W_1$ and $a_2, b_2 \in W_2$

Consider

$$\begin{aligned} \alpha a + b &= \alpha(a_1 + a_2) + (b_1 + b_2) \\ &= (\alpha a_1 + b_1) + (\alpha a_2 + b_2) \end{aligned}$$

Thus

$a_1, b_1 \in W_1, \alpha \in F$

W_1 is a subspace of V.

$\alpha a_1 + b_1 \in W_1$

Similarly, $\alpha a_2 + b_2 \in W_2$

$\alpha a + b = (\alpha a_1 + b_1) + (\alpha a_2 + b_2) \in W_1 + W_2$

Hence, $\alpha a + b \in W_1 + W_2$

$\forall\ a, b \in W_1 + W_2, \alpha \in F$

Therefore, $W_1 + W_2$ is a subspace of V.

Let W' be a subspace of V such that $W_1 \cup W_2 \subseteq W'$

Let $\alpha \in W_1 + W_2$

Then $\alpha = x + y; x \in W_1, y \in W_2$

$x \in W_1 \subseteq W_1 \cup W_2 \subseteq W'$ and $y \in W_2 \subseteq W_1 \cup W_2 \subseteq W'$

$x, y \in W'$ and W' is a subspace of V.

$x + y \in W' \Rightarrow \alpha \in W'$

Therefore, $W_1 + W_2 \subseteq W'$

Hence $W_1 + W_2 = < W_1 \cup W_2 >$

Task:

Let $P_3(R)$ denotes the vector space of polynomials with the degree at the most 3. Then find two subspaces of $P_3(R)$ such that union of both the subspaces is

1. A subspace
2. Not a subspace

3.3 Basis and Dimension of Vector Space

Definition 3.3.1: Let $x_1, x_2, \dots, x_n$ be a finite number of members (not necessarily all distinct) of a vector space V_F.

These vectors are said to be **linearly dependent** if for some scalars $\alpha_1, \alpha_2, \dots, \alpha_n \in F$, with at least one of them non-zero and

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = 0$$

Definition 3.3.2: The vectors $x_1, x_2, \dots, x_n \in V_F$ are said to be linearly independent over the field F if for all $\alpha_i; 1 \leq i \leq n$,

such that

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = 0$$

we get

$$\alpha_i = 0\ \forall\ 1 \leq i \leq n$$

Remarks 3.3.3:Linearly Dependence/ Independence in infinite sets of vectors

Consider the infinite set S of vectors then set S is said to be **Linearly Independent** if and only if all its finite subsets are Linearly Independent.Otherwise, it is called **Linearly Dependent**.

Results 3.3.4:A singleton set $\{x\}$ is linearly dependent if and only if $x = 0$.

Proof: Let the singleton set $\{x\}$ is L. D.

So, there exists non-zero $\alpha \in F$ such that $\alpha x = 0$.

Also, if $\alpha x = 0$, then either $\alpha = 0$ or $x = 0$.

Since, $\alpha \neq 0$, therefore, $x = 0$.

Conversely, consider $x = 0$

Then since we know that $1x = x \forall\ x \in V$

We have, $1 \cdot 0 = 0$ and $1 \neq 0$.

So, there exist non-zero $\alpha \in F$, such that $\alpha 0 = 0$

This implies, {0} is L. D.

A set containing an L. D. set is L. D.

Let $S = \{x_1, x_2, \ldots, x_n\}$ and $T = \{x_1, x_2, \ldots, x_l\}$ such that $l > n$ and S is L.D.

Then $S \subseteq T$. Since S is L. D. therefore, there exists $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ (not all zero) such that

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = 0$$

We can also write,

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n + 0x_{n+1} + \cdots + 0x_l = 0$$

which implies that T is L. D.

The subset of an L. I. set is L. I.

Let $S = \{x_1, x_2, \ldots, x_n\}$ and $T = \{x_1, x_2, \ldots, x_l\}$ such that $l > n$ and T is L.I.

If possible, let Sbe L. D.

Then by the result that a set containing an L. D. set is always L. D., we get that T is L. D.

which is contradictory to the fact that T is L. I.

Therefore, our assumption was wrong.

That is, S is L. I.

A set containing 0 is always linearly dependent.

Let S be a set containing 0.

That is, $\{0\} \subseteq S$

Singleton set {0} is L. D. and a set containing an L. D. set is always L. D.

Therefore, we get that S is L. D.

Example 3.3.5: The set $\{(1, 0), (0, 1)\}$ in the vector space $V = \{(x, y) | x, y \in \mathbb{R}\}$ is linearly independent over the field of real numbers.

Let $\alpha, \beta \in \mathbb{R}$ such that $\boldsymbol{\alpha}(\mathbf{1}, \mathbf{0}) + \boldsymbol{\beta}(\mathbf{0}, \mathbf{1}) = (\mathbf{0}, \mathbf{0})$

That is, $(\alpha, \beta) = (0, 0)$

$\Rightarrow \ \boldsymbol{\alpha} = \mathbf{0}, \boldsymbol{\beta} = \mathbf{0}$

This implies, $\{(1, 0), (0, 1)\}$ is L. I.

Theorem 3.3.6: If $v_1, v_2, \ldots, v_n$ are L. I. in a vector space V_F, then each element of the subspace W spanned by them is expressible uniquely as a linear combination of $v_1, v_2, \ldots, v_n$.

Proof: If possible, let $v \in W$ can be expressed as

$$v = \sum_{i=1}^{n} \alpha_i v_i = \sum_{i=1}^{n} \beta_i v_i$$

for $\alpha_i, \beta_i \in F \ \forall i$

This implies,

$$\sum_{i=1}^{n} \alpha_i v_i - \sum_{i=1}^{n} \beta_i v_i = 0$$

That is,

$$\sum_{i=1}^{n} (\alpha_i - \beta_i) v_i = 0$$

Since$v_1, v_2, \ldots, v_n$ are L. I. therefore,

$$\alpha_i - \beta_i = 0 \ \forall i$$

That is,

$$\alpha_i = \beta_i \; \forall i$$

This proves the uniqueness of expression.

Theorem 3.3.7: Let $u_1, u_2, \dots, u_n$ be any n L. I. vectors in a vector space V_F. Any $n+1$ vectors $v_1, v_2, \dots, v_{n+1}$, each of which is a linear combination of $u_1, u_2, \dots, u_n$ are L. D.

Proof: If $v_i = 0$ for some i, then the vectors $v_1, v_2, \dots, v_{n+1}$ are L.D. So, without loss of generality, we may assume that $v_i \neq 0$ for all i.

We prove the result by using Induction on n.

For $n = 1$, consider u_1; v_1 and v_2 are two vectors which is a linear combination of u_1.

Then there exist $\alpha_1, \alpha_2 \in F$, for which

$v_1 = \alpha_1 u_1$ and $v_2 = \alpha_2 u_1$

Then since $v_1, v_2 \neq 0$, therefore, $\alpha_1, \alpha_2 \neq 0$

Consider $\alpha_2 v_1 - \alpha_1 v_2 = \alpha_2 \alpha_1 u_1 - \alpha_1 \alpha_2 u_1 = 0$

Thus, v_1 and v_2 are linearly dependent.

So, the result is true for $n = 1$.

Suppose that the result holds for any $k(< n)$ linearly independent vectors.

Now we prove the result for n linearly independent vectors.

Then there exist $\alpha_{ij} \in F$.

$$v_1 = \alpha_{11} u_1 + \alpha_{12} u_2 + \cdots + \alpha_{1n} u_n$$
$$v_2 = \alpha_{21} u_1 + \alpha_{22} u_2 + \cdots + \alpha_{2n} u_n$$
$$\dots \quad \dots \quad \dots \quad \dots \quad \dots$$
$$\dots \quad \dots \quad \dots \quad \dots \quad \dots$$
$$v_{n+1} = \alpha_{n+1,1} u_1 + \alpha_{n+1,2} u_2 + \cdots + \alpha_{n+1,n} u_n \quad \dots (1)$$

If $\alpha_{in} = 0$ for all $1 \leq i \leq n+1$, then each v_i is a linear combination of $n-1$ vectors,

then by the induction hypothesis, we get that $v_1, v_2, \dots, v_n$ and hence $v_1, v_2, \dots, v_{n+1}$ are L.D.

Now we suppose that $\alpha_{in} \neq 0$ for some i.

We assume that $\alpha_{1n} \neq 0$

Multiplying the equation $v_1 = \alpha_{11} u_1 + \alpha_{12} u_2 + \cdots + \alpha_{1n} u_n$

with $\alpha_{2n} \alpha_{1n}^{-1}$ and subtracting from each equation in the system (1), we get for each $2 \leq i \leq n+1$,

$$w_i = v_i - \alpha_{in} \alpha_{1n}^{-1} v_1 = \sum_{1 \leq j \leq n-1} (\alpha_{ij} - \alpha_{in} \alpha_{1j} \alpha_{1n}^{-1}) u_j$$

So, by the induction hypothesis, w_i, $2 \leq i \leq n+1$ are L. D.

Therefore, there exist $\beta_2, \beta_3, \dots, \beta_{n+1} \in F$, not all zero, such that

$$\sum_{i=2}^{n+1} \beta_i w_i = 0$$

This implies,

$$\sum_{i=2}^{n+1} \beta_i (v_i - \alpha_{in} \alpha_{1n}^{-1} v_1) = 0$$

This implies that $v_1, v_2, \dots, v_{n+1}$ are L. D.

So, by the Principle of Mathematical Induction, the result is true for all n.

Corollary 3.3.8: If $\{v_1, v_2, \dots, v_n\}$ is a linearly independent subset of a vector space V_F then any subset W of V having more than n vectors each of which can be expressed as a linear combination of $v_1, v_2, \dots, v_n$ must be L.D.

Proof: Since W contains more than n elements. Choose a subset W_1 of W consisting of $n+1$ elements.

Then W_1 is a set consisting of $n+1$ elements, all of which are linear combinations of n vectors $v_1, v_2, \dots, v_n$. By theorem, W_1 is L. D. and hence W is L. D.

Definition 3.3.9: A subset B of a vector space V_F is called a basis of V if

1. B is linearly independent
2. B spans V

A vector space V is called finitely generated if it has a finite subset that spans V.

Lemma 3.3.10: If $S = \{x_1, x_2, \dots, x_n\}$ is a linearly dependent set of non-zero vectors in V_F, then for some $2 \le i \le n$, x_i is a linear combination of its predecessors $x_1, x_2, \dots, x_{i-1}$ and the subspace spanned by S is same as the subspace spanned by $S - \{x_i\}$.

Proof: Since the set S is L.D., therefore, there exist $\alpha_i \in F\ \forall\ 1 \le i \le n$, such that at least one $\alpha_i \neq 0$ and

$$\sum_{j=1}^{n} \alpha_j x_j = 0 \dots (1)$$

Let i be the largest suffix such that $\alpha_i \neq 0$. That is, $\alpha_j = 0\ \forall\ j > i$.

So, (1) implies,

$$\sum_{j=1}^{i} \alpha_j x_j = 0 \dots (2)$$

This implies,

$$x_i = \sum_{j=1}^{i-1} -\alpha_i^{-1}\alpha_j x_j = \sum_{j=1}^{i-1} \beta_j x_j \dots (3) \quad \text{where } \beta_j = -\alpha_i^{-1}\alpha_j\ \forall\ 1 \le j \le i-1$$

This proves that x_i is a linear combination of its predecessors $x_1, x_2, \dots, x_{i-1}$.

Again, let W be the subspace of V spanned by elements of S.

For any $x \in W$, there exist $\gamma_j \in F$, $1 \le j \le n$, such that

$$x = \sum_{j=1}^{n} \gamma_j x_j$$

$$\sum_{j=1}^{n} \gamma_j x_j = \sum_{j \neq i} \gamma_j x_j + \gamma_i x_i$$

$$= \sum_{j \neq i} \gamma_j x_j + \gamma_i \sum_{j=1}^{i-1} \beta_j x_j \quad (from\ (3))$$

$$= \sum_{j=1}^{i-1} (\gamma_j + \gamma_i \beta_j) x_j + \sum_{j=i+1}^{n} \gamma_j x_j$$

which is a linear combination of elements of $S - \{x_i\}$, which proves the second part of the lemma.

Theorem 3.3.11: Let V_F be a finitely generated vector space. Then V_F has a finite basis and any two bases of V_F have the same number of vectors.

Proof: Since V_F is a finitely generated vector space therefore, there exists a finite subset $B = \{x_1, x_2, \dots, x_n\}$ which spans V. Without loss of generality, we may assume that $0 \notin$ B.

If B is linearly independent, then B is the basis of V.

If B is linearly dependent, then by lemma, we may choose some x_i in B such that x_i can be expressed as a linear combination of its preceding elements and $B_1 = B - \{x_i\}$ spans V.

If B_1 is linearly independent, then B_1 is the basis of V.

If B_1 is linearly dependent, then by lemma, we may choose some x_j in B_1 such that x_j can be expressed as a linear combination of its preceding elements and $B_2 = B_1 - \{x_j\}$ spans V.

Since the number of vectors in B is finite, therefore, this process can not continue after at the most $n-1$ steps.

At the most, we will be left with a set containing only one element which is non-zero and hence linearly independent.

Thus, we will get a basis of V.

Suppose B′ is another basis of V_F having m elements

Let $m > n$.

Each element of V and hence B′ is a linear combination of elements of B and B is linearly independent.

Therefore, B′has to be L. D. but B′ being basis is L. I.

So, we arrive at a contradiction.

That is, $m \leq n$.

Also, B' is a basis of V implies that each element of V and hence B is a linear combination of elements of B' and B' is linearly independent.

If $m < n$, then B is L. D. but B being a basis is *L. I.*

This implies $m = n$ which proves that two bases of a vector space have the same number of elements.

Remarks 3.3.12: Number of elements in a basis of a vector space V_F is called the dimension of V.

- If the dimension of a vector space, $V = n$, then any set containing more than n elements is L. D.
- If the dimension of a vector space, $V = n$, then an L.I. set containing n elements is a basis of V.

Theorem 3.3.13: If $\{u_1, u_2, \dots, u_k\}$ is an L. I. subset of a finite-dimensional vector space V_F, then it can be extended to a basis of V.

Proof: Let $\dim V = n$.

Then any $n+1$ vectors in V are L. D. Hence, $k \leq n$.

Let $\{w_1, w_2, \dots, w_n\}$ is a basis of V. Consider the set $S = \{u_1, u_2, \dots, u_k, w_1, w_2, \dots w_n\}$. Since S contains more than n elements, therefore, S is L. D.

Hence, there exist some elements in S, which can be expressed as a linear combination of its proceeding elements.

If possible, let that element is u_i for some $1 \leq i \leq k$. Then there exist $\beta_j \in F$, $1 \leq j \leq i-1$ such that

$$u_i = \sum_{j=1}^{i-1} \beta_j u_j$$

which proves that the set $\{u_1, u_2, \dots, u_i\}$ and hence $\{u_1, u_2, \dots, u_n\}$ is L. D.

But the set $\{u_1, u_2, \dots, u_n\}$ is L. I.

Therefore, the element which can be expressed as a linear combination of its proceeding elements is w_j for some $1 \leq j \leq n$. Also, $S - \{w_j\}$ spans V.

If $S - \{w_j\}$ is L.I. then it is the required basis. Otherwise, we continue the process until we get an L.I. set.At the most, after eliminating $n-k$ elements, we will get a subset of S containing with n elements which is the same as dim V.

Since the eliminated elements are all from the set $\{w_1, w_2, \dots w_n\}$ therefore, the set obtained by eliminating $n-k$ elements is the basis containing the set $\{u_1, u_2, \dots, u_k\}$.

Corollary 3.3.14: If dimension V = n, then any set S containing less than n elements, subspace spanned by S is a proper subset of V.

Corollary 3.3.15:For any subspace W of a finite-dimensional vector space V_F, dim $W \le$ dim V. Further, $W = V$ if and only if dim $W =$ dim V.

Proof: Let dim $V = n$.

Since V cannot contain an L. I. set having more than n vectors, W cannot have any L.I. subset containing more than n elements.

So, we can find L.I. subset $B = \{y_1, y_2, \dots, y_m\}$ of W containing the maximum number, say m, of elements.

Then $m \le n$ and any $m+1$ vectors in W are L. D.

Therefore, for some $y \in W$, $y_1, y_2, \dots, y_m$, y is L. D.

So, there exists $\beta_1, \beta_{2,\dots}, \beta_m$, $\beta \in F$ (not all zero) such that

$$\sum_{j=1}^{m} \beta_j y_j + \beta y = 0$$

If $\beta = 0$, then we get,

$$\sum_{j=1}^{m} \beta_j y_j = 0$$

Since B is L. I. therefore, we get that $\beta_j = 0 \;\forall\, j$

which is a contradiction to the fact that $\beta_1, \beta_{2,\dots}, \beta_m$, β are not all zero.

So, $\beta \ne 0$.

This implies,

$$y = \sum_{1 \le j \le m} -\beta^{-1} \beta_j y_j$$

That is B spans W.

Now, if B contains n elements then B is an L.I. subset of V containing n elements where $n =$dim V. This implies that B is a basis of V.

Hence, span $(B) = V = W$.

Conversely, if V = W, then trivially dim V = dim W.

Theorem 3.3.16:If U and W are subspaces of a finite-dimensional vector space V_F, then

$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$$

Proof:

Let $\dim U = r, \dim W = s$ and $\dim(U \cap W) = t$

Let $\{e_1, e_2, \dots, e_t\}$ be a basis of $U \cap W$.

Since $U \cap W$ is a subspace of U, we can extend the above basis to a basis $\{e_1, \dots, e_t, g_1, \dots, g_{s-t}\}$ of W and a basis $\{e_1, \dots, e_t, f_1, \dots, f_{r-t}\}$ of U.

Let $B = \{e_1, \dots, e_t, f_1, \dots, f_{r-t}, g_1, \dots, g_{s-t}\}$.

We claim that B is the basis of $U + W$.

Let $x \in U + W$

Then $x = u + w; u \in U, w \in W$

Since $u \in U$ and $\{e_1, \dots, e_t, f_1, \dots, f_{r-t}\}$ is a basis of U.

So, there exist $\alpha_i, \beta_j \in F$, such that

$$u = \sum_{i=1}^{t} \alpha_i e_i + \sum_{j=1}^{r-t} \beta_j f_j$$

Again, $w \in W$ and $\{e_1, \dots, e_t, g_1, \dots, g_{s-t}\}$ is a basis of W.

So, there exist $\gamma_i, \delta_j \in F$, such that

$$w = \sum_{i=1}^{t} \gamma_i e_i + \sum_{j=1}^{s-t} \delta_j g_j$$

Adding these equations, we get,

$$x = u + w = \sum_{i=1}^{t} (\alpha_i + \gamma_i) e_i + \sum_{j=1}^{r-t} \beta_j f_j + \sum_{j=1}^{s-t} \delta_j g_j$$

So, every $x \in U + W$ is a linear combination of elements of B.

That is B spans $U + W$.

Now, we prove that B is linearly independent.

Let $\alpha_i, \beta_j, \gamma_k \in F$ such that

$$\sum_{i=1}^{t} \alpha_i e_i + \sum_{j=1}^{r-t} \beta_j f_j + \sum_{k=1}^{s-t} \gamma_k g_k = 0$$

$$\Rightarrow \sum_{i=1}^{t} \alpha_i e_i + \sum_{j=1}^{r-t} \beta_j f_j = -\sum_{k=1}^{s-t} \gamma_k g_k \dots \text{ (1)}$$

Therefore,

$$\sum_{i=1}^{t} \alpha_i e_i + \sum_{j=1}^{r-t} \beta_j f_j, \sum_{k=1}^{s-t} \gamma_k g_k \in U \cap W$$

But $U \cap W$ has the basis $\{e_1, e_2, \dots, e_t\}$

Therefore,

$$\sum_{k=1}^{s-t} \gamma_k g_k = \sum_{i=1}^{t} \delta_i g_i$$

That is,

$$\sum_{k=1}^{s-t} \gamma_k g_k - \sum_{i=1}^{t} \delta_i g_i = 0$$

Since the left side is a linear combination of elements of basis, therefore, we get, $\gamma_k = 0 \ \forall\ k$

Putting in (1), we get,

$$\sum_{i=1}^{t} \alpha_i e_i + \sum_{j=1}^{r-t} \beta_j f_j = 0$$

Now again it is a linear combination of elements of a basis, which implies,

$$\alpha_i = \beta_j = 0 \ \forall\ i, j$$

This implies that B is $L.I.$

Hence, B is a basis of $U + W$.

$$\begin{aligned} dim(U + W) &= r + s - t \\ &= dim\, U + dim\, W - dim\, U \cap W \end{aligned}$$

Theorem 3.3.17: If U and W are subspaces of a finite-dimensional vector space V_F, then

$$\dim(U+W) = \dim U + \dim W - \dim(U \cap W)$$

Proof:

Let $\dim U = r, \dim W = s$ and $\dim(U \cap W) = t$

Let $B' = \{e_1, e_2, \ldots, e_t\}$ be a basis of $U \cap W$.

Since $U \cap W$ is a subspace of U as well as W, we can extend the above basis to bases $B_U = \{e_1, \ldots, e_t, f_1, \ldots, f_{r-t}\}$ of U and $B_W = \{e_1, \ldots, e_t, g_1, \ldots, g_{s-t}\}$ of W.

Let $B = \{e_1, \ldots, e_t, f_1, \ldots, f_{r-t}, g_1, \ldots, g_{s-t}\}$.

We claim that B is the basis of U + W.

Let $x \in U + W$

Then $x = u + w; u \in U, w \in W$

Since $u \in U$ and $B_U = \{e_1, \ldots, e_t, f_1, \ldots, f_{r-t}\}$ is a basis of U.

So, for $1 \le i \le t$, $1 \le j \le r-t$, there exist α_i, $\beta_j \in F$, such that

$$u = \sum_{i=1}^{t} \alpha_i e_i + \sum_{j=1}^{r-t} \beta_j f_j$$

Again, $w \in W$ and $B_W = \{e_1, \ldots, e_t, g_1, \ldots, g_{s-t}\}$ is a basis of W.

So, for $1 \le i \le t$, $1 \le j \le s-t$, there exist γ_i, $\delta_j \in F$, such that

$$w = \sum_{i=1}^{t} \gamma_i e_i + \sum_{j=1}^{s-t} \delta_j g_j$$

Adding these equations, we get,

$$x = u + w = \sum_{i=1}^{t} (\alpha_i + \gamma_i) e_i + \sum_{j=1}^{r-t} \beta_j f_j + \sum_{j=1}^{s-t} \delta_j g_j$$

So, every $x \in U + W$ is a linear combination of elements of B.

That is B spans $U + W$.

Now, we prove that B is linearly independent.

For $1 \le i \le t$, $1 \le j \le r-t$, $1 \le k \le s-t$, let $\alpha_i, \beta_j, \gamma_k \in F$ such that

$$\sum_{i=1}^{t} \alpha_i e_i + \sum_{j=1}^{r-t} \beta_j f_j + \sum_{k=1}^{s-t} \gamma_k g_k = 0$$

$$\Rightarrow \sum_{i=1}^{t} \alpha_i e_i + \sum_{j=1}^{r-t} \beta_j f_j = -\sum_{k=1}^{s-t} \gamma_k g_k \quad \ldots. (1)$$

Therefore,

$$\sum_{k=1}^{s-t} \gamma_k g_k \in U \cap W$$

But $U \cap W$ has the basis $B' = \{e_1, e_2, \ldots, e_t\}$

Therefore,

$$\sum_{k=1}^{s-t} \gamma_k g_k = \sum_{i=1}^{t} \delta_i e_i$$

That is,

$$\sum_{k=1}^{s-t} \gamma_k g_k - \sum_{i=1}^{t} \delta_i e_i = 0$$

Since the left side is a linear combination of elements of the basis B_W, therefore, we get, $\gamma_k = 0 \; \forall \; 1 \leq k \leq s-t$.

Putting in equation (1), we get,

$$\sum_{i=1}^{t} \alpha_i e_i + \sum_{j=1}^{r-t} \beta_j f_j = 0$$

Now again it is a linear combination of elements of a basis B_U, which implies,

$$\alpha_i = \beta_j = 0 \; \forall \; i, j$$

This implies that B is L. I.

Hence, B is a basis of $U + W$.

$$dim(U+W) = r + s - t$$
$$= dim\, U + dim\, W - dim\, U \cap W$$

Example 3.3.18: The set B = {(1, 0), (0,1)} is a basis of vector space $\mathbb{R}^2$ over ℝ.

First, we prove that the set B is L.I.

Let $\alpha, \beta \in \mathbb{R}$ such that $\boldsymbol{\alpha(1,0) + \beta(0,1) = (0,0)}$

That is, $(\alpha, \beta) = (0, 0)$

$\Rightarrow \boldsymbol{\alpha = 0, \beta = 0}$

This implies the set B is L. I.

Next, we prove that B generates $\mathbb{R}^2$.

Let $(x, y) \in \mathbb{R}^2$

Then we can observe that $(x, y) = x(1,0) + y(0,1)$

That is, every element in $\mathbb{R}^2$ is expressible as a linear combination of elements of B.

This proves that B is the basis of $\mathbb{R}^2$.

Note:

The basis of a vector space over a field is not unique but there is a unique standard basis for vector space.

Standard Basis: The set $B = \{(1, 0), (0,1)\}$ is called the standard basis of $\mathbb{R}^2$ and hence Dim $(\mathbb{R}^2) = 2$.

The set $B = \{e_1, e_2, e_3, \ldots, e_n\}$ is standard basis of F^n; where F is any field and e_i is n −tuple with ith coordinate equal to 1 and all others 0.

For example, $e_1 = (1, 0, 0, \ldots, 0)$, $e_2 = (0, 1, 0 \ldots, 0) \ldots$

So, for any field F, Dim $(F^n) = n$.

- Let $V = F[x] = \{a_0 + a_1 x + a_2 x^2 + \cdots | a_i \in F\}$ be the vector space of all polynomials over a field F in indeterminate x, then the V has infinite basis and its standard basis is given by $\{1, x, x^2, \ldots\}$. Thus, V is infinite-dimensional.
- Let $V = P_3 = \{a_0 + a_1 x + a_2 x^2 + a_3 x^3 | a_i \in F\}$ be the vector space of all polynomials of degree less than or equal to 3, over a field F in indeterminate x, then the standard basis of V is $\{1, x, x^2, x^3\}$. Therefore, Dim $(P_3) = 4$.
- Let $V = M_{2\times2}(\mathbb{R})$, then the standard basis of V is given by $\left\{\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}, \begin{bmatrix}0 & 1\\0 & 0\end{bmatrix}, \begin{bmatrix}0 & 0\\1 & 0\end{bmatrix}, \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}\right\}$. Hence, Dim $(M_{2\times2}) = 4$

Dimension: For any field F, Dim $(F^n) = n$.

- Dim $(P_n) = n + 1$

- Dim $(M_{m\times n}) = m\cdot n$
- Dim $(\{0\}) = 0$
- The vector space of all polynomials over a field F in indeterminate x is infinite-dimensional.

Example 3.3.19: Find the basis and dimension of the vector space V of symmetric matrices of order 2over the field of real numbers

Consider the set

$$B = \left\{\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}, \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}, \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}\right\}$$

First, we prove that B is L.I.

Let $\alpha,\beta,\gamma \in \mathbb{R}$ such that

$$\alpha\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix} + \beta\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix} + \gamma\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix} = \begin{bmatrix}0 & 0\\0 & 0\end{bmatrix}$$

$$\Rightarrow \begin{bmatrix}\alpha & \beta\\\beta & \gamma\end{bmatrix} = \begin{bmatrix}0 & 0\\0 & 0\end{bmatrix}$$

$$\Rightarrow \alpha = \beta = \gamma = 0$$

This implies, B is L.I.

Now, let $\begin{bmatrix}a & b\\b & c\end{bmatrix} \in V$

Then $\begin{bmatrix}a & b\\b & c\end{bmatrix} = a\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix} + b\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix} + c\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}$

This implies each element of V is a linear combination of elements of B. Hence B is a basis of V.

Finding a basis: Let $V = \mathbb{R}^3$. Find a basis of the subspace W of V generated by the vectors $x_1 = (1,\ 1,\ 0)$, $x_2 = (0,\ 1,\ 1)$, $x_3 = (2,\ 3,\ 1)$ and $x_4 = (1,\ 1,\ 1)$

Since Dim $(\mathbb{R}^3)$= 3. Therefore, the set $\{x_1, x_2, x_3, x_4\}$ is L. D.

Now we need to form a relation $\alpha_1x_1 + \alpha_2x_2 + \alpha_3x_3 + \alpha_4x_4 = 0$ such that $\alpha_i \in F\ \forall i$ and $\alpha_i's$ are not all zero.

That is,

$$\alpha_1(1,1,0) + \alpha_2(0,1,1) + \alpha_3(2,3,1) + \alpha_4(1,1,1) = (0,\ 0,\ 0)$$

$$(\alpha_1 + 2\alpha_3 + \alpha_4, \alpha_1 + \alpha_2 + 3\alpha_3 + \alpha_4, \alpha_2 + a_3 + \alpha_4) = (0,0,0)$$

So, we get a system of equations,

$$\alpha_1 + 2\alpha_3 + \alpha_4 = 0$$

$$\alpha_1 + \alpha_2 + 3\alpha_3 + \alpha_4 = 0$$

$$\alpha_2 + a_3 + \alpha_4 = 0$$

Equivalently,

$$\begin{bmatrix}1 & 0 & 2 & 1\\1 & 1 & 3 & 1\\0 & 1 & 1 & 1\end{bmatrix}\begin{bmatrix}\alpha_1\\\alpha_2\\\alpha_3\\\alpha_4\end{bmatrix} = \begin{bmatrix}0\\0\\0\end{bmatrix}$$

Now we apply row reduction on the matrix

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

Applying $R_2 - R_1$, we get,

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

Applying $R_3 - R_2$,

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

System of linear equations becomes,

$$\begin{bmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

That is,

$$\alpha_1 + 2\alpha_3 + \alpha_4 = 0$$

$$\alpha_2 + \alpha_3 = 0, \alpha_4 = 0$$

This implies,

$$\alpha_1 = -2\alpha_3 , \alpha_2 = -\alpha_3, \alpha_4 = 0$$

So, $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (-2t, -t, t, 0);\ t = \alpha_3$

Therefore, the basis of the subspace W is given by $\{(-2,\ -1,\ 1,\ 0)\}$ and Dim (W) = 1.

Extension of an L.I. set to a basis: Let $x_1 = (0,\ 1,\ 0)$ and $x_2 = (-2,\ 0,\ 1)$. Extend the set $\{x_1, x_2\}$ to a basis of $\mathbb{R}^3$.

First, we check that the given vectors are L. I.

Let $\alpha,\ \beta \in \mathbb{R}$ such that $\alpha(0,1,0) + \beta(-2,0,1) = (0,0,0)$

This implies, $(0, \alpha, 0) + (-2\beta, 0, \beta) = (0,0,0)$

$$\Rightarrow (-2\beta, \alpha, \beta) = (0,0,0)$$

$$\Rightarrow \alpha = \beta = 0$$

So, the given vectors are L. I.

Since an L.I. set containing the same number of elements as the dimension of the vector space is always a basis so next, we try to find a vector $x_3 \in \mathbb{R}^3$ such that $\{x_1, x_2, x_3\}$ is an L. I. set.

Consider the set $B = \{(0,\ 1,\ 0),\ (-2,\ 0,\ 1), (1,\ 0,\ 0)\}$

Let $\alpha, \beta, \gamma \in \mathbb{R}$ such that

$$\alpha(0,1,0) + \beta(-2,0,1) + \gamma(1,0,0) = (0,0,0)$$

$$\Rightarrow\ (0, \alpha, 0) + (-2\beta, 0, \beta) + (\gamma, 0,0) = (0,0,0)$$

$$\Rightarrow (-2\beta + \gamma, \alpha, \beta) = (0,0,0)$$

$$\Rightarrow \alpha = \beta = \gamma = 0$$

Therefore, B is L. I. set and hence the required basis of $\mathbb{R}^3$.

Summary

- The concept of vectors done in vector analysis and geometry in such a way that it is no more restricted to two or three dimensions is generalized.
- The concept of vector space and its properties are explained.
- Subspace is defined.
- linear dependent and linear independent set of vectors are defined.
- The basis and dimension of a vector spaceare defined, and related results are proved.
- The standard basis and dimension of some vector spaces are found.
- The basis and dimension of a subspace generated by a given set of vectors is explained.
- An L. I. set to a basis of vector space is extended to a basis.

Keywords

- Vector Space
- Subspace
- Linear dependence and independence of vectors
- Basis and dimension
- Standard basis
- Extension and reduction theorem of basis

Self Assessment

1. Let V be a vector space over a field F. Then which of the following options are incorrect?
A. V is a group under addition of vectors.
B. V is abelian under addition
C. V is a commutative group under multiplication
D. $cx \in V$ for every $c \in F, x \in V$

2. Minimum number of elements in a vector space are
A. 0
B. 1
C. 2
D. 3

3. Which of the following is a vector space over the field of real numbers?
A. Set of all rational numbers
B. Set of all irrational numbers
C. Set of all matrices
D. Set of all square matrices of order 2

4. Let V= R^3. Then which of the following is a subspace of V?
A. $\{(x, y, z)|z = 1\}$
B. $\{(x, y, z)|z = x^2\}$
C. $\{(x, y, z)|x + y + z = 0\}$
D. $\{(x, y, z)|y = x + 1\}$

5. Let V be the set of all polynomials over the set of real numbers. Then which of the following is a subspace of V
A. Set of all polynomials with degree equal to 3.
B. Set of all polynomials with degree less than or equal to 3.
C. Set of all polynomials with degree greater than 3.
D. Set of all polynomials with degree greater than or equal to 3.

6. Which of the following is NOT a subspace of vector space of square matrices of order n
A. All upper triangular matrices of order n
B. All non-singular matrices of order n
C. All symmetric matrices of order n
D. All matrices of order n with trace 0

7. Which of the following set is linearly independent in R^3.
A. {(1, 0, 0), (0,0, 1), (0, 1, 0), (1, 1, 0)}
B. {(1, 0, 0), (0,0, 1), (1, 1, 0)}
C. {(1, 0, 0), (2, 0, 0)}
D. {(1, 0, 0), (0, 1, 0), (1, 1, 0)}

8. Which of the following sets is linearly dependent always?

A. ϕ (Empty set)
B. {0}
C. {3}
D. None of the above

9. Let S = $\{2 - x + 3x^2, x + x^2, 1 - 2x^2\}$ be a subset of vector space V of all the polynomials with degree less than or equal to 2. Then
A. S is linearly dependent.
B. S is linearly independent.
C. S contains a linearly dependent set.
D. Every set containing Sis linearly independent.

10. Let V be a vector space over a field F such that dim V= n and W be its proper subspace such that dim W= m. Then which of the following is NOT correct?
A. Any basis of W can be extended to a basis of V.
B. Any non-zero singleton set in W can be extended to a basis of V.
C. Corresponding to every basis B of W, we can find a basis C of V such that C contains B.
D. $m > n$

11. Let S be a generating set of a vector space V with dim V= 10. Then the number of elements in S is
A. ≤ 10
B. $= 10$
C. ≥ 10
D. > 10

12. The dimension of the subspace of vector space of square matrices of order 2, spanned by the set S where S= $\{\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}\}$ is

A. 1
B. 2
C. 3
D. 4

13. The dimension of vector space of symmetric matrices of order n is given by
A. $n(n+1)$
B. $n(n-1)$
C. $n(n+1)/2$
D. $n(n-1)/2$

14. The dimension of vector space of all the polynomials of degree less than or equal to 3 with $f(0) = 0$ is
A. 4
B. 3
C. 2
D. 1

15. Let S= $\{2 - x + 3x^2, x + x^2, 1 - 2x^2\}$ be a subset of vector space V of all the polynomials with degree less than or equal to 2. Then
A. S is linearly dependent.
B. S is linearly independent but L(S) ≠ V.
C. L(S)= V but S is not Linearly independent.
D. S is a basis of V.

Answers for Self Assessment

1.	C	2.	B	3.	D	4.	C	5.	B
6.	B	7.	B	8.	B	9.	B	10.	D
11.	C	12.	B	13.	C	14.	B	15.	D

Review Questions

1. Let F be a field. Consider the three sets A, B and C such that
   (i) $A = \{(x_1, x_2); x_1 \leq x_2\}$
   (ii) $B = \{(x_1, x_2) | x_1 x_2 \geq 0\}$
   (iii) $C = \{(x_1, x_2) | x_1 = x_2\}$

Which of these are subspaces of F^2? Give reasons?

2. Let V be the vector space of functions from R into R. Let V_e be the subset of V containing all the even functions f such that $f(x) = f(-x) \; \forall \; x \in V$. Let V_0 be the subset of odd functions that is, $f(-x) = -f(x)$. Then
   (i) Prove that V_e and V_0 are subspaces of V.
   (ii) Prove that $V_e + V_0 = V$
   (iii) Prove that $V_e \cap V_o = \{0\}$
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.
5. Prove that the set of vectors containing null vector is always linearly dependent.

Further Readings

- Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress
- Topics in algebra by I.N. Hartstein, Wiley
- Abstract algebra by David S Dummit and Richard M Foote, Wiley

Weblinks

- https://nptel.ac.in/courses/111/102/111102009/
- https://nptel.ac.in/courses/111/105/111105112/#

Unit 04: Linear Transformations

CONTENTS

Objective

After studying this unit, you will be able to

- define linear transformations from a vector space to another vector space over the same field
- understand linear transformations with the help of examples
- find the matrix of a linear transformation
- define null space and range space of a linear transformation
- find null space and range space of a linear transformation
- state and prove Rank Nullity theorem
- observe the similarity between matrices corresponding to two different sets of bases

Introduction

In this unit, you will be introduced to linear transformations from a vector space V to a vector space W, where W my or may not be equal to V. Various examples will be given to elaborate the concept. The matrix of a linear transformation with respect to a given basis will be found. Null space and Range space of the linear transformation will be defined, and related results will be explained. The Rank-Nullity theorem will be stated and proved. It will be observed that matrices corresponding to two different sets of bases are similar.

4.1 Linear Transformation

Definition 4.1.1: Let U and V be two vector spaces over a field F. A mapping $T: U \to V$ is called a linear transformation if it satisfies the following properties

1. $T(x+y) = T(x) + T(y)$
2. $T(\alpha x) = \alpha T(x)$

for all $x, y \in U$ and $\alpha \in F$.

Theorem 4.1.2: Let U and V be two vector spaces over a field F. A mapping $T: U \to V$ is a linear transformation if and only if $T(\alpha x + \beta y) = \alpha T(x) + \beta T(y)\ \forall\ \alpha, \beta \in F; x, y \in U$

Proof: Let $T: U \to V$ is a linear transformation.

Consider $\alpha, \beta \in F; x, y \in U$; then by the definition of vector space, $\alpha x, \beta y \in U$

Then by property (1) of the definition of a linear transformation, we have,

$$T(\alpha x + \beta y) = T(\alpha x) + T(\beta y) \ldots (1)$$

Using property (2) of the definition of a linear transformation, we have,

$$T(\alpha x) = \alpha T(x), T(\beta x) = \beta T(x) \ldots (2)$$

Using equations (1) and (2), we get,

$$T(\alpha x + \beta y) = \alpha T(x) + \beta T(y)$$

for all $\alpha, \beta \in F,\ x, y \in U$.

Conversely, let $T(\alpha x + \beta y) = \alpha T(x) + \beta T(y)$

for all $\alpha, \beta \in F,\ x, y \in U$.

Since $1 \in F$, Taking $\alpha = \beta = 1$, we get that,

$$T(x + y) = T(x) + T(y)\ \forall x, y \in U$$

Also, $0 \in F$, Taking $\beta = 0$, we get that,

$$T(\alpha x) = \alpha T(x)\ \forall \alpha \in F, x \in U$$

Hence, T is a linear transformation.

Example 4.1.3:

Let U and V be two vector spaces over a field F. Then the zero-mapping defined as $T(x) = 0\ \forall x \in U$ is a linear transformation.

Proof: Let $x, y \in U$ and $\alpha, \beta \in F$

Then $T(\alpha x + \beta y) = 0$

Also, $\alpha T(x) + \beta T(y) = \alpha \cdot 0 + \beta \cdot 0 = 0$

This implies, $T(\alpha x + \beta y) = \alpha T(x) + \beta T(y)\ \forall x, y \in U; \alpha, \beta \in F$

Hence, T is a linear transformation.

Example 4.1.4:

Let U be a vector space over a field F. Then the identity mapping defined as $T(x) = x\ \forall x \in U$ is a linear transformation.

Proof: Let $x, y \in U$ and $\alpha, \beta \in F$

Then $T(\alpha x + \beta y) = \alpha x + \beta y = \alpha T(x) + \beta T(y)$

This implies, $T(\alpha x + \beta y) = \alpha T(x) + \beta T(y)\ \forall x, y \in U; \alpha, \beta \in F$

Hence, T is a linear transformation.

Example 4.1.5:

Let $V = F[x]$. Then for any polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, the mapping defined as $T(f(x)) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$ is a linear transformation.

Proof: Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ and $g(x) = b_0 + b_1 x + \cdots + b_m x^m \in F[x]$ and $\alpha, \beta \in F$

Without loss of generality let $n \leq m$.

Then

$$T(\alpha f(x) + \beta g(x)) = T((\alpha a_0 + \beta b_0) + (\alpha a_1 + \beta b_1)x + \cdots + (\alpha a_n + \beta b_n)x^n + \beta b_{n+1} x^{n+1} + \cdots + \beta b_m x^m)$$

$$= (\alpha a_1 + \beta b_1) + \cdots + (\alpha a_n + \beta b_n) n x^{n-1} + \beta (n+1) b_{n+1} x^n + \cdots + \beta m b_m x^{m-1}$$

Also,

$$T(\alpha f(x)) + T(\beta g(x)) = T(\alpha a_0 + \alpha a_1 x + \cdots + \alpha a_n x^n) + T(\beta b_0 + \beta b_1 x + \cdots + \beta b_m x^m)$$
$$= \alpha a_1 + \cdots + (\alpha a_n) n x^{n-1} + \beta b_1 + \cdots + \beta b_n + \beta\,(n+1) b_{n+1} x^n + \cdots + \beta m b_n x^{m-1}$$
$$= (\alpha a_1 + \beta b_1) + \cdots + (\alpha a_n + \beta b_n) n x^{n-1} + \beta\,(n+1) b_{n+1} x^n + \cdots + \beta m b_m x^{m-1}$$
$$= T(\alpha f(x) + \beta g(x))$$

Hence, $T$is a linear transformation.

Example 4.1.6:

For any field F, consider the map $T: F^3 \to F^2$ given by $T(\alpha, \beta, \gamma) = (\alpha, \beta)$ is a linear transformation.

Let $x = (\alpha_1, \beta_1, \gamma_1), y = (\alpha_2, \beta_2, \gamma_2) \in F^3; \alpha, \beta \in F$

Consider

$$T(\alpha x + \beta y) = T\big(\alpha(\alpha_1, \beta_1, \gamma_1) + \beta(\alpha_2, \beta_2, \gamma_2)\big)$$
$$= T(\alpha\alpha_1 + \beta\alpha_2, \alpha\beta_1 + \beta\beta_2, \alpha\gamma_1 + \beta\gamma_2)$$
$$= (\alpha\alpha_1 + \beta\alpha_2, \alpha\beta_1 + \beta\beta_2)$$

Also,

$$\alpha T(x) + \beta T(y) = \alpha T(\alpha_1, \beta_1, \gamma_1) + \beta T(\alpha_2, \beta_2, \gamma_2)$$
$$= \alpha(\alpha_1, \beta_1) + \beta(\alpha_2, \beta_2)$$
$$= (\alpha\alpha_1 + \beta\alpha_2, \alpha\beta_1 + \beta\beta_2)$$
$$= T(\alpha x + \beta y)$$

Therefore, T is a linear transformation.

Example 4.1.7:

Let C denote the field of complex numbers. Then C is a vector space over itself. Define $T: C \to C$ as $T(x + iy) = x$. Then T is not a linear transformation.

Consider $\alpha = 2 + i$, $x = 2 - i \in C$

Then $(2 + i)\,T(2 - i) = (2 + i)\,2 = 4 + 2i$

and $T\big((2 + i)(2 - i)\big) = T(5) = 5$

So, $\alpha T(x) \neq T(\alpha x)$

Therefore, T is not linear transformation.

Properties 4.1.8: Let U and V be two vector spaces over a field F. Let $T: U \to V$ is a linear transformation. Denote additive identity of U as 0_U and additive identity of V as 0_V. Then

1. $T(0_U) = 0_V$

Proof: Since $T$is a linear transformation, therefore,

$T(\alpha x + \beta y) = \alpha T(x) + \beta T(y)$ for every $\alpha, \beta \in F, x, y \in U$

Taking $x = y = 0_U$, $\alpha = \beta = 1$, we get,

$T(0_U + 0_U) = T(0_U) + T(0_U)$

$\Rightarrow T(0_U) = T(0_U) + T(0_U)$

$\Rightarrow T(0_U) + 0_V = T(0_U) + T(0_U)$

$\Rightarrow T(0_U) = 0_V$

2. $T(-x) = -T(x)\ \forall\, x \in U$

Proof: $T(\alpha x + \beta y) = \alpha T(x) + \beta T(y) \forall\, \alpha, \beta \in F, x, y \in U$

Let $\alpha = -1$ and $\beta = 0$, we get that

$T((-1)x + 0y) = -1\,T(x) + 0\,T(y)$

This implies,

$T(-x) = -T(x)$

3. $T(x - y) = T(x) - T(y)\ \forall\, x \in U$

Proof: $T(\alpha x + \beta y) = \alpha T(x) + \beta T(y) \forall\, \alpha, \beta \in F, x, y \in U$

Let $\alpha = 1$ and $\beta = -1$, we get that

$T(1 \cdot x + (-1)y) = 1 \cdot T(x) + (-1)\,T(y)$

This implies, $T(x - y) = T(x) - T(y)$

4. If $u_1, u_2, \dots, u_n$ are L. D. vectors in U then $T(u_1), T(u_2), \dots, T(u_n)$ are L. D. in V.

Proof: Since $u_1, u_2, \dots, u_n$ are L. D. therefore, there exist $\alpha_1, \alpha_2 \dots, \alpha_n \in F$, not all zero such that

$\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n = 0_U$

$\Rightarrow T(\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n) = T(0_U)$

$\Rightarrow\ \alpha_1 T(u_1) + \alpha_2 T(u_2) + \cdots + \alpha_n T(u_n) = 0_V$

Since $\alpha_1, \alpha_2 \dots, \alpha_n \in F$ are not all zero, therefore, we get that the vectors $T(u_1), T(u_2), \dots, T(u_n)$ are L. D. in V.

Task:

1. In two-dimension space V_2, consider the transformation
$$T(x, y) = (x\cos\theta - y\sin\theta,\ \ x\sin\theta + y\cos\theta)$$
Check whether T is a linear transformation or not?
2. Give an example of a linear transformation that is neither one-one nor onto.

4.2 Re-presentation of Transformations by Matrices

Definition 4.2.1: Let V_F be a vector space of finite dimension n. Then any ordered $n-$ tuple $(x_1, x_2, \dots, x_n)$ of n members of V_F is called an ordered basis of V_F if the set $\{x_1, x_2, \dots, x_n\}$ is a basis of V_F.

In an ordered basis, the order of arrangement of members of the basis is also considered.

For example, the sets $\{(1,\ 0),\ (0,\ 1)\}$ and $\{(0,1),\ (1,\ 0)\}$ are two distinct ordered bases of $\mathbb{R}^2_{\mathbb{R}}$.

Definition 4.2.2: Now we define how we find the matrix of any r –tuple $(y_1, y_2, \dots, y_r)$ of vectors in a vector space V_F with respect to some ordered basis $B = \{x_1, x_2, \dots, x_n\}$ of V_F.

Since $B = \{x_1, x_2, \dots, x_n\}$ is a basis of V_F, therefore, each element of V_F is uniquely expressible as a linear combination of elements of B.

Also, $y_j \in V_F\ \forall\, 1 \le j \le r$

So, there exist unique $\alpha_{ij} \in F\,;\, 1 \le i \le n,\ 1 \le j \le r$ such that

$$y_j = \sum_{i=1}^{n} \alpha_{ij}\, x_i$$

The column vector $(\alpha_{1j}, \alpha_{2j}, \dots, \alpha_{nj})'$ is called coordinate vector associated with y_j.

Thus, we get $n \times r$ matrix over F given by

$$\alpha_{ij}] = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1r} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2r} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nr} \end{bmatrix}$$

We call this matrix, the matrix of $(y_1, y_2, \dots, y_r)$ relative to or with respect to the ordered basis $B = \{x_1, x_2, \dots, x_n\}$.

Theorem 4.2.3: Let $\{x_1, x_2, \dots, x_n\}$ is an ordered basis of V_F and $(y_1, y_2, \dots, y_n)$ is an ordered $n-$tuples of elements of V_F. Then $\{y_1, y_2, \dots, y_n\}$ is an ordered basis of V_F if and only if the matrix of $(y_1, y_2, \dots, y_n)$ relative to the basis $\{x_1, x_2, \dots, x_n\}$ is non-singular.

Proof: Let (α_{ij}) be the matrix of $(y_1, y_2, \dots, y_n)$ relative to the basis $\{x_1, x_2, \dots, x_n\}$.

Then by definition

$$y_j = \sum_{i=1}^{n} \alpha_{ij} x_i \,;\, 1 \le j \le n \dots (1)$$

Let $\{y_1, y_2, \dots, y_n\}$ is an ordered basis of V_F and let (β_{ij}) be the matrix of $(x_1, x_2, \dots, x_n)$ relative to the basis $\{y_1, y_2, \dots, y_n\}$ so that

$$x_i = \sum_{k=1}^{n} \beta_{ki} y_k \,;\, 1 \le i \le n \dots (2)$$

From (1) and (2), we get,

$$x_i = \sum_{k=1}^{n} \beta_{ki} \left(\sum_{l=1}^{n} \alpha_{lk} x_l \right)$$

$$= \sum_{l=1}^{n} \left(\sum_{k=1}^{n} \alpha_{lk} \beta_{ki} \right) x_l$$

However,

$$x_i = \sum_{l=1}^{n} \delta_{li} x_l \,;$$

where $\delta_{li} = 0 \ \forall\ l \ne i,\ \delta_{ii} = 1 \ \forall\ i$

Therefore,

$$\sum_{l=1}^{n} \delta_{li} x_l = \sum_{l=1}^{n} \left(\sum_{k=1}^{n} \alpha_{lk} \beta_{ki} \right) x_l$$

This gives us,

$$\delta_{li} = \sum_{k=1}^{n} \alpha_{lk} \beta_{ki}$$

So that $(\delta_{li}) = (\alpha_{ij})(\beta_{ij})$

That is, $(\alpha_{ij})(\beta_{ij}) = I$

Similarly, we can show that

$$(\beta_{ij})(\alpha_{ij}) = I$$

Hence, the matrix (α_{ij}) is non-singular.

Conversely,

Let (α_{ij}) is non-singular and $(\beta_{ij}) = (\alpha_{ij})^{-1}$. Then for any $1 \le i \le n$,

$$\sum_{j=1}^{n} \beta_{ji} y_j = \sum_{j=1}^{n} \beta_{ji} \left(\sum_{k=1}^{n} \alpha_{kj} x_k \right)$$

$$= \sum_{k=1}^{n} \left(\sum_{j=1}^{n} \alpha_{kj} \beta_{ji} \right) x_k = x_i$$

Hence each $x_i \in W$; where W is a subspace of V_F spanned by elements $\{y_1, y_2, \dots, y_n\}$.

So, $\{y_1, y_2, \ldots, y_n\}$ is a basis of V_F.

Hence $(y_1, y_2, \ldots, y_n)$ is an ordered basis of V_F.

Example 4.2.4: Consider a field F, we know that F^3 is a vector space over F. Consider $f_1 = (1, 0, 0)$, $f_2 = (1, \alpha, 0)$, $f_3 = (1, \alpha, \beta)$ where $\alpha, \beta \in F - \{0\}$. Then

1. Find the matrix of (f_1, f_2, f_3) relative to a standard ordered basis of F^3.
2. Prove that $\{f_1, f_2, f_3\}$ is a basis for F^3.
3. Find the matrix of standard basis relative to the ordered basis $\{f_1, f_2, f_3\}$.

Solution: Standard basis of F^3 is given by $\{e_1, e_2, e_3\}$ where $e_1 = (1,0,0)$, $e_2 = (0,1,0)$, $e_3 = (0,0,1)$.

1. $f_1 = (1,\ 0,\ 0) = e_1 = 1\, e_1 + 0\, e_2 + 0\, e_3$

$$f_2 = (1,\ \alpha,\ 0) = 1\, e_1 + \alpha\, e_2 + 0\, e_3$$

$$f_3 = (1,\ \alpha,\ \beta) = 1\, e_1 + \alpha\, e_2 + \beta e_3$$

So that the matrix of (f_1, f_2, f_3) relative to standard ordered basis of F^3 is given by

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & \alpha & \alpha \\ 0 & 0 & \beta \end{bmatrix}$$

2. Since the matrix of (f_1, f_2, f_3) relative to standard ordered basis of F^3 is given by

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

Given that α, β are non-zero elements of a field and a field is always without proper zero divisors.

The determinant of this matrix is $\alpha\beta \neq 0$, which proves that the matrix A is non-singular.

Hence $\{f_1, f_2, f_3\}$ is a basis for F^3

3. In this case, matrix of standard basis relative to the ordered basis $\{f_1, f_2, f_3\}$ is given by A^{-1}.

Note that

For any $(x,\ y,\ z) \in F^3$

Since $\{f_1, f_2, f_3\}$ is a basis of F^3, therefore, there exist $a, b, c \in F$ such that $(x, y,\ z) = af_1 + bf_2 + cf_3$

That is, $(x, y, z) = a(1,0,0) + b(1, \alpha, 0) + c(1, \alpha, \beta)$

$\Rightarrow (x, y, z) = (a, 0, 0) + (b, b\alpha, 0) + (c, c\alpha, c\beta)$

$\Rightarrow (x, y, z) = (a + b + c, b\alpha + c\alpha, c\beta)$

which implies,

$z = c\beta;\ c = z\beta^{-1}$

$y = (b + c)\alpha;\ b = y\alpha^{-1} - z\beta^{-1}$

$x = a + b + c;\ a = x - y\alpha^{-1}$

Using these we get, $e_1 = (1,\ 0,\ 0) = 1f_1 + 0f_2 + 0f_3$

$$e_2 = (0,\ 1,\ 0) = -\alpha^{-1} f_1 + \alpha^{-1} f_2 + 0 f_3$$

$$e_3 = (0,\ 0,\ 1) = 0f_1 - \beta^{-1} f_2 + \beta^{-1} f_3$$

so that the matrix of standard basis relative to the ordered basis $\{f_1, f_2, f_3\}$ is given by

$$\begin{bmatrix} 1 & -\alpha^{-1} & 0 \\ 0 & \alpha^{-1} & -\beta^{-1} \\ 0 & 0 & \beta^{-1} \end{bmatrix}$$

Note:

Let V and W be two finite-dimensional vector spaces over the same field F.

Let $T: V \to W$ be a linear transformation. Let $\dim V = n$. Consider the basis $\{x_1, x_2, \dots, x_n\}$ of V.

Then T can be uniquely determined from $T(x_1), T(x_2), \dots, T(x_n)$.

Matrix of Linear Transformation: Let V and W be two finite-dimensional vector spaces over the same field F. $T: V \to W$ be a linear transformation. Let $\dim V = n$ and $\dim W = m$.

Consider the bases $B = \{x_1, x_2, \dots, x_n\}$ and $B' = \{y_1, y_2, \dots y_m\}$ of V and W respectively.

Then for any $x \in V$, we have seen that $T(x)$ can be uniquely determined from $T(x_1), T(x_2), \dots, T(x_n)$.

So, we find $T(x_1), T(x_2), \dots, T(x_n)$.

Also, $T(x_i) \in W \; \forall i$ and B' is a basis of W.

So, there exist unique $\alpha_{ji} \in F$ such that

$$T(x_i) = \sum_{j=1}^{m} \alpha_{ji} y_j;\; 1 \le i \le n$$

Then the matrix (α_{ij}) is called the matrix of T with respect to the bases B and B'; It is denoted as $[T, B; B']$.

Note:

The matrix of a linear transformation depends on the bases. Corresponding to a pair of bases, the matrix is unique. Uniqueness follows from the fact that every element of a vector space is uniquely expressed as a linear combination of elements of its basis. In case, $T: V \to V$; we call T is a linear operator on V. Then for any basis B of V; the matrix of T is denoted as $[T; B]$ or $[T]_B$. Let $T: V \to W$ be a linear transformation. If $\dim V = n$ and $\dim W = m$ then a matrix of T is of order $m \times n$.

Example 4.2.5: Consider the derivative map from P_3 to P_2; that is,

$T: P_3 \to P_2$ is given by $T(a_0 + a_1 x + a_2 x^2 + a_3 x^3) = a_1 + 2a_2 x + 3a_3 x^2$.

Find the matrix of $[T, B; B']$ where B and B' are standard bases of P_3 and P_2 respectively.

$B = \{1, x, x^2, x^3\}$ and $B' = \{1, x, x^2\}$

$$T(1) = 0 = 0 \cdot 1 + 0 \cdot x + 0 \cdot x^2$$

$$T(x) = 1 = 1 \cdot 1 + 0 \cdot x + 0 \cdot x^2$$

$$T(x^2) = 2x = 0 \cdot 1 + 2 \cdot x + 0 \cdot x^2$$

$$T(x^3) = 3x^2 = 0 \cdot 1 + 0 \cdot x + 3 \cdot x^2$$

$$[T, B; B'] = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}$$

Remark 4.2.6: For any linear transformation T from $\mathbb{R}^n \to \mathbb{R}^m$; we can always find a matrix A such that $T(x) = Ax \; \forall x \in \mathbb{R}^n$. Consider the standard bases $B = \{e_1, e_2, \dots, e_n\}$ and $B' = \{e'_1, e'_2, \dots, e'_m\}$ of $\mathbb{R}^n$ and $\mathbb{R}^m$ respectively. Then the matrix A is the matrix with $i-th$ column equal to $T(e_i)$.

Example 4.2.7: Let $T: \mathbb{R}^2 \to \mathbb{R}^2$ be a linear transformation such that $T(1, 1) = (1, 2)$ and $T(0, -1) = (3, 2)$.

Find the transformation T and matrix A of T such that $T(x) = Ax \; \forall x \in \mathbb{R}^2$.

Consider $B = \{(1, 1), (0, -1)\}$

Note that $\begin{vmatrix} 1 & 0 \\ 1 & -1 \end{vmatrix} = -1 \neq 0$

Also, B contains 2 elements. Therefore, B is a basis of R^2.

$$B = \{(1, 1), (0, -1)\}$$

$$T(1,\ 1) = (1,\ 2)$$

$$T(0,\ -1) = (3,\ 2)$$

For $(x,\ y) \in R^2$

$$(x,\ y) = a(1,1) + b(0,\ -1)$$
$$= (a,\ a-b)$$

That is, $a = x,\ a - b = y\ \Rightarrow b = x - y$

$$(x,\ y) = x(1,1) + (x-y)(0,\ -1)$$
$$T(x,\ y) = x\,T(1,1) + (x-y)\,T(0,\ -1)$$
$$= x(1,\ 2) + (x-y)(3,\ 2)$$
$$= (x + 3x - 3y,\ 2x + 2x - 2y)$$
$$= (4x - 3y,\ 4x - 2y)$$

So,

$$T(1,\ 0) = (4,\ 4) = 4(1,0) + 4(0,\ 1)$$
$$T(0,\ 1) = (-3,\ -2) = -3\ (1,\ 0) - 2(0,\ 1)$$

Hence, $A = \begin{bmatrix} 4 & -3 \\ 4 & -2 \end{bmatrix}$

Remark 4.2.8: Let V and W be two finite-dimensional vector spaces over the same field ℝ.

$T: V \to W$ be a linear transformation. Let dim $V = n$ and dim $W = m$

Then every element $x \in V$, there exist unique scalars $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{R}$ such that

$$x = \sum_{i=1}^{n} \alpha_i x_i$$

Associating each $x \in V$ with the vector $(\alpha_1, \alpha_2, \ldots, \alpha_n)$, we see that V can be mapped to $\mathbb{R}^n$. Similarly, W can be mapped to $\mathbb{R}^n$ and hence T can be associated with a unique linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^n$.

Task:

1. If T and U are two linear operators on R^2 defined by $T(x,y) = (y,x)$ and $U(x,y) = (x,0)$. Then find the matrix of T with respect to the standard basis of R^2. Further, find the matrix of U with respect to the basis $\{(1,2),(2,1)\}$.
2. Let T be the unique linear operator on C^3 for which $T(1,0,0) = (1,0,i), T(0,1,0) = (0,1,1), T(0,0,1) = (i,1,0)$. Is T invertible?

Let T be the unique linear operator on C^3 for which

$Te_1 = (1, 0, i),\ Te_2 = (0, 1, 1,)\ Te_3 = (i, 1, 0).$

Is T invertible?

4.3 Rank-Nullity Theorem

Definition 4.3.1: Let U and V be two vector spaces over a field F.

Let $T: U \to V$ is a linear transformation.

Then the kernel of T $(Ker\ T)$ is defined by

$$Ker\ T = \{x \in U \mid T(x) = 0\}$$

Kernel T is also known as null space of T.

Theorem 4.3.2: Let U and V be two vector spaces over a field F. Let $T: U \to V$ is a linear transformation. Kernel T is a subspace of U.

Note that $T(0) = 0$

Therefore, $0 \in Ker\ T$

That is, $Ker\ T$ is a non-empty subset of U.

Let $x, y \in \ker T,\ \alpha \in F$

Since $x, y \in \ker T$, therefore, $T(x) = T(y) = 0$

Also, $T(x + y) = T(x) + T(y) - 0 + 0 - 0$

and $T(\alpha x) = \alpha T(x) = \alpha 0 = 0$

This implies $x + y, \alpha x \in Ker\ T$ for all $x, y \in \ker T,\ \alpha \in F$

Hence, $Ker\ T$ is a subspace of U.

Definition 4.3.3: Let U and V be two vector spaces over a field F.

Let $T: U \to V$ is a linear transformation.

Then range space of T is given by $R = \{T(x)|x \in U\}$

Theorem 4.3.4: Let U and V be two vector spaces over a field F. Let $T: U \to V$ is a linear transformation. $R =$ $Range$ space of T is a subspace of V.

Note that $T(0) = 0$

Therefore, $0 \in R$

That is, R is a non-empty subset of V.

Let $x,\ y \in R,\ \alpha \in F$

Since $x,\ y \in R$, so there exist $x_1, y_1 \in U$ such that

$x = T(x_1)$ and $y = T(y_1)$

Then $x + y = T(x_1) + T(y_1) = T(x_1 + y_1) \in R$

and $\alpha x = \alpha T(x_1) = T(\alpha x_1) \in R$

Hence R is a subspace of V.

Remarks 4.3.5: Let U and V be two finite-dimensional vector spaces over a field F.

Let $T: U \to V$ is a linear transformation.

Then

- $Ker\ T$, being subspace of U is finite-dimensional. So, $Ker\ T$ has a basis. Dimension of $Ker\ T$ is called nullity of T and it is denoted as $\nu(T)$.
- $R =$Range T, being subspace of V is finite-dimensional. So, R has a basis. Dimension of R is called the rank of T and it is denoted as $\rho(T)$.
- Range T is a subspace of V implies $\dim R \leq \dim V$.

Similarly, $Ker\ T$ is a subspace of U implies $\dim(Ker\ T) \leq \dim U$.

Theorem 4.3.6: Let U and V be two finite-dimensional vector spaces over a field F. Let $T: U \to V$ is a linear transformation.

Then $Ker\ T = \{0\}$ if and only if T is a one-one map.

Proof: Let $Ker\ T = \{0\}$

Let $x,\ y \in U$ such that $T(x) = T(y)$

This implies, $T(x) - T(y) = 0$

$$\Rightarrow T(x - y) = 0$$

$\Rightarrow x - y \in \ker T$

But $Ker\ T = \{0\}$

Therefore, $x - y = 0$

$\Rightarrow x = y$

$\Rightarrow T$ is one-one.

Conversely,

Let T is one-one.

Let $x \in Ker\, T$

$\Rightarrow T(x) = 0$

But $T(0) = 0$

$\Rightarrow T(x) = T(0)$

Since T is one-one, therefore, we get, $x = 0$.

That is, $Ker\, T = \{0\}$

Theorem (Rank- Nullity Theorem) 4.3.7: Let U and V be two finite-dimensional vector spaces over a field F. Let $T: U \to V$ is a linear transformation. Then dim $U = \nu T + \rho T$.

Proof: Let dim $U = n$, $\nu(T) = t, \rho(T) = s$

Let $B = \{u_1, u_2, \ldots, u_t\}$ be a basis of $Ker\, T$. Then B is a linearly independent subset of U and hence, it can be extended to a basis of U.

Let $B' = \{u_1, u_2, \ldots, u_n\}$ is the basis of U obtained by extending B.

Claim: The set $S = \{T(u_{t+1}), T(u_{t+2}), \ldots, T(u_n)\}$ is a basis of R.

Let $y \in R$. Then by definition of range space, there exists $x \in U$ such that $y = T(x)$.

Now, $x \in U$ and B' is a basis of U. So, there exist unique $\alpha_i; 1 \le i \le n$ such that

$$x = \sum_{i=1}^{n} \alpha_i u_i$$

so that,

$$T(x) = T\left(\sum_{i=1}^{n} \alpha_i u_i\right)$$

$$= T\left(\sum_{i=1}^{t} \alpha_i u_i + \sum_{i=t+1}^{n} \alpha_i u_i\right)$$

$$= \sum_{i=1}^{t} \alpha_i T(u_i) + \sum_{i=t+1}^{n} \alpha_i T(u_i)$$

$$= \sum_{i=t+1}^{n} \alpha_i T(u_i)$$

That is, every element of R is a linear combination of elements of S. Hence S spans R.

Now we prove that S is linearly independent

Let $\alpha_{t+1}, \alpha_{t+2,\ldots,}\alpha_n \in F$ such that

$$\sum_{i=t+1}^{n} \alpha_i T(u_i) = 0$$

$$\Rightarrow T\left(\sum_{i=t+1}^{n} \alpha_i u_i\right) = 0$$

$$\Rightarrow \sum_{i=t+1}^{n} \alpha_i u_i \in Ker\, T$$

Since B is a basis of $Ker\, T$, so, there exist $\beta_1, \beta_2, \ldots, \beta_t \in F$ such that

$$\sum_{i=t+1}^{n} \alpha_i u_i = \sum_{i=1}^{t} \beta_i u_i$$

That is,

$$\sum_{i=1}^{n} \gamma_i u_i = 0$$

where $\gamma_i = \alpha_i \; \forall \; t+1 \leq i \leq n$ and $\gamma_i = -\beta_i \; \forall \; 1 \leq i \leq t$

This is a linear combination of elements of basis B' of U, hence $\gamma_i = 0 \; \forall \; i$

That is, $\alpha_i = 0 \; \forall i$. This implies S is linearly independent.

Hence, S is a basis of R.

$\rho(T)$ =Number of elements in $S = n - t$

$$= \dim U - \nu(T)$$

That is, $\dim U = \nu(T) + \rho(T)$.

Corollary4.3.8: Let U be a finite-dimensional vector space over a field F. Let $T: U \to U$ is a linear transformation. Then T is one-one if and only if it is onto.

Proof: Let T is one-one

This implies $\ker T = \{0\}$

So, $\nu(T) = 0$

By Rank Nullity theorem,

$$dim\, U = \rho(T)$$

That is $\dim U = \dim R$; R is range space of T.

We have proved that R is a subspace of U.

So, $\dim U = \dim R$ implies that $R = U$

That is, range= codomain

So, T is onto.

Conversely,

Let T is onto

This implies Range $T = U$

That is $\rho(T) = dim\, U$

Using this and the Rank Nullity theorem, we get,

$$\nu(T) = 0$$

This implies $Ker\, T = \{0\}$ and hence T is one-one.

Example 4.[illegible]:

Let V_F and W_F be two vector spaces. Define a linear transformation $T: V \to W$ as $T(x) = 0 \; \forall x \in V$. Find null space and range space of T. Also, find nullity and rank of T.

Range space $= R = \{T(x) | x \in V\} = \{0\}$. $R = \{0\}$

Hence rank $T = \rho(T) = 0$

By Rank Nullity Theorem,

$\dim V = \rho(T) + \nu(T)$

$= 0 + \nu(T)$

Hence, nullity $T = \dim V$

That is $\dim Ker\, T = \dim V$

Also, Ker T is a subspace of V.

This implies $Ker\, T = V$

Example 4.3.10:

For any field F, consider the map $T: F^3 \to F^2$ given by $T(\alpha, \beta, \gamma) = (\alpha, \beta)$ is a linear transformation. Find null space and range space of T. Also, find nullity and rank of T.

Let $(\alpha,\ \beta,\ \gamma) \in Ker\, T$

$\Rightarrow T(\alpha,\ \beta,\ \gamma) = (0,\ 0)$

$\Rightarrow (\alpha,\ \beta) = (0,\ 0)$

$\Rightarrow \alpha = 0,\ \beta = 0$

Hence, $(\alpha,\ \beta,\ \gamma) = (0,\ 0,\ \gamma)$

Therefore, $Ker\, T = \{(0,\ 0,\ \gamma) | \gamma \in F\}$

Hence, $Ker\, T = \ < \{(0,\ 0,\ 1)\} >$

So, $\{(0,\ 0,\ 1)\}$ is a basis of $Ker\, T$ and $\nu(T) = 1$.

Again, $R = \{(\alpha,\ \beta) | \alpha,\ \beta \in F\} = F^2$.

Therefore, $\rho(T) = \dim F^2 = 2$

So, $\nu(T) + \rho(T) = 1 + 2 = 3 = \dim F^3$

Example 4.3.11: Let $V = P_3(\mathbb{R})$. Then for any polynomial $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3$, the mapping defined as $T(f(x)) = a_1 + 2a_2x + 3a_3x^2$ is a linear transformation. Find null space and range space of T. Also, find nullity and rank of T.

Let $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 \in Ker\, T$

$\Rightarrow T(f(x)) = 0$

$a_1 + 2a_2x + 3a_3x^2 = 0$

This implies, $a_1 = a_2 = a_3 = 0$

Thus,

$Ker\, T = \{a_0 + a_1x + a_2x^2 + a_3x^3 | a_0 \in R,\ a_1 = a_2 = a_3 = 0\} = \{a_0 | a_0 \in R\} = R$

$\nu(T) = 1$

By Rank Nullity theorem,

$\rho(T) = \dim P_3 - \nu(T) = 4 - 1 = 3$

Let $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 \in P_3(R)$

$T(f(x)) = a_1 + 2a_2x + 3a_3x^2$

$\qquad = b_1 + b_2x + b_3x^2;$

$b_1 = a_1,\ b_2 = 2a_2,\ b_3 = 3a_3$

Therefore, R is spanned by $\{1,\ x,\ x^2\} = P_2(R)$

Hence, $R = P_2(R)$

Remarks 4.3.12: A field F is always vector space over itself.

The dimension of a field is 1.

Let $B = \{1\}$; where 1 is the unity of F.

Since B is a singleton set containing a non-zero element, therefore, it is L. I.

Also, every element $\alpha \in F$ can be written as $\alpha.1$, which proves that B spans V.

Hence, the set containing unity of the field is a basis of F_F.

Let V be a vector space over a field F then a linear transformation $T: V \to F$ is called linear functional.

Let T be a non-zero linear functional on a vector space V_F such that $\dim V = n$.

$\rho(T) \leq \dim F$, that is $\rho(T) \leq 1$

This implies, $\rho(T) = 0$ or 1

Since $T \neq 0$, therefore, $\rho(T) \neq 0$.

That is, $\rho(T) = 1$

Using the Rank Nullity theorem, we get, $\nu(T) = \dim V - 1$.

4.4 The Similarity of Linear Transformations

Theorem 4.4.1: Let V and W be two finite-dimensional vector spaces over the field F such that $\dim V = n$ and $\dim W = m$. Let $T: V \to W$ be a linear transformation. Let $B = \{x_1, x_2, \ldots, x_n\}$ and $B' = \{x'_1, x'_2, \ldots, x'_n\}$ be two bases of V. Let $C = \{y_1, y_2, \ldots, y_m\}$ and $C' = \{y'_1, y'_2, \ldots, y'_m\}$ be two bases of W. Let $[T, B; C] = (\alpha_{ij})$ and $[T, B'; C'] = (\beta_{ij})$. Let P and Q be the matrices of sets B' and C' relative to the bases B and C respectively. Then $(\beta_{ij}) = Q^{-1}(\alpha_{ij})P$

Proof: Since P is the matrix of set B' relative to the basis B.

Therefore, we have

$$x'_i = \sum_{j=1}^{n} x_j p_{ji} \,; 1 \leq i \leq n \ldots (1)$$

Similarly, if $Q^{-1} = \left(q'_{ij}\right)$, then

$$y_i = \sum_{j=1}^{m} y'_j q'_{ji} \,; 1 \leq i \leq m \ldots (2)$$

Further, $T, B; C] = (\alpha_{ij})$ implies

$$T(x_i) = \sum_{j=1}^{m} y_j \alpha_{ji} \,; 1 \leq i \leq n \ldots (3)$$

From (1)

$$T(x'_i) = T\left(\sum_{j=1}^{n} x_j p_{ji}\right) = \sum_{j=1}^{n} T(x_j) p_{ji}$$

From (2),

$$T(x'_i) = \sum_{j=1}^{n} \left(\sum_{k=1}^{m} y_k \alpha_{kj}\right) p_{ji} = \sum_{j=1} \left[\sum_{k=1} \left(\sum_{t=1}^{m} y'_t q'_{tk}\right) \alpha_{kj}\right] p_{ji}$$

$$T(x'_i) = \sum_{t=1} y'_t \left[\sum_{k=1} \left(\sum_{j=1}^{n} q'_{tk}\right) \alpha_{kj}\right] p_{ji} = \sum_{t=1}^{m} y'_t \alpha'_{ti}$$

where $\alpha'_{ti} = \sum_{k=1}^{m} \sum_{j=1}^{n} q'_{tk} \alpha_{kj} p_{ji}$

Thus, the matrix (α'_{ti}) of T relative to the bases B' and C' is $Q^{-1}(\alpha_{kj})P$.

Theorem 4.4.2: Let V be a finite-dimensional vector space over the field F. T be a linear operator on V. Let $\dim V = n$ and $B = \{x_1, x_2, ..., x_n\}$ is a basis of V. Let $[T, B] = (\alpha_{ij})$. Consider another ordered basis $B' = \{x'_1, x'_2, ..., x'_n\}$ of V. Let P be the matrix of set B' relative to the basis B.

By taking $B = C$ and $B' = C'$ in the previous theorem, we get $P = Q$ and hence $[T, B'] = P^{-1}(\alpha_{ij}) P$.

Example 4.4.3:

Let T be the linear operator on $\mathbb{C}^2$ defined by $T(x, y) = (x, 0)$. Let B is the standard ordered basis for $\mathbb{C}^2$ and let $B' = \{\alpha_1, \alpha_2\}$, where $\alpha_1 = (1, i)$, $\alpha_2 = (-i, 2)$.

1. Find the matrix P of B' relative to the basis B.
2. Find $[T, B]$
3. Find $[T, B']$

Matrix of B' relative to the basis B

First, we express elements of B' as a linear combination of elements of basis B

$$(1, i) = 1(1, 0) + i(0, 1)$$
$$(-i, 2) = -i\,(1, 0) + 2(0, 1)$$

The matrix

$$P = \begin{bmatrix} 1 & -i \\ i & 2 \end{bmatrix}$$

2. $[T, B]$

$$B = \{(1, 0), (0, 1)\}$$
$$T(1, 0) = (1, 0) = 1\,(1, 0) + 0(0, 1)$$
$$T(0, 1) = (0, 0) = 0(1, 0) + 0(0, 1)$$

So, the matrix

$$[T, B] = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

3. $[T, B']$

$$B' = \{(1, i), (-i, 2)\}$$

Matrix of B' relative to the basis $P = \begin{bmatrix} 1 & -i \\ i & 2 \end{bmatrix}$

$$P^{-1} = \begin{bmatrix} 2 & i \\ -i & 1 \end{bmatrix}$$

Then

$$[T, B'] = P^{-1}[T, B]P$$
$$= \begin{bmatrix} 2 & -2i \\ -i & -1 \end{bmatrix}$$

Definition 4.4.4: Two square matrices A and B of order n are said to be similar if there exists an invertible matrix P such that

$$A = P^{-1}BP$$

By taking $P^{-1} = Q$ we can observe that

$$B = Q^{-1}AQ$$

Hence this relation of similarity is symmetric.

Remark 4.4.5: In the theorem, we have seen that if T is a linear operator on a vector space V_F.

Then the matrices (α_{ij}) and (β_{ij}) corresponding to two different bases B and B' of V have the relation

$$(p_{ij})^{-1}(\alpha_{ij})(p_{ij}) = (\beta_{ij})$$

That is, the matrices (α_{ij}) and (β_{ij}) are similar matrices. In other words, we can say that matrices of a linear operator corresponding to different bases are similar to each other.

Theorem 4.4.6: Let V be a finite-dimensional vector space over the field F. T be a linear operator on V. Let $\dim V = n$ and $B = \{x_1, x_2, \dots, x_n\}$ is a basis of V.Let A = $[T, B] = (\alpha_{ij})$. Then $\rho(T) =$ Row rank of A.

Proof: Let $[T, B] = (\alpha_{ij})$ implies

$$T(x_i) = \sum_{j=1}^{n} x_j \alpha_{ji} \,; 1 \leq i \leq n \dots (1)$$

Let column rank of A is s.

Now, we can find $i_1, i_2, \dots, i_s$ such that the $i_1 th, i_2 th, \dots, i_s th$ columns of A are linearly independent and all other columns are expressible as a linear combination of these columns.

Suppose

$$\sum_{k=1}^{s} T(x_{i_k})\beta_k = 0$$

for some $\beta_i \in F$

From (1),

$$T(x_{i_k}) = \sum_{j=1}^{n} x_j \alpha_{j i_k}$$

That is,

$$\sum_{k=1}^{s} \left(\sum_{j=1}^{n} x_j \alpha_{j i_k} \right) \beta_k = 0$$

Or,

$$\sum_{j=1}^{n} x_j \left(\sum_{k=1}^{s} \alpha_{j i_k} \beta_k \right) = 0$$

This implies,

$$\sum_{k=1}^{s} \alpha_{j i_k} \beta_k = 0$$

Since $i_1 th, i_2 th, \dots, i_s th$ columns of A are linearly independent, therefore, $\beta_k = 0 \; \forall \; k$. Hence, $T(x_{i_1}), T(x_{i_2}), \dots, T(x_{i_s})$ are linearly independent.All the columns are expressible as a linear combination of $i_1 th, i_2 th, \dots, i_s th$ columns of A. So, there exist scalars $\alpha_{1i}, \alpha_{2i}, \dots, \alpha_{si} \in F$ such that

$$\alpha_{lj} = \sum_{k=1}^{s} \alpha_{l i_k} \alpha_{kj}$$

Also, from (1),

$$T(x_i) = \sum_{j=1}^{n} x_j \alpha_{ji}$$

$$= \sum_{j=1}^{n} x_j \left(\sum_{k=1}^{s} \alpha_{j i_k} \alpha_{ki} \right)$$

$$= \sum_{k=1}^{s} \left(\sum_{j=1}^{n} x_j \alpha_{ji_k} \right) a_{k_i}$$

$$= \sum_{k=1}^{s} T(x_{i_k}) a_{ki}$$

Now the space $T(V)$ is spanned by $T(x_1)$, $T(x_2)$, ... , $T(x_n)$.

Further, $T(x_{i_k})$; $1 \leq k \leq s$ are L.I. and all other $T(x_i)$'s are expressible as linear combinations of these s vectors.

Consequently, $\{T(x_{i_k})\}_{1 \leq k \leq s}$ is a basis of $T(V)$.

Hence, $\rho(T) = \dim(T(V)) = s =$ column rank of A.

Summary

- linear transformations from a vector space to another vector space over the same fieldare defined.
- linear transformations are explained with the help of examples.
- the matrix of a linear transformation is found.
- null space and range space of a linear transformation is defined.
- method to find the null space and range space of a linear transformation is given.
- Rank Nullity theorem is proved.
- the similarity between matrices corresponding to two different sets of bases is observed.

Keywords

- linear transformations
- Null space of a linear transformation
- Range of a linear transformation
- Matrix corresponding to a linear transformation
- Rank Nullity theorem
- The similarity between the matrices

Self Assessment

1. Let V be the vector space of all the polynomials over the field of real numbers. Then which of the following is a linear transformation from V to itself

A. $T(f) = f'$ where f' denotes the derivative of f
B. $T(f) = f + 1$
C. $T(f) = f + 2$
D. $T(f) = f + 3$

2. Let V be the vector space of square matrices of order 3. Then T from V to itself defined as $T(A) = A + cI$ is a linear transformation (where c is a real number, and I is identity map of order 3 if and only if $c =$

A. 3
B. 2
C. 1
D. 0

3. Let V= R^2 be the vector space over the field of real numbers. Then which of the following is not a linear transformation from V to R

A. $T(x, y) = x + y$
B. $T(x, y) = xy + 1$
C. $T(x, y) = 2x + y$

D. $T(x,y) = 5x$

4. Let T be a linear transformation from a vector space V to itself. Let 0 be the additive identity of V. Then which of the following is true

A. $T(0) = 0$
B. $T(-x) = x$ for $x \in V$
C. $T(x-y) = T(x) + T(y)$
D. $T(cx) = c^2 x$

5. Let $T: R^2 \to R^3$ be a linear transformation. Then the order of the matrix of T with respect to any bases of R^2 and R^3 is

A. 2× 3
B. 3×2
C. 2×2
D. 3×3

6. Let $T: R^2 \to R^3$ is given by $T(x,y) = (x, y, x+y)$. Then matrix of T with respect to standard bases of R^2 and R^3 is

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

B: $\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}$

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

D: $\begin{bmatrix} -1 & 0 \\ 0 & 1 \\ -1 & 1 \end{bmatrix}$

7. Let $T: R^2 \to R^2$ is given by $T(x,y) = (-y, x)$. Then matrix of T with respect to the basis B= $\{(1,2),(1,-1)\}$ is

A: $\begin{bmatrix} \frac{1}{3} & \frac{2}{3} \\ \frac{5}{3} & \frac{1}{3} \end{bmatrix}$

B: $\begin{bmatrix} -\frac{1}{3} & \frac{2}{3} \\ -\frac{5}{3} & -\frac{1}{3} \end{bmatrix}$

C: $\begin{bmatrix} -\frac{1}{3} & \frac{2}{3} \\ -\frac{5}{3} & \frac{1}{3} \end{bmatrix}$

D: $\begin{bmatrix} \frac{1}{3} & -\frac{2}{3} \\ \frac{5}{3} & -\frac{1}{3} \end{bmatrix}$

8. Let V be the vector space of polynomials of degree 3 or less than 3 in variable x over the field of real numbers. Let B_1 and B_2 be two bases of the vector space V given by $B_1 = \{1, x, x^2, x^3\}$ and $B_2 = \{2, 3x, 4x^2, 5x^3\}$. Then matrix P of B_2 from B_1 is given by

A: $\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 5 \end{bmatrix}$

B: $\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 5 \end{bmatrix}$

C: $\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & -4 & 0 \\ 0 & 0 & 0 & 5 \end{bmatrix}$

D: $\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & -5 \end{bmatrix}$

9. Null space of a linear transformation T from a vector space V to a vector space W is defined as
A. $\{x \in V | T(x) = 0_V\}, 0_V$ denotes the additive identity of V
B. $\{x \in V | T(x) = 0_W\}, 0_W$ denotes the additive identity of W
C. $\{T(x) | x \in V\}$
D. $\{T(x) | x \in W\}$

10. Let $V = R^2$. Then V is a vector space over the field of real numbers. Let $T: V \to V$ be defined as $T(x, y) = (x + y, x - y)$, then null space of T is given by
A. $\{(0, 0)\}$
B. ϕ
C. $\{(1, 0)\}$
D. $\{(0, 1)\}$

11. Range space of zero transformation defined on vector space R^4 to R^3 is
A. R^4
B. $\{(0,0,0,0)\}$
C. $\{(0,0,0)\}$
D. R^3

12. Let P_n denotes the vector space of polynomials with degree less than or equal to n. Let T be a linear transformation from P_2 to P_3 such that nullity of T = 2. Then rank T=
A. 1
B. 2
C. 3
D. 4

13. Let V be the vector space of square matrices of order 2 over the field of real numbers. Let T be a linear transformation on V defined as $T\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} a & 0 \\ 0 & c \end{bmatrix}$. Then nullity of T is
A. 1
B. 2
C. 3
D. 4

14. Let V be a vector space with an odd dimension. Then for a linear transformation defined on V
A. Nullity T is odd
B. Nullity T is 0
C. Nullity T is either odd or zero
D. Rank T is even

15. Let $T: R^2 \to R^2$ be a linear transformation such that matrix of T with respect to the standard basis of R^2 is given by $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Then matrix of T with respect to the basis B= $\{(1,2),(1,-1)\}$ is

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

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

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

D: $\begin{bmatrix} -1 & 0 \\ -1 & -1 \end{bmatrix}$

Answers for Self Assessment

1.	A	2.	D	3.	B	4.	A	5.	B
6.	B	7.	C	8.	A	9.	B	10.	A
11.	C	12.	A	13.	B	14.	C	15.	C

Review Questions

1. Consider the space V_2 represented geometrically by the plane and the transformation $T(x,y) = (ax, by)$. Then prove/disprove that T is a linear transformation.
2. Let R be the field of real numbers and let V be the space of all functions from R into R which are continuous. Define T by

$$T(f(x)) = \int_0^x f(t)\, dt$$

Then prove that T is a linear transformation from V to itself.

3. Let F be a field. Show that $F^m \cong F^n$ if and only if $m = n$.
4. 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. $T(x+iy) = \begin{bmatrix} x+7y & 5y \\ -10y & x-7y \end{bmatrix}$. Then verify that $T\big((x+iy)(t+iw)\big) = T(x+iy)\,T(t+iw)$.
5. Prove that the mapping T defined in problem 4, is a one-one real linear transformation of V into the space of 2×2 real matrices.

Further Readings

- Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress
- Topics in algebra by I.N. Hartstein, Wiley
- Abstract algebra by David S Dummit and Richard M Foote, Wiley

Weblinks

- https://nptel.ac.in/courses/111/102/111102009/
- https://nptel.ac.in/courses/111/105/111105112/#

Unit 05: Modules

CONTENTS

Objective

After studying this unit, you will be able to

- define modules over a ring and understand modules with the help of examples
- define submodules,
- define R −homomorphisms and relate R −homomorphisms with linear transformations,
- understand important properties and results about R −homomorphisms,
- define quotient modules,
- state and prove the Fundamental theorem of R −homomorphism,
- define exact sequences and prove important results based on it.

Introduction

In this unit, you will be introduced to modules and submodules. Both the structure will be explained with the help of examples. R − homomorphisms will be defined and it will be discussed that every R − homomorphism is a linear transformation. Quotient modules will be defined. The fundamental theorem of R −homomorphisms will be proved.

5.1 Definition, Examples, and Properties of Modules

Definition 5.1.1: Let M be an additive abelian group. Let $End\,(M)$ be the ring of endomorphisms of M. If $r \in End\,(M)$, $m \in M$, then rm will denote the image of m by r. Therefore,

i. $r(m_1 + m_2) = rm_1 + rm_2$,

ii. $(r_1 + r_2)m = r_1m + r_2m$,

iii. $(r_1r_2)m = r_1(r_2m)$

iv. $1m = m$,

where $r,\ r_1, r_2 \in R; m,\ m_1, m_2 \in M$.

Then we say M is a left module over the ring $R = End\,(M)$ according to the following definition.

Definition 5.1.2: Let R be a ring and M be an additive abelian group. Let $(r,\ m) \mapsto rm$, a mapping of $R \times M$ into M such that

i. $r(m_1 + m_2) = rm_1 + rm_2$,

ii. $(r_1 + r_2)m = r_1m + r_2m$,

iii. $(r_1r_2)m = r_1(r_2m)$

iv. $1m = m$, if $1 \in R$

where $r, r_1, r_2 \in R; m, m_1, m_2 \in M$.

Then M is called a left R −module.

Definition 5.1.3: Let R be a ring and M be an additive abelian group. Let $(m, r) \mapsto mr$, a mapping of $R \times M$ into M such that:

i. $(m_1 + m_2)r = m_1r + m_2r$,

ii. $m(r_1 + r_2) = mr_1 + mr_2$,

iii. $m(r_1r_2) = (mr_1)r_2$

iv. $m1 = m$, if $1 \in R$

where $r, r_1, r_2 \in R; m, m_1, m_2 \in M$

Then M is called a right R −module.

Note:

- If R is a division ring, then a left R −module is called a left vector space over R.
- rm is called the scalar multiplication of m by r on the left.
- If R is a commutative ring and M is a left R −module, then M can be made into a right R −module by defining $mr = rm$. Hence, over a commutative ring, left and right R −modules are the same. In this case, we simply call it an R −module.

Theorem 5.1.4 (Properties of an R −module M)

Let M be a left R −module. Let 0_M and 0_R be the additive identities of M and R respectively. Then

1. $0_Rm = 0_M$

Proof:

For $a \in R$, $m \in M$

$a + 0_R = a$

$\Rightarrow (a + 0_R)m = am$

$\Rightarrow am + 0_Rm = am + 0_M$

$\Rightarrow 0_Rm = 0_M$

2. *For* $a \in R$, $a0_M = 0_M$

Proof:

Let $a \in R$, $m \in M$

$m + 0_M = m$

$\Rightarrow a(m + 0_M) = am$

$\Rightarrow am + a0_M = am + 0_M$

$\Rightarrow a0_M = 0_M$

3. For $a \in R$, $m \in M$,

$(-a)m = -(am) = a(-m)$

Proof:

Let $a \in R$, $m \in M$

$\Rightarrow a0_M = 0_M$

$\Rightarrow a(m + (-m)) = 0_M$

$\Rightarrow am + a(-m) = 0_M$

$\Rightarrow -(am) = a(-m)$ ...(1)

Again, $0_R m = 0_M$

$\Rightarrow (a + (-a))m = 0_M$

$\Rightarrow am + (-a)m = 0_M$

$\Rightarrow -(am) = (-a)m \ldots (2)$

From (1) and (2), we get,

$(-a)m = -(am) = a(-m)$

Note:

From here, we will consider the modules as left modules, unless otherwise stated.

Example:

Let A be an additive abelian group. Then A is a left (right) Z −module.

For $k, k_1, k_2 \in Z$ and for $a, a_1, a_2 \in A$

Consider $k(a_1 + a_2)$

If $k > 0$

$$k(a_1 + a_2) = (a_1 + a_2) + (a_1 + a_3) + \cdots + (a_1 + a_2)$$
$$= (a_1 + a_1 + \cdots + a_1) + (a_2 + a_2 + \cdots + a_2)$$
$$= ka_1 + ka_2$$

If $k < 0$, then $l = -k > 0$

$l(a_1 + a_2) = la_1 + la_2$

$-k(a_1 + a_2) = (-k)a_1 + (-k)a_2$

$-(k(a_1 + a_2)) = -(ka_1 + ka_2)$

$k(a_1 + a_2) = ka_1 + ka_2$

If $k = 0$ then

$k(a_1 + a_2) = 0 = ka_1 + ka_2$

So, in all the cases, we have, $k(a_1 + a_2) = ka_1 + ka_2$

Similar arguments show that

$(k_1 + k_2)a = k_1 a + k_2 a$

$(k_1 k_2)a = k_1(k_2 a)$

$1a = a$

for all $k, k_1, k_2 \in Z$ and for $a, a_1, a_2 \in A$

This proves that A is left Z −module.

In other words, every additive abelian group is a left Z −module.

Since Z is commutative, therefore, every additive abelian group is a right Z −module as well.

That is, every additive abelian group is a Z −module.

Example 5.1.5:

Let R be a ring. Then R itself can be regarded as a left R −module by defining am, $m \in R$, $a \in R$, to be a product of a and m as elements of the ring R.

Then the distributive law and associative law for multiplication in the ring R show that R is left R −module. Similarly, R is also a right R −module.

Direct Product of Modules: Let M and N be two R −modules. Consider the cartesian product $M \times N = \{(x, y) | x \in M, y \in N\}$.

Define the compositions as

$$(x, y) + (x', y') = (x + x', y + y')$$
$$r(x, y) = (rx, ry)$$

for all $x, x' \in M$, $y, y' \in N$, $r \in R$. Then $M \times N$ is an $R-$module and it is called the direct product of the $R-$modules M and N.

Definition 5.1.6: A non-empty subset N of an $R-$module M is called an $R-$submodule (or simply submodule) of M if

i. $a - b \in N \ \forall\, a, b \in N$

ii. $ra \in N \ \forall\, a \in N,\ r \in R$

Clearly, $\{0\}$ and M are $R-$submodules, called trivial submodules. Any other submodule of M is called the proper submodule of M.

Example 5.1.7:

Each left ideal of a ring R is an $R-$submodule of the left $R-$module R, and conversely.

From the definition of a left ideal of ring R.

A non-empty subset I of a ring R is a left ideal of R if

i. $a - b \in I \ \forall\, a, b \in I$

ii. $ra \in I \ \forall\, a \in I,\ r \in R$

So, from the definition of the left ideal, the result is clear.

Example 5.1.8: If M is an $R-$module and $x \in M$, then the set

$$Rx = \{rx \mid r \in R\}$$

is an $R-$submodule of M, for,

$$r_1x - r_2x = (r_1 - r_2)x \in Rx$$
$$r_1(r_2x) = (r_1r_2)x \in Rx$$

for all $r_1, r_2 \in R$

Task:

1. Show that the polynomial ring $R[x]$ over the ring R is an $R-$module.
2. Let R be a ring and let S denote the set of all sequences $(a_i), i \in N, a_i \in R$. Define $(a_i) + (b_i) = (a_i + b_i), \alpha(a_i) = (\alpha a_i)$, where $\alpha, a_i, b_i \in R$. Then S is a left-R module.

5.2 Theorems on Modules and Submodules

Definition 5.2.1: Let f be a mapping of an $R-$module M to an $R-$module N such that for all $x, y \in M$, $r \in R$,

i. $f(x + y) = f(x) + f(y)$

ii. $f(rx) = rf(x)$

then f is called an $R-$linear mapping or a linear mapping or an $R-$homomorphism of M into N.

Notations:

- The set of all $R-$homomorphisms of M into N is denoted as $Hom_R(M, N)$.
- If $M = N$, then f is called an endomorphism of M, and then the set $Hom_R(M, M)$ is also denoted as $Hom_R(M)$.
- If R is a field or a division ring, then f is also called a linear transformation of the vector space M to the vector space N.

Examples:

- Let M be an $R-$module. Then the mapping $i: x \to x$ of M onto M is an

$R-$homomorphism called identity homomorphism.

- The mapping $f: M \to N$ defined by $f(x) = 0 \ \forall \ x \in M$ is an $R-$homomorphism called zero homomorphism.
- Every linear transformation defined from a vector space V_F to a vector space W_F is an $R-$homomorphism.

Properties of $R-$homomorphism

Let $f: M \to N$ be an $R-$ homomorphism of an $R-$module M into an $R-$module N. Then

i. $f(0) = 0$

ii. $f(-x) = -f(x),\ x \in M$

iii. $f(x-y) = f(x) - f(y),\ x, y \in M$

$$f(0) = 0$$

Proof:

$$0 + 0 = 0$$
$$f(0+0) = f(0)$$
$$f(0) + f(0) = f(0) + 0$$
$$f(0) = 0$$

(ii) $f(-x) = -f(x),\ x \in M$

Let $x \in M,\ \ x + (-x) = 0$

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

Since N is an additive abelian group.

Hence, $f(x) + f(-x) = f(-x) + f(x) = 0$

So, $f(-x) = -f(x)$

(iii) $f(x-y) = f(x) - f(y),\ x, y \in M$

For $x,\ y \in M$

$$f(x-y) = f\big(x + (-y)\big)$$
$$= f(x) + f(-y)$$
$$= f(x) - f(y)$$

Definition 5.2.2: Let $f: M \to N$ be an $R-$homomorphism of an $R-$module M into an $R-$module N. Then

- The set $K = \{x \in M \mid f(x) = 0\}$ is called the kernel of f and is denoted as $Ker\ f$.
- The set $f(M) = \{f(x) \mid x \in M\}$ is called the homomorphic image (or simply image) of M under f and is denoted as $Im\ f$.

Results: *1.* $Ker\ f$ is an $R-$submodule of M.

Proof: Since $f(0) = 0$

Therefore, $0 \in Ker\ f$

So, $Ker\ f \neq \phi$

Let $x,\ y \in Ker\ f,\ r \in R$

This implies, $f(x) = f(y) = 0$

Consider $f(x-y) = f(x) - f(y)$

$$= 0 - 0 = 0$$

and

$f(rx) = rf(x)$

$$= r0 = 0$$

Therefore, $x - y,\ rx \in Ker\ f\ \forall\ x, y \in Ker\ f,\ r \in R$

Hence, $Ker\ f$ is an R −submodule of M.

2. $Im\ f$ is an R −submodule of N.

Proof: Since $f(0) = 0$

Therefore, $0 \in Im\ f$

So, $Im\ f \neq \phi$

Let $x, y \in Im\ f, r \in R$

This implies, there exist $x_1,\ y_1 \in M$ such that $x = f(x_1),\ \ y = f(y_1)$

Consider $f(x_1 - y_1) = f(x_1) - f(y_1)$

$$= x - y$$

and

$f(rx_1) = rf(x_1)$

$$= rx$$

Therefore, $x - y,\ rx \in Im\ f\ \forall\ x, y \in Im\ f,\ r \in R$

Hence, $Im\ f$ is an R −submodule of M.

3.$Ker\ f = \{0\}$ if and only if f is 1-1.

Let $Ker\ f = \{0\}$ and $f(x) = f(y)$ for some $x, y \in M$

Then $f(x - y) = f(x) - f(y) = 0$

This implies, $x - y \in Ker\ f = \{0\}$

$x - y = 0$ which implies, $x = y$

Hence, f is 1-1.

Conversely, let f is 1-1 and $x \in Ker\ f$

Then

$$f(x) = 0$$

But

$f(0) = 0$

That is,

$f(x) = f(0)$

f is 1-1, which implies, $x = 0$.

Notations:

- If f is 1-1, we say that M is isomorphic or R −isomorphic into N, or M is embeddable in N, or there is a copy of M in N.
- We write it as $M \hookrightarrow N$.
- If f is both 1-1 and onto, then we say that M is isomorphic or R −isomorphic onto N
- We write it as $M \cong N$.

Theorem 5.2.3: Relation of R −isomorphism is an equivalence relation in the set of R −modules.
Proof:

Reflexive:

For an R −module M, $f: M \to M$ given by $f(x) = x\ \forall\ x \in M$ is 1-1, onto and R −homomorphism. Hence, $M \cong M$.

Therefore, this relation is reflexive.

Symmetric:

Let M and N are two R −modules such that $M \cong N$.

So, there exists function $f: M \to N$ such that

f is 1-1, onto and R −homomorphism.

Since f is 1-1 and onto,

therefore, $f^{-1}: N \to M$ exists and it is 1-1 and onto.

Now we will prove that f^{-1} is R −homomorphism.

Let $x,\ y \in N$

$f: M \to N$ is onto. So, there exist $x_1, y_1 \in M$ such that

$f(x_1) = x$ and $f(y_1) = y$

Consider

$$f(x_1 + y_1) = f(x_1) + f(y_1) = x + y$$

That is,

$$f^{\ \ 1}(x + y) = x_1 + y_1 = f^{-1}(x) + f^{-1}(y)$$

That is,

$f^{-1}(x + y) = x_1 + y_1 = f^{-1}(x) + f^{-1}(y)$

Again for $r \in R$

$$f(rx_1) = rf(x_1) = rx$$

That is,

$$f^{-1}(rx) = rx_1 = rf^{-1}(x)$$

Hence, $f^{-1}: N \to M$ is R −isomorphism and $N \cong M$.

Therefore, this relation is symmetric.

Transitive:

Let M, N, and P be three R −modules such that $M \cong N$ and $N \cong P$.

Then there exist mappings $f: M \to N$ and $g: N \to P$ such that f and g are both 1-1, onto and R −homomorphisms.

Consider the composite map $h = g \circ f: M \to P$.

Since the composite map of two 1-1, onto maps is 1-1 and onto.

Hence, h is 1-1 and onto.

Again for $x,\ y \in M$

$$h(_{x+y)} = {}_{g \circ f(x+y)}$$

$$= {}^{g \circ f(x+y)}_{g(f(x+y))}$$

$$= {}^{g(f(x+y))}_{g(f(x)+f(y))}$$

$$= {}^{g(f(x)+f(y))}_{g(f(x))+g(f(y))}$$

$$= {}^{g(f(x))+g(f(y))}_{g \circ f(x)+g \circ f(y)}$$

Again for $x \in M$, $r \in R$,

$$h(_{rx)} = {}_{g \circ f(rx)}$$

$$= g(f(rx))$$

$$= g(f(rx))$$

$$= g(rf(x))$$

$$= rg(f(x)) = r \text{ [illegible] } (x)$$

Hence, $h: M \to P$ is 1-1, onto and R −homomorphism which proves that $M \cong P$.

That is, this relation is transitive.

Hence, this relation is an equivalence relation.

Theorem 5.2.4: Let M be an R −module. Then $Hom_R(M, M)$ is a subring of $Hom\,(M, M)$ where $Hom_R(M, M)$ is the set of all R −homomorphisms on R −module M and $Hom\,(M, M)$ is a set of all group homomorphisms regarding M as an additive group.

Proof:

Clearly, $Hom_R(M, M) \subseteq Hom\,(M, M)$.

Again let $f,\ g \in Hom_R(M, M),\ x \in M,\ r \in R$

Then

$$(f - g)(rx) = f(rx) - g(rx)$$
$$= rf(x) - rg(x)$$
$$= r(f(x) - g(x))$$
$$= r((f - g)(x))$$

Further,

$$(fg)(rx) = f(g(rx))$$
$$= f(rg(x))$$
$$= rf(g(x))$$
$$= r(fg(x))$$

Therefore, $f - g,\ fg \in Hom_R(M, M)$.

Hence, $Hom_R(M, M)$ is a subring of $Hom\,(M, M)$.

Theorem 5.2.5: Let R be a ring with unity. Let $Hom_R(R, R)$ denote the ring of endomorphisms of R regarded as a right R −module. Then $R \cong Hom_R(R, R)$ as rings.

Solution: Consider the mapping $f: R \to Hom_R(R, R)$, given by $f(a) = a^*$, where $a^*(x) = ax,\ x \in R$. Let $x,\ y,\ r \in R$. Then

$a^*(x + y) = a(x + y) = ax + ay = a^*(x) + a^*(y)$

and

$$a^*(xr) = a(xr) = (ax)r = (a^*x)r$$

Thus, a^* is an R −homomorphism of the right R −module R into itself; that is, $a^* \in Hom_R(R, R)$.

We now show that f is a ring homomorphism.

Let $a,\ b \in R$. Then for any $x \in R$,

$$(a + b)^*(x) = (a + b)x = ax + bx = a^*(x) + b^*(x) = (a^* + b^*)(x)$$

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

Similarly,

$(ab)^*(x) = (ab)x$

$\quad = a(bx) = a(b^*x)$

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

So, $(ab)^* = a^*b^*$.

Hence,

$f(a+b) = (a+b)^* = a^* + b^* = f(a) + f(b)$

and

$f(ab) = (ab)^* = a^*b^* = f(a)f(b)$

***f* is 1-1**

Let $a, b \in R$ such that $a^* = b^*$

Then $a^*(x) = b^*(x)\ \forall\ x \in R$

This implies, $ax = bx\ \forall\ x \in R$,

In particular, since $1 \in R$, $(a-b)1 = 0$

That is, $a = b$

So, f is 1-1.

***f* is onto**

Now suppose $t \in Hom_R(R, R)$

Let $t(1) = a$

Claim: $t = a^*$

Now for any $x \in R$,

$$t(x) = t(1x) = t(1)x = ax = a^*(x)$$

Hence, $t = a^*$

So, f is an onto map.

Therefore, $R \cong Hom_R(R, R)$

Definition 5.2.6: The opposite of a ring is another ring with the same elements and addition operation, but with the multiplication performed in the reverse order.

More explicitly, the opposite of a ring (R, +, ·) is the ring (R, +, ∗) whose multiplication ∗ is defined by a ∗ b = b · a for all a, b in R.

Theorem 5.2.7: Let R be a ring with unity. Let $Hom_R(R, R)$ denote the ring of endomorphisms of R regarded as a left $R-$module. Then $R^{op} \cong Hom_R(R, R)$ as rings.

Solution: By taking the map $f: R^{op} \to Hom_R(R, R)$, given by $f(a) = a^*$, where $a^*(x) = a \circ x = xa$.

Then a^* is an $R-$homomorphism of the left $R-$module R into itself, and the mapping f is a ring isomorphism. The proof is exactly similar to the previous theorem.

Definition 5.2.8: Let N be an $R-$submodule of an $R-$module M.

Let $a_1, a_2 \in M$.

Define a relation $\equiv$ on M as

$a_1 \equiv a_2 (mod\ N)$ if and only if $a_1 - a_2 \in N$.

Theorem 5.2.9:This relation is an equivalence relation.

Proof:

Reflexive: Since N is an $R-$submodule of $R-$module M.

Therefore, $0 \in N$

That is, $a - a \in N\ \forall\ a \in M$

This implies, $a \equiv a\ (mod\ N)\ \forall\ a \in N$.

Hence, this relation is reflexive.

Symmetric:

Let $a, b \in M$ such that $a \equiv b(mod\ N)$

That is, $a - b \in N$

Since N being R −submodule of R −module M is additive group, $-(a - b) \in N$

This implies, $b - a \in N$

Hence $b \equiv a(mod\ N)$

This implies this relation is symmetric.

Transitive:

Let $a, b, c \in M$ such that

$a \equiv b(mod\ N)$ and $b \equiv c\ (mod\ N)$

That is, $a - b,\ b - c \in N$

Since N is an additive group, therefore, $(a - b) + (b - c) \in N$

This implies, $a - c \in N$.

Hence, $a \equiv c(mod\ N)$

So, this relation is transitive.

Hence, this relation is an equivalence relation.

Equivalence Class: Let $a \in M$ and $\bar{a}$ denotes the equivalence class of a.

Then $\bar{a} = \{b \in M | b \equiv a(mod\ N)\}$

Now, $b \equiv a\ (mod\ N)$ implies, $b - a \in N$

That is, $b - a = x; x \in N$

$$b = a + x; x \in N$$

So, $\bar{a} = \{a + x | x \in N\} = a + N$

The set of these equivalence classes is denoted as M/N or $M - N$ or $\frac{M}{N}$.

Definition 5.2.10: (Quotient module) Consider the set M/N as defined and the operations in M/N as given

For $a, b \in M$, $r \in R$

$$(a + N) + (b + N) = (a + b) + N$$

$$ra + N = r(a + N)$$

Then M/N is an R −module under these compositions. This module is called the quotient module.

Theorem 5.2.11: The submodules of the quotient module M/N are of the form U/N, where U is a submodule of M containing N.

Proof: Let $f: M \to M/N$ be the canonical mapping given by

$$f(x) = x + N\ \forall x \in M.$$

Let X be an R −submodule of M/N.

Consider

$$U = \{x \in M | f(x) \in X\}$$

Claim: U is an R −submodule of M.

Let $x, y \in U$, $r \in R$,

Then $f(x), f(y) \in X$ and X is an R −submodule of M/N.

Therefore, $f(x) - f(y) \in X$

Since f is R −homomorphism, so, $f(x) - f(y) = f(x - y) \in X$ and $rf(x) = f(rx) \in X$

That is, $x-y,\ rx \in U$

So, U is an R −submodule of M.

$$\boldsymbol{N \subseteq U}$$

Let $x \in N$ then $f(x) = x + N = N = \bar{0} \in X$

This implies, $x \in U$

That is, $\boldsymbol{N \subseteq U}$

Also, since f is onto map, therefore, for $x \in X$, there exists $y \in M$ such that $f(y) = x$.

That is, $f(y) \in X \Rightarrow y \in U$

This implies, $X \subseteq f(U)$ ... (1)

Again for $x \in f(U)$

There exists $y \in U$ such that $x = f(y)$

Since $y \in U$, therefore, $f(y) \in X$

That is, $x \in X$

This implies, $f(U) \subseteq X$ ... (2)

Thus, $X = f(U)$

But $f(U) = U/N$.

Thus $X = U/N$.

Theorem 5.2.12: Fundamental theorem of R −homomorphisms

Let f be an R −homomorphism of an R −homomorphism of an R −module M into an R −module N. Then

$$\frac{M}{Ker\ f} \cong f(M)$$

Proof: Consider the mapping

$$g: \frac{M}{Ker\ f} \to f(M)$$

as

$$g(m + Ker\ f) = f(m)\ \forall\, m \in M$$

***g* is 1-1**

Let $m_1 + Ker\ f,\ m_2 + Ker\ f \in \frac{M}{Ker\ f}$

such that

$$g(m_1 + Ker\ f) = g(m_2 + Ker\ f)$$
$$\Rightarrow f(m_1) = f(m_2)$$
$$\Rightarrow f(m_1) - f(m_2) = 0$$
$$\Rightarrow f(m_1 - m_2) = 0$$
$$\Rightarrow m_1 - m_2 \in Ker\ f$$
$$\Rightarrow m_1 + Ker\ f = m_2 + Ker\ f$$

Hence, g is 1-1.

***g* is R −homomorphism**

Let $m_1 + Ker\ f,\ m_2 + Ker\ f \in \frac{M}{Ker\ f},\ r \in R$

Consider

$$g\big((m_1 + Ker\ f) + (m_2 + Ker\ f)\big)$$
$$= g(m_1 + m_2 + Ker\ f)$$

$$= f(m_1 + m_2)$$

$$= f(m_1) + f(m_2)$$

$$= g(m_1 + Ker\, f) + g(m_2 + Ker\, f)$$

Again,

$$g\big(r(m_1 + Ker\, f)\big) = g(rm_1 + Ker\, f)$$

$$= f(rm_1)$$

$$= rf(m_1)$$

$$= rg(m_1 + Ker\, f)$$

Hence, g is R −homomorphism.

***g* is onto**

For any $y \in f(M)$, there exists $x \in M$ such that $y = f(x)$

Since $x \in M$, $x + Ker\, f \in \frac{M}{Ker\, f}$

$$g(x + Ker\, f) = f(x) = y$$

Hence, g is onto.

This implies,

$$\frac{M}{Ker\, f} \cong f(M)$$

Theorem 5.2.13: Let A and B be R −submodules of R −modules M and N respectively. Then

$$\frac{M \times N}{A \times B} \cong \frac{M}{A} \times \frac{N}{B}$$

Proof: Define a mapping

$$f: M \times N \to \frac{M}{A} \times \frac{N}{B}$$

by $f(m, n) = (m + A,\ n + B)\ \forall\ m \in M,\ n \in N$

***f* is *R* −homomorphism**

Let $m_1,\ m_2 \in M,\ n_1, n_2 \in N,\ r \in R$

$$f((m_1, n_1) + (m_2, n_2)) = f(m_1 + m_2,\ n_1 + n_2)$$

$$= (m_1 + m_2 + A,\ n_1 + n_2 + B)$$

$$= ((m_1 + A) + (m_2 + A),\ (n_1 + B) + (n_2 + B))$$

$$= (m_1 + A, n_1 + B) + (m_2 + A, n_2 + B)$$

$$= f(m_1, n_1) + f(m_2, n_2)$$

Again,

$$f(r(m_1, n_1)) = f(rm_1,\ rn_1)$$

$$= (rm_1 + A,\ rn_1 + B)$$

$$= (r(m_1 + A),\ r(n_1 + B))$$

$$= r(m_1 + A,\ n_1 + B)$$

$$= rf(m_1, n_1)$$

Hence, f is R −homomorphism.

***f* is onto**

Let $(m+A,\ n+B) \in \frac{M}{A} \times \frac{N}{B}$

This implies, $m + A \in \frac{M}{A}$ and $n + B \in \frac{N}{B}$,

so that, $m \in M,\ n \in N$

Consider $f(m,n) = (m+A,\ n+B)$

Thus, f is onto.

$$Ker\, f = A \times B$$

Let

$$\begin{aligned}
Ker\, f &= \{(m,n) \mid m \in M,\ n \in N,\ f(m,n) = (A,B)\} \\
&= \{(m,n) \mid m \in M,\ n \in N,\ (m+A,\ n+B) = (A,B)\} \\
&= \{(m,n) \mid m \in M,\ n \in N,\ m+A = A,\ n+B = B\} \\
&= \{(m,n) \mid m \in M,\ n \in N,\ m \in A,\ n \in B\} \\
&= \{(m,n) \mid m \in M \cap A,\ n \in N \cap B\} \\
&= \{(m,n) \mid m \in A,\ n \in B\} \\
&= A \times B
\end{aligned}$$

So, by the Fundamental theorem of R −homomorphisms

$$\frac{M \times N}{A \times B} \cong \frac{M}{A} \times \frac{N}{B}$$

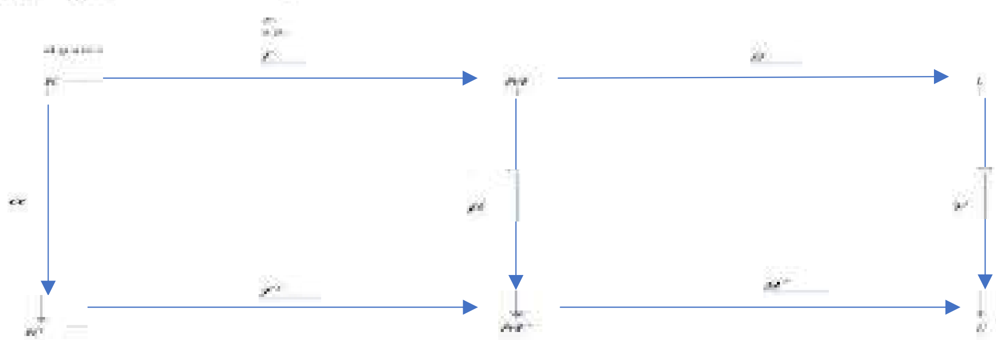
Definition 5.2.14: We call a sequence (finite or infinite) of R −modules and R −homomorphisms

exact if $Im\, f_n = Ker\, f_{n+1}\ \forall\, n$.

Theorem 5.2.15: Suppose that the following diagram of R −modules and R −homomorphismsis commutative and has exact rows. Show that

If α, γ and f' are 1-1, then so is β.

If α, γ, and g are onto, then so is β.



Proof: Let $m \in Ker\,\beta$

Because the diagram commutes,

$$\gamma g(m) = g'\beta(m) = 0,$$

So, $g(m) = 0$

Therefore, $m \in Ker\, g = Im\, f$

This implies, $m = f(k)$ for some $k \in K$.

Again, because the diagram commutes, $f'\alpha = \beta f$.

Thus, $f'\alpha(k) = \beta f(k) = \beta(m) = 0$.

This implies, $k = 0$

Then $m = f(k) = f(0) = 0$ which proves part (i).

Let $m' \in M'$

Then $g'(m') \in L'$

Since γ is onto, there exists $l \in L$

such that $g'(m') = \gamma(l)$

Also, g is onto

There exists, $m \in M$ such that $g(m) = l$

Now, $g'(\beta(m)) = \gamma g(m)$

$$= \gamma(l);\, g(m) = l$$

$$= g'(m')$$

Again $0 = g'(\beta(m) - m')$

This implies,

$\beta(m) - m' \in Ker\, g' = Im\, f'$

So, there exists $k' \in K'$ such that $f'(k') = \beta(m) - m'$

Since α is onto.

So, there exists $k \in K$ such that $\alpha(k) = k'$

Now, $m - f(k) \in M$

Also,

$$\beta(m - f(k)) = \beta(m) - \beta(f(k))$$

Since the diagram is commutative,

$$\beta f(k) = f'\alpha(k)$$

$$= f'(k')$$

$$= \beta(m) - m'$$

Hence

$$\beta(m - f(k)) = \beta(m) - \beta(f(k))$$

$$= \beta(m) - (\beta(m) - m') = m'$$

So, $m - f(k) \in M$ such that $\beta(m - f(k)) = m'$

Hence β is onto.

Summary

- modules over a ring are defined and explained with the help of examples.
- submodules are defined.
- R −homomorphisms are defined and related to linear transformations.
- understand important properties and results about R −homomorphisms.
- quotient modules are defined.
- The fundamental theorem of R −homomorphism is proved.
- exact sequences are defined,and important results based on them are proved.

Keywords

- modules
- submodules
- R −homomorphisms
- Quotient modules
- Fundamental theorem of R −homomorphism
- Exact sequence

Self Assessment

1. Consider the statements
I. Every module is a vector space
II. Every vector space is a module
A. Iis true but II is false
B. II is true but I is false
C. Both I and II are true
D. Both I and II are false

2. Let R be a commutative ring. Then R is always a …… over itself
A. Module
B. Vector space
C. Field
D. None of the above

3. Let M be an R −module. Then M is called a vector space
A. If R is commutative
B. If R is a ring with unity
C. If R is without zero-divisors
D. If R is a field

4. Let M be a left R −module over a commutative ring R with unity 1. Then which of the following is NOT true?
A. $rm \in R\ \forall\ m \in M$
B. $1m = m\ \forall\ m \in M$
C. $1r = r\ \forall\ r \in R$
D. $nm \in M\ \forall\ n \in Z, m \in M$

5. True/ False Let N be an R −submodule of an R −module M. Then $(N, +)$ is a subgroup of $(M, +)$.
A. True
B. False

6. Let M and N be two R −modules. A map $f: M \to N$ is called an R −endomorphism if and only if
A. f is R −homomorphism
B. $M = N$

C. $\dim M = \dim N$
D. f is R −homomorphism and $M = N$

7. Let A be an additive abelian group. Then which of the following is an Z −homomorphism on A?
A. $f(x) = 2x \; \forall \; x \in A$
B. $f(x) = x^2 \; \forall \; x \in A$
C. $f(x) = 2x + 1 \; \forall \; x \in A$
D. $f(x) = x^2 + 1 \; \forall \; x \in A$

8. Let M be an R −module. Define $f: M \to M$ as $f(m) = 0 \; \forall \; m \in M$. Then
A. f is an R − homomorphism but not an R − endomorphism
B. f is an R −endomorphism
C. f is an onto R − endomorphism
D. f is a 1-1 R − endomorphism

9. Let M be an R −module. Define $f: M \to M$ as $f(m) = m \; \forall \; m \in M$. Then
A. $Ker\, f = M$, $Im\, f = M$
B. $Ker\, f = \{0\}$, $Im\, f = \{0\}$
C. $Ker\, f = \{0\}$, $Im\, f = M$
D. $Ker\, f = M$, $Im\, f = \{0\}$

10. Relation of R −isomorphism on the set of R −modules is
A. Reflexive and symmetric but not transitive
B. Transitive and symmetric but not reflexive
C. Reflexive and transitive but not symmetric
D. All Reflexive, symmetric and transitive

11. True/ False Let $Hom_R(M,M)$ is set of all R −homomorphisms on an R −module M and $Hom(M,M)$ is set of all group homomorphisms on module M. Then $Hom_R(M,M)$ is a subgroup of $Hom(M,M)$ considering both as groups under the usual addition of functions.
A. True
B. False

12. Let M be an R −module and N be an R −submodule of M. Then M/N consists of
A. All the subgroups of $(N, +)$
B. All the cosets of N in M considering both as additive groups
C. All the R −submodules of M containing N
D. All the sets of the type U/N; where U is an R −submodule of M containing N.

13. Let M be an R −module and N be an R −submodule of M. Then R −submodules of M/N are
A. Subgroups of $(N, +)$
B. Cosets of N in M considering both as additive group
C. R −submodules of M containing N
D. The sets of the type U/N; where U is an R −submodule of M containing N.

14. Let M and N are two R −modules such that there exists a function $f: M \to N$ which is onto and R −homomorphism. Then
A. N is isomorphic to M
B. N is isomorphic to a proper R −submodule of M
C. N is isomorphic to a quotient module of M

D. N is isomorphic to R

15. Let $M, N,$ and P be three $R-$ submodules. Let $f: M \to N$ and $g: N \to P$ be two $R-$homomorphisms. Then the sequence is given below

is exact if and only if

$$M \xrightarrow{f} N \xrightarrow{g} P$$

A. $Im\ f = Ker\ g$
B. $Im\ f = N$
C. $Ker\ f = Im\ g$
D. $Im\ g \circ f = P$

Answers for Self Assessment

1.	B	2.	A	3.	D	4.	A	5.	A
6.	D	7.	A	8.	B	9.	C	10.	D
11.	A	12.	B	13.	D	14.	C	15.	A

Review Questions

1. Let M be an additive abelian group. Show that there is only one way of making it a $Z-$module.
2. Let $V = R^3$ be a vector space of $3-$tuples over the field R. Determine if W is a subspace of V, where W is the set of all (x, y, z) such that $x = 0$.
3. Let $V = R^3$ be a vector space of $3-$tuples over the field R. Determine if W is a subspace of V, where W is the set of all (x, y, z) such that $x + y \geq 0$
4. Show that the set of all functions f from the real field R to R can be made into a vector space by the usual operations of sum and scalar product.
5. Let $A, B,$ and C be $R-$submodules of an $R-$module M such that $B \subset A$. Show that

$$A \cap (B + C) = B + (A \cap C)$$

Further Readings

- Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress
- Topics in algebra by I.N. Hartstein, Wiley
- Abstract algebra by David S Dummit and Richard M Foote, Wiley

Weblinks

- https://nptel.ac.in/courses/111/102/111102009/
- https://nptel.ac.in/courses/111/105/111105112/#

Unit 06: Cyclicand Simple Modules

CONTENTS

Objective

After studying this unit, you will be able to

- find generating set of a given subset S of an R −module M,
- define cyclic module and observe its structure,
- prove that the sum of R −modules is generated by the set obtained by taking their union,
- define semi-simple or completely reducible modules,
- prove that an R −submodule and a quotient module of a semi-simple module is semi-simple,
- define the basis of a free module and analyze that not every module is a free module,
- prove that every basis of a free module has the same number of elements,
- define the rank of a free module and observe that a vector space is always semi-simple.

Introduction

In this unit, you will be introduced to the concept of cyclic, simple, and semi-simple modules. Important results about these classes of modules are proved. It will be proved that an R −submodule and a quotient module of a semi-simple module is semi-simple. Further, the basis of a module will be defined. It will be proved that not every module has a basis. Based on this, a free module will be defined.

6.1 Cyclic and Simple Modules

Theorem 6.1.1: If M is an R −module and $x \in M$, then the set $K = \{rx + nx \mid r \in R,\ n \in Z\}$ is an R − submodule of M containing x. Further, if R has unity, then $K = Rx$.

Proof: $(K, +)$ is an abelian subgroup of $(M, +)$

Let $a, b \in K$

Then $a = r_1x + n_1x$ and $b = r_2x + n_2x$; $r_1, r_2 \in R$ and $n_1, n_2 \in Z$

$$a - b = (r_1x + n_1x) - (r_2x + n_2x)$$
$$= (r_1 - r_2)x + (n_1 - n_2)x \in K$$

Let $r \in R$

$$ra = r(r_1x + n_1x)$$

If $n_1 > 0$

$$r(r_1x + n_1x) = r(r_1x + x + x + \cdots + x) = (rr_1 + r + r + \cdots + r)x$$

If $n_1 < 0$

$$r(r_1x + n_1x) = r[r_1x + (-x) + (-x) + \cdots + (-x)] = (rr_1 + (-r) + (-r) + \cdots + (-r))x$$

If $n_1 = 0$

$$r(r_1x + n_1x) = r(r_1x + 0x) = rr_1x$$

In all the cases, $r(r_1x + n_1x) = ux$ for some $u \in R$

Hence, $ra \in K$

Therefore, $(K, +)$ is an abelian subgroup of $(M, +)$.

$x \in K$

$x = 0x + 1x; 0 \in R,\ 1 \in Z$

Hence, $x \in K$

If L is any R −submodule containing x, then $K \subseteq L$

Let L is any R −submodule containing x

Consider $r \in R,\ n \in Z$ so that,

$rx + nx \in K$

Since $r \in R,\ x \in L$;

L is R −submodule of R −module M, therefore,

$rx \in L$

Again, $n \in Z,\ x \in L$, and L is additive group, therefore, $nx \in L$

Also, $rx,\ nx \in L$ implies, $rx + nx \in L$

This implies, $K \subseteq L$.

Therefore, K is the smallest R −submodule containing x.

Further, let R has unity e.

Claim: $\{rx + nx | r \in R,\ n \in Z\} = \{rx | r \in R\}$

Let $r \in R,\ n \in Z$

If $n > 0$

$$rx + nx = rx + n(ex) = rx + ex + ex + \cdots + ex = (r + e + e + \cdots + e)x = ux$$

If $n < 0$

$$rx + (-n)(-x) = rx + (-n)(e(-x)) = rx + (-ex) + (-ex) + \cdots + (-ex)$$

= (

If $n = 0$

$$rx + nx = rx$$

In all the cases, $rx + nx = vx$ for some $v \in R$

Therefore, $\{rx + nx | r \in R,\ n \in Z\} \subseteq \{rx | r \in R\}$ ...(1)

Again for $r \in R$,

$rx = rx + 0x; r \in R$ and $0 \in Z$

That is, $\{rx | r \in R\} \subseteq \{rx + nx | r \in R,\ n \in Z\}$ ...(2)

From (1) and (2),

$\{rx + nx | r \in R,\ n \in Z\} = \{rx | r \in R\}$.

Theorem 6.1.2: Let $\{N_i\}_{i \in \wedge}$ be a family of R −submodules of an R −module M. Then $\bigcap_{i \in \wedge} N_i$ is also an R −submodule.

Proof: Let $\{N_i\}_{i \in \wedge}$ be a family of R −submodules of an R −module M.

Let

$$N = \bigcap_{i \in \wedge} N_i$$

For $x, y \in N, r \in R$,

$$x, y \in N_i,\ r \in R\ \forall i \in \wedge$$

Since N_i is an R −submodule of R −module M, therefore, $x - y,\ rx \in N_i\ \forall i \in \wedge$.

That is, $x - y,\ rx \in N\ \forall x, y \in N$

Hence, N is also an R −submodule of R −module M.

Definition 6.1.3: Let S be a non-empty subset of an R − module M. Let $A = \{N | N$ is an R −submodule of M containing $S\}$.

Then $A \neq \phi$ because $M \in A$.

Let $K = \bigcap_{N \in A} N$.

Then K is the smallest R −submodule of M containing S and is denoted by $< S >$.

The smallest R −submodule of M containing a subset S is called the R −submodule generated by S.

If $S = \{x_1, x_2, \ldots, x_m\}$ is a finite set, then $< S >$ is also written as $< \{x_1, x_2, \ldots, x_m\} >$.

Definition 6.1.4: An R −module M is called a finitely generated module if for some $x_i \in M$, $1 \le i \le m$, $M =< \{x_1, x_2, \ldots, x_m\} >$. The elements $\{x_1, x_2, \ldots, x_m\}$ are said to generate M.

Definition 6.1.5: An R −module M is called a cyclic moduleif $M =< x >$ for some $x \in M$. This shows that a cyclic module generated by x is precisely $\{rx + nx | r \in R,\ n \in Z\}$, and if R has unity then it simplifies to $\{rx | r \in R\} = Rx$.

Theorem 6.1.6: If an R −module M is generated by a set $\{x_1, x_2, \ldots, x_n\}$ and $1 \in R$, then $M = \{r_1x_1 + r_2x_2 + \cdots + r_nx_n | r_i \in R\}$. The right side is symbolically written as $\sum_{i=1}^{n} Rx_i$.

Proof: First, we prove that the set $\sum_{i=1}^{n} Rx_i$ is an R −submodule of R −module M.

Let $m, m_1, m_2 \in \sum_{i=1}^{n} Rx_i$ and $r \in R$,

Then $m = \sum_{i=1}^{n} r_{0i}x_i$, $m_1 = \sum_{i=1}^{n} r_{1i}x_i$, $m_2 = \sum_{i=1}^{n} r_{2i}x_i$; for some $r_{0i}, r_{1i}, r_{2i} \in R\ \forall\ 1 \le i \le n$

$$m_1 - m_2 = \sum_{i=1}^{n} r_{1i}x_i - \sum_{i=1}^{n} r_{2i}x_i = \sum_{i=1}^{n} (r_{1i} - r_{2i})x_i \in \sum_{i=1}^{n} Rx_i$$

Also,

$$rm = r\sum_{i=1}^{n} r_{0i}x_i$$

$$= \sum_{i=1}^{n} r(r_{0i}x_i)$$

$$= \sum_{i=1}^{n} (rr_{0i})x_i \in \sum_{i=1}^{n} Rx_i$$

Therefore,

$\sum_{i=1}^{n} Rx_i$ is an R −submodule of R −module M.

Now we prove that the set $\{x_1, x_2, \dots, x_n\} \subseteq \sum_{i=1}^{n} Rx_i$

For $1 \le i \le n$, since $1 \in R$

$$x_i = 0x_1 + 0x_2 + \cdots + 0x_{i-1} + 1x_i + 0x_{i+1} + \cdots + 0x_n \in \sum_{i=1}^{n} Rx_i$$

That is, $x_i \in \sum_{i=1}^{n} Rx_i \ \forall i$. Hence, $\{x_1, x_2, \dots, x_n\} \subseteq \sum_{i=1}^{n} Rx_i$

Let N be any R −submodule of M containing $\{x_1, x_2, \dots, x_n\}$, then by definition of submodule $r_1x_1 + r_2x_2 + \cdots + r_nx_n \in N$ where $r_i \in R \ \forall \ 1 \le i \le n$. Hence **$\sum_{i=1}^{n} Rx_i \subseteq N$**

That is, $\sum_{i=1}^{n} Rx_i$ is the smallest R −submodule of R −module M containing the set $\{x_1, x_2, \dots, x_n\}$.

As per the statement, the smallest R−submodule of R −module M containing the set $\{x_1, x_2, \dots, x_n\}$ is M itself. Therefore, **$\sum_{i=1}^{n} Rx_i = M$.**

Definition 6.1.7: If an element $m \in M$ can be expressed as $m = r_1x_1 + r_2x_2 + \cdots + r_nx_n$, $r_i \in R$ for some $x_i \in M$, $\forall \ 1 \le i \le n$, then we say that m is a linear combination of elements $x_1, x_2, \dots, x_n$ over R.

Note:

The set of generators of a module need not be unique.

For example, let S be the set of all polynomials in x over the field F of degree less than or equal to n.

Then S is a vector space over F with $\{1, x, x^2, x^3, \dots, x^n\}$ and $\{1, 1+x, x^2, x^3, \dots, x^n\}$ as two distinct sets of generators.

Definition 6.1.8: Let $\{N_i\}_{1 \le i \le k}$ be a family of $R-$ submodules of a module M. Then the submodule generated by $\bigcup_{i=1}^{k} N_i$, that is, the smallest submodule containing the submodules N_i, $1 \le i \le k$, is called the sum of submodules N_i, $1 \le i \le k$, and is denoted by $\sum_{i=1}^{k} N_i$.

Theorem 6.1.9: If $\{N_i\}_{1 \le i \le k}$ be a family of $R-$ submodules of a module M. Then

$$\sum_{i=1}^{k} N_i = \{x_1 + x_2 + \cdots + x_k \mid x_i \in N_i\}$$

Proof: Let

$$S = \sum_{i=1}^{k} N_i = \{x_1 + x_2 + \cdots + x_k \mid x_i \in N_i\}.$$

Consider $x, y \in S$

$$x = x_1 + x_2 + \cdots + x_k$$

and

$$y = y_1 + y_2 + \cdots + y_k; x_i, y_i \in N_i \ \forall \ 1 \le i \le k$$

Then

$$x - y = (x_1 + x_2 + \cdots + x_k) - (y_1 + y_2 + \cdots + y_k)$$

$$= (x_1 - y_1) + (x_2 - y_2) + \cdots + (x_k - y_k)$$

Since $x_i,\ y_i \in N_i$ and

N_i is an R −submodule of R −module M,

therefore, $x_i - y_i \in N_i\ \forall\, i$

Hence,

$$x - y = \sum_{i=1}^{k} (x_i - y_i) \in \sum_{i=1}^{k} N_i$$

Consider,

$$rx = r(x_1 + x_2 + \cdots + x_k) = rx_1 + rx_2 + \cdots + rx_k$$

Since $x_i \in N_i$, $r \in R$ and N_i is an R −submodule of R −module M, therefore, $rx_i \in N_i\ \forall\, i$

Hence,

$$rx = \sum_{i=1}^{k} rx_i \in \sum_{i=1}^{k} N_i$$

Also, for

$$r \in R,\ x = x_1 + x_2 + \cdots + x_k \in \sum_{i=1}^{k} N_i$$

we have proved that $rx \in \sum_{i=1}^{k} N_i$

So, $S = \sum_{i=1}^{k} N_i$ is a left R −submodule of R −module M.

Let K is any left R −submodule that contains each submodule N_i, then for $x_1 + x_2 + \cdots + x_k \in S$

$$x_i \in N_i \subseteq K\ \forall\, 1 \le i \le k$$

So, $x_i \in K\ \forall\, i$ and K being R −submodule is an additive group. That is, $x_1 + x_2 + \cdots + x_k \in K$.

Thus, K contains all elements of the form $x_1 + x_2 + \cdots + x_k;\ x_i \in N_i\ \forall\, 1 \le i \le k$.

That is, $S \subseteq K$.So, S is the smallest R −submodule of R −module M containing each N_i, $1 \le i \le k$.

Therefore, by definition of$\sum_{i=1}^{k} N_i$,

$$S = \sum_{i=1}^{k} N_i.$$

Remark 6.1.10: The sum $\sum_{i\in\Lambda} N_i$ of a family $\{N_i\}_{i\in\Lambda}$ of R −submodules of an $R -$ module M is defined similarly as the submodule generated by $\bigcup_{i\in\Lambda} N_i$. As done for a finite number of submodules, it can be easily observed that

$$\sum_{i\in\Lambda} N_i = \left\{ \sum_{finite} x_i \,\middle|\, x_i \in N_i \right\}$$

where $\sum_{finite} x_i$ stands for any finite sum of elements of R −submodules N_i, $i \in \Lambda$.

Definition 6.1.11: The sum $\sum_{i\in\Lambda} N_i$ of a family $\{N_i\}_{i\in\Lambda}$ of R −submodules of an $R -$ module M is called a direct sumif each element x of $\sum_{i\in\Lambda} N_i$ can be uniquely written as$x = \sum_i x_i$, where $x_i \in N_i$ and $x_i = 0$ for almost all $i \in \Lambda$.When the sum $\sum_{i\in\Lambda} N_i$ is direct, we write it as $\oplus \sum_{i\in\Lambda} N_i$.

If Λ is a finite set,$\{1,\ 2,\ \ldots,\ k\}$, then the direct sum $\oplus \sum_{i\in\Lambda} N_i$ is written as

$$N_1 \oplus N_2 \oplus \ldots \oplus N_k.$$

Each N_i in this direct sum is called a direct summand of the direct sum.

Theorem 6.1.12: Let $\{N_i\}_{1\le i\le k}$ be a family of $R-$ submodules of an $R-$ module M. Then the following are equivalent.

(i) $\sum_{i\in\Lambda} N_i$ is a direct sum.

(ii) $0 = \sum_i x_i \in \sum_{i\in\Lambda} N_i$ implies $x_i = 0\ \forall\ i$

(iii) $N_i \cap \sum_{j\in\Lambda,\ j\neq i} N_j = \{0\},\ i \in\Lambda$

i implies ii

Let $\sum_{i\in\Lambda} N_i$ is a direct sum.

Let $0 = \sum_i x_i \in \sum_{i\in\Lambda} N_i$

$$\sum_i x_i = 0$$

Also,

$$\sum_i 0 = 0$$

By definition of direct sum, representation of 0 as a sum of elements of $N_i,\ i\in\Lambda$ is unique. Hence, $x_i = 0\ \forall\ i$

ii implies iii

Let $0 = \sum_i x_i \in \sum_{i\in\Lambda} N_i$ implies $x_i = 0\ \forall\ i$.

Let $x \in N_i \cap \sum_{j\in\Lambda,\ j\neq i} N_j$

$x \in N_i$ implies $x = x_i \in N_i$

$x \in \sum_{j\in\Lambda,\ j\neq i} N_j$ implies $x = \sum_{j\in\Lambda,\ j\neq i} x_j$

That is $x_i = \sum_{j\in\Lambda,\ j\neq i} x_j$

This implies, $\sum_{j\in\Lambda} y_j = 0$ where $y_j = x_j\ \forall\ j\neq i$ and $y_i = -x_i$

From ii. we get $y_j = 0\ \forall\ j$

That is, $x_j = 0\ \forall\ j$

In particular, $x_i = 0$

Hence, $x = x_i = 0$

So, $N_i \cap \sum_{j\in\Lambda,\ j\neq i} N_j = \{0\}$

iii implies i

Let $N_i \cap \sum_{j\in\Lambda,\ j\neq i} N_j = \{0\}$

Let $x \in \sum_{i\in\Lambda} N_i$

Then by definition x can be expressed as a sum of elements of $N_i,\ i\in\Lambda$. If possible, let

$$x = \sum_{j\in\Lambda} x_j = \sum_{j\in\Lambda} y_j$$

This implies,

$$\sum_{j\in\Lambda} x_j - \sum_{j\in\Lambda} y_j = 0$$

That is,

$$\sum_{j\in\Lambda}(x_j - y_j) = 0$$

Choose any $i \in \Lambda$,

$$\Rightarrow \sum_{j\in\Lambda,\, j\neq i}(x_j - y_j) + (x_i - y_i) = 0$$

$$\Rightarrow \sum_{j\in\Lambda,\, j\neq i}(x_j - y_j) = -(x_i - y_i) \dots (1)$$

$x_i, y_i \in N_i$ and N_i is an R −submodule of an R −module M. Hence, $x_i - y_i \in N_i \dots (2)$

Similarly, $x_j, y_j \in N_j \ \forall j$ implies $x_j - y_j \in N_j$. That is,

$$\sum_{j\in\Lambda,\, j\neq i}(x_j - y_j) \in \sum_{j\in\Lambda, j\neq i} N_j \dots (3)$$

From (1), (2) and (3), we get,

$$x_i - y_i \in N_i \cap \sum_{j\in\Lambda, j\neq i} N_j$$

By ii

$$N_i \cap \sum_{j\in\Lambda, j\neq i} N_j = \{0\}$$

This implies,

$$x_i = y_i \forall\, i$$

That is, the expression of x as a sum of elements of $N_i; i \in\Lambda$ is unique. So,$\sum_{i\in\Lambda} N_i$ is a direct sum.

Theorem 6.1.13: Let R be a ring with unity. An R −module M is cyclic if and only if

$$M \cong \frac{R}{I}$$

for some left ideal I of R.

Proof: Let $M = Rx$ be a cyclic module generated by x.

Let $I = \{r \in R | rx = 0\}$

For $r_1, r_2 \in I,\ r \in R$

$$r_1x = 0,\ r_2x = 0$$

This implies, $r_1x - r_2x = 0 \Rightarrow (r_1 - r_2)x = 0$

That is, $r_1 - r_2 \in I$

Again $r(r_1x) = r0 = 0$

This implies, $rr_1 \in I$

Hence, I is a left ideal of R.

Define a mapping $f: R \to Rx$ by $f(r) = rx,\ r \in R$

So, f is an R −homomorphism and onto.

Also, $Ker\ f = \{r \in R | rx = 0\} = I$

So, by the Fundamental theorem of$R$ −homomorphisms,

$$\frac{R}{I} \cong Rx$$

Conversely,

Given that $M \cong \frac{R}{I}$

Since R is a ring with unity 1.

$$1 + I \in \frac{R}{I}$$

For $r + I \in \frac{R}{I}$, $r \in R$

$$r + I = 1r + I = (1 + I)(r + I)$$

So, $\frac{R}{I}$ is cyclic left R −module generated by $1 + I$.

Being isomorphic to a cyclic module,

M is a cyclic module.

Definition 6.1.14: Let R be a ring and M be an R −module. Then $RM = \{\sum_i r_i m_i \,|\, r_i \in R,\ m_i \in M\}$where the summation $\sum_i r_i m_i$ is a finite sum.An R −module M is called simple or irreducible if

$(i)\ RM \neq \{0\}$

$(ii)\ \{0\}$ and M are the only R −submodules of M.

Remark 6.1.15: If R is a ring with unity 1, $RM = \{0\}$ only if $M = \{0\}$

Proof: Let $RM = \{0\}$

Let $x \in M$

Since $1 \in R$, therefore, $1x = x \in RM$

But $RM = \{0\}$

This implies, $x = 0$

Hence, $M = \{0\}$.

Example:

Every field is a simple module over itself.

Proof: Let F be a field.

Since F is non-zero and a ring with unity, so, $RM = F^2 \neq \{0\}$.

Let N be an F −submodule of F −module F.

Let $N \neq \{0\}$

Then there exists at least one non-zero element $x \in N$

So, x is a non-zero element of N and hence of field F. Hence $x^{-1} \in F$.

By definition ofthe module, $x^{-1}x \in N$

That is, $1 \in N$

This implies $N = F$

Hence, $\{0\}$ and F are the only F −submodules of F.

Thus, every field is a simple module over itself.

Similarly, we can show that every division ring is a simple module over itself.

Example 6.1.16:

Let $R = F_2$ be the ring of 2×2 matrices over a field F.

Let $A = \left\{\begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix} \,|\, a, c \in F\right\}$. Then A is an R −submodule of R −module R.

Claim: A is simple.

Let $\{0\} \neq N$ be any R −submodule of A.

Then $\forall \begin{bmatrix} a & c \\ b & d \end{bmatrix} \in N \subseteq$ A, we have, $c = d = 0$.

Since $N \neq \{0\}$, therefore, atleast one of a or b is non-zero.

If $a \neq 0$, $b = 0$

Then for any $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \in R$

$$\begin{bmatrix} p & q \\ r & s \end{bmatrix}\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} pa & 0 \\ ra & 0 \end{bmatrix} \notin N$$

So, we arrive at a contradiction as N is a submodule of A.

If $a = 0$, $b \neq 0$

Then for any $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \in R$

$$\begin{bmatrix} p & q \\ r & s \end{bmatrix}\begin{bmatrix} 0 & 0 \\ b & 0 \end{bmatrix} = \begin{bmatrix} qb & 0 \\ sb & 0 \end{bmatrix} \notin N$$

So, we arrive at a contradiction as N is a submodule of A.

Therefore, $a, b \neq 0$

But in that case, $A = N$

Therefore, A has no proper submodule, and hence, A is a simple $R-$module.

Remark 6.1.17:A minimal left ideal in a ring R is not necessary a simple $R-$module.Let A be an additive abelian group of order p, p is a prime number. Defining multiplication in A as $ab = 0\ \forall\ a, b \in R$, we see that A is a ring. Then A is a minimal left ideal but A is not a simple $A-$module because $A^2 = \{0\}$.Note that a minimal left ideal in a ring R with unity is always a simple $R-$module.

Theorem 6.1.18: Let R be a ring with unity and let M be an $R-$module. Then the following statements are equivalent:

i. M is simple.

ii. $M \neq \{0\}$, and M is generated by any $0 \neq x \in M$

iii. $M \cong \frac{R}{I}$, where I is a maximal left ideal of R.

Proof:

i implies ii

Let $0 \neq x \in M$.

Then $< x > = Rx$ is a non-zero $R-$submodule generated by x.

From i, M is simple

So, $Rx = M$

That is, $M =< x >$.

ii implies i

Let $\{0\} \neq N$ be an $R-$submodule of M.

Let $0 \neq x \in N$.

Then by ii, $M =< x > \subseteq N$

Hence, $N = M$

This implies M is simple.

i implies iii

Because i implies ii, therefore $M = Rx$, for $x(\neq 0) \in M$

Define a map $f: R \to Rx$ by $f(a) = ax\ \forall\ a \in R$

***f* is *R* −homomorphism**

For $a, b, r \in R$, we have

$$f(a + b) = (a + b)x = ax + bx = f(a) + f(b)$$

and

$$f(ra) = (ra)x = r(ax) = rf(a)$$

Therefore, f is R −homomorphism.

f is onto

$\forall\ ax \in Rx$, there exists $a \in R$ such that $f(a) = ax$

Therefore, f is onto.

So, by the Fundamental theorem of R − homomorphism,

$$\frac{R}{Ker\ f} \cong Rx$$

Let $Ker\ f = I$

Then,

$$\frac{R}{I} \cong Rx = M$$

Since M is a simple module, R/I is a simple module.

We know that a submodule K of R/I is left ideal of R/I as ring and vice versa.

Since R/I is a simple module, so, it has no proper submodule and hence no proper left ideal as ring.

Thus, R/I is a simple ring.

If I is not maximal left ideal of R, then there exists some ideal J of R such that $I \subset J \subset R$.

But then R/J is a proper left ideal of R/I as rings which contradicts the fact that R/I is a simple ring.

Hence, I is a maximal left ideal of R.

iii implies i

From iii, $\frac{R}{I} \cong M$ where I is a maximal left ideal of R.

Because I is a maximal left ideal of R, so, R is the only left ideal properly containing I.

But any submodule of $\frac{R}{I}$ is of type $\frac{U}{I}$ where U is a submodule of R containing I.

Therefore, R/I has no proper submodule hence, $\frac{R}{I}$ is a simple module.

Being isomorphic to $\frac{R}{I}$, M is a simple R −module.

6.2 Semi-Simple Modules and Schur's Lemma

Definition 6.2.1: An R −module M is called semi-simple or completely reducible if

$$M = \sum_{\alpha \in \Lambda} M_{\alpha},$$

where M_{α} are simple R −submodules.

Example 6.2.2:

Let $R = F_2$ be the ring of 2×2 matrices over a field F. Show that R is a semi-simple F −module.

Sol.

Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R;\ a,\ b,\ c,\ d \in F$

Let $A = \left\{\begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} \middle| a,\ c \in F\right\}$ and $B = \left\{\begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} \middle| b,\ d \in F\right\}$

We have already proved that A is a simple module. Similarly, we can show that B is a simple module.

Also,

$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R$,

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} + \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} \in A + B$

Hence, $R = A + B$; where A and B are simple R −submodules.

Hence, R is semi-simple.

Theorem 6.2.3:Let $M = \sum_{\alpha \in \Lambda} M_\alpha$ be a sum of simple R − submodules M_α. Let K be a submodule of M. Then there exists a subset Λ' of Λ such that $\sum_{\alpha \in \Lambda'} M_\alpha$ is a direct sum, and

$$M = K \oplus \left(\oplus \sum_{\alpha \in \Lambda'} M_\alpha \right)$$

Proof:

Let $S = \{ A \subset \Lambda \mid \sum_{\alpha \in A} M_\alpha$ is a direct sum, and $K \cap \sum_{\alpha \in A} M_\alpha = \{0\}\}$.

If $A = \phi$, we take $\sum_{\alpha \in A} M_\alpha$ as $\{0\}$.

Clearly, $\phi \in S$, $S \neq \phi$.

S is partially ordered by inclusion, and every chain $\{A_i\}$ in S has an upper bound $\bigcup_i A_i$ in S.

By Zorn's lemma, S has a maximal member, say A.

Let

$$N = K \oplus \left(\oplus \sum_{\alpha \in A} M_\alpha \right)$$

Claim:$N = M$

Let $\beta \in \Lambda$, M_β is simple,

either $M_\beta \cap N = \{0\}$ or $M_\beta \cap N = M_\beta$.

If $M_\beta \cap N = \{0\}$

Let $x \in M_\beta \cap \sum_{\alpha \in A} M_\alpha$

Then $x \in M_\beta$ and $x \in \sum_{\alpha \in A} M_\alpha$

Also, $N = K \oplus (\oplus \sum_{\alpha \in A} M_\alpha)$

That is, $\oplus \sum_{\alpha \in A} M_\alpha \subseteq N$

This implies, $x \in M_\beta \cap N = \{0\}$

Hence, $x = 0$

That is, $M_\beta \cap \sum_{\alpha \in A} M_\alpha = \{0\}$.

So, $\sum_{\alpha \in A \cup \{\beta\}} M_\alpha$ is a direct sum.

Also, by choice of A, $K \cap \sum_{\alpha \in A} M_\alpha = \{0\}$ ... (1)

Also, $M_\beta \cap N = \{0\}$ and $K \subseteq N$

Therefore, $M_\beta \cap K = \{0\}$ ... (2)

From (1) and (2),

$$\left(K \cap \oplus \sum_{\alpha \in A} M_\alpha \right) \oplus (K \cap M_\beta) = \{0\}$$

That is,

$$K \cap \left(\oplus \sum_{\alpha \in A \cup \{\beta\}} M_\alpha \right) = \{0\}$$

which implies that $A \cup \{\beta\} \in S$

By the choice of A, A is the maximal member of S.

Therefore, $\beta \in A$

This implies, $\forall\, \beta \in \Lambda$, $M_\beta \subset N$, which implies, $N = M$.

Corollary 6.2.4: Let $M = \sum_{\alpha \in \Lambda} M_\alpha$ be a sum of the family of simple $R-$submodules M_α. Then there exists a subfamily Λ' of Λ such that $\sum_{\alpha \in \Lambda'} M_\alpha$ is a direct sum, and

$$M = \oplus \sum_{\alpha \in \Lambda'} M_\alpha$$

Proof: By taking $K = \{0\}$, in the theorem, we get this result.

Lemma 6.2.5: If A and B are $R-$modules, then

$$\frac{A + B}{A} \cong \frac{B}{A \cap B}$$

Proof: Define a map

$$f: A + B \to \frac{B}{A \cap B}$$

as $f(a + b) = b + (A \cap B)\ \forall\, a + b \in A + B$

***f* is well defined**

Let $a + b = a' + b'$; $a, a' \in A$; $b, b' \in B$

This implies $a - a' = b' - b$

$a - a' \in A$ and $b' - b \in B$

So, $b - b' \in A \cap B$

That is $b + (A \cap B) = b' + (A \cap B)$

or, $f(a + b) = f(a' + b')$

So, f is well defined.

***f* is $R-$homomorphism**

Let $a, a' \in A$; $b, b' \in B$, $r \in R$

Then

$$\begin{aligned} f((a + b) + (a' + b')) &= f(a + a' + b + b') \\ &= b + b' + (A \cap B) \\ &= (b + (A \cap B)) + (b' + (A \cap B)) \\ &= f(a + b) + f(a' + b') \end{aligned}$$

Again,

$$\begin{aligned} f(r(a + b)) &= f(ra + rb) \\ &= rb + (A \cap B) \\ &= r(b + (A \cap B)) \\ &= r(f(a + b)) \end{aligned}$$

Hence, f is R −homomorphism.

***f* is onto**

$\forall\, b + (A \cap B) \in \frac{B}{A \cap B}$

There exists $b \in B$. Consider any element $a \in A$,

Then $f(a + b) = b + (A \cap B)$

Hence, f is onto.

So, by the Fundamental theorem of R −homomorphism, we get,

$$\frac{A+B}{Ker\, f} \cong \frac{B}{A \cap B} \ldots (1)$$

$$Ker\, f = \{a + b \mid a \in A,\ b \in B, \text{ and } b + (A \cap B) = A \cap B\}$$

$$= \{a + b \mid a \in A,\ b \in B, \text{ and } b \in A \cap B\}$$

$$= \{a + b \mid a \in A,\ b \in A \cap B\} = A$$

From (1)

$$\frac{A+B}{A} \cong \frac{B}{A \cap B}$$

Theorem 6.2.6: Let M be a semi-simple module and K be a non-zero submodule of M. Then K is semi-simple and K is a direct summand of M.

Proof: Since M is a completely reducible module, therefore,

$M = \sum_{\alpha \in \Lambda} M_\alpha$, where M_α are simple modules.

Also, we have proved that, if K is a submodule of M, then there exists $\Lambda' \subset \Lambda$ such that

$$M = K \oplus \left(\oplus \sum_{\alpha \in \Lambda'} M_\alpha \right) \ldots (1)$$

which shows that K is a direct summand of M.

Also, by lemma and the fact that $K \cap (\oplus \sum_{\alpha \in \Lambda'} M_\alpha) = \{0\}$, we get,

$$\frac{K \oplus (\oplus \sum_{\alpha \in \Lambda'} M_\alpha)}{\oplus \sum_{\alpha \in \Lambda'} M_\alpha} \cong \frac{K}{\{0\}}$$

This implies,

$$\frac{M}{\oplus \sum_{\alpha \in \Lambda'} M_\alpha} \cong K$$

or,

$$\frac{\sum_{\alpha \in \Lambda} M_\alpha}{\oplus \sum_{\alpha \in \Lambda'} M_\alpha} \cong K \ldots (2)$$

Let $\Lambda'' = \Lambda - \Lambda'$

so that

$$\sum_{\alpha \in \Lambda} M_\alpha = \sum_{\alpha \in \Lambda'} M_\alpha + \sum_{\alpha \in \Lambda''} M_\alpha$$

That is,

$$\sum_{\alpha \in \Lambda} M_\alpha = \oplus \sum_{\alpha \in \Lambda'} M_\alpha + \sum_{\alpha \in \Lambda''} M_\alpha \ldots (3)$$

Claim: $\oplus \sum_{\alpha \in \Lambda'} M_\alpha \oplus \sum_{\alpha \in \Lambda''} M_\alpha$ is a direct sum.

Consider $M_\beta \cap M_\gamma$, where $\beta, \gamma \in \Lambda''$ such that $\beta \neq \gamma$

Since $M_\beta \cap M_\gamma \subseteq M_\gamma$ and M_γ is simple,

therefore, $M_\beta \cap M_\gamma = M_\gamma$ or $\{0\}$

If $M_\beta \cap M_\gamma = M_\gamma$, then $M_\gamma \subseteq M_\beta$, which is not possible as M_β is simple. Also, $M_\gamma \neq M_\beta$ and $M_\gamma \neq \{0\}$.

Therefore, $M_\beta \cap M_\gamma = \{0\}$.

Hence, $\sum_{\alpha\in\Lambda''} M_\alpha$ is a direct sum.

Similarly, if we consider $M_\delta \cap M_\epsilon$ where $\delta \in \Lambda'$ and $\epsilon \in \Lambda''$, we get that $M_\delta \cap M_\epsilon = \{0\}$,

which shows that $\oplus \sum_{\alpha\in\Lambda'} M_\alpha \oplus \sum_{\alpha\in\Lambda''} M_\alpha$ is a direct sum.

Also, from (2), we have,

$$\frac{\sum_{\alpha\in\Lambda} M_\alpha}{\oplus \sum_{\alpha\in\Lambda'} M_\alpha} \cong K$$

From (3),

$$\frac{\oplus \sum_{\alpha\in\Lambda'} M_\alpha + \sum_{\alpha\in\Lambda''} M_\alpha}{\oplus \sum_{\alpha\in\Lambda'} M_\alpha} \cong K$$

From the claim,

$$\frac{\oplus \sum_{\alpha\in\Lambda'} M_\alpha \oplus \sum_{\alpha\in\Lambda''} M_\alpha}{\oplus \sum_{\alpha\in\Lambda'} M_\alpha} \cong K$$

Using lemma, we get,

$$\frac{\oplus \sum_{\alpha\in\Lambda''} M_\alpha}{(\oplus \sum_{\alpha\in\Lambda'} M_\alpha) \cap (\oplus \sum_{\alpha\in\Lambda''} M_\alpha)} \cong K$$

This implies,

$$\frac{\oplus \sum_{\alpha\in\Lambda''} M_\alpha}{\{0\}} \cong K$$

That is,

$$K \cong \oplus \sum_{\alpha\in\Lambda''} M_\alpha$$

where M_α are simple submodules of K.

Hence, K is completely reducible.

Theorem 6.2.7: Let M be a semi-simple module and $K \neq M$ be a submodule of M. Show that $\frac{M}{K}$ is completely reducible.

Proof: Since M is a completely reducible module, therefore there exist simple $R-$modules M_α, $\alpha \in \Lambda$ such that

$$M = \sum_{\alpha\in\Lambda} M_\alpha$$

Therefore,

$$M = K \oplus \left(\oplus \sum_{\alpha\in\Lambda'} M_\alpha\right)$$

for some $\Lambda' \subseteq \Lambda$.

Also,

$$\frac{K \oplus (\oplus \sum_{\alpha\in\Lambda'} M_\alpha)}{K} \cong \frac{\oplus \sum_{\alpha\in\Lambda'} M_\alpha}{K \cap (\oplus \sum_{\alpha\in\Lambda'} M_\alpha)}$$

This implies,

$$\frac{M}{K} \cong \frac{\oplus \sum_{\alpha\in\Lambda'} M_\alpha}{\{0\}}$$

That is,

$$\frac{M}{K} \cong \oplus \sum_{\alpha \in \Lambda'} M_\alpha$$

Therefore, M/K is isomorphic to the direct sum of simple submodules.

Hence M/K is a completely reducible module.

Lemma 6.2.8 (Schur's Lemma): Let M be a simple R −module. Then $Hom_R(M, M)$ is a division ring.

Proof:

We know that $Hom_R(M, M)$ is a subring of $Hom(M, M)$, so, $Hom_R(M, M)$ is a ring.

To prove that it is a division ring, it is sufficient to prove that every non-zero element of $Hom_R(M, M)$ is a unit.

Let $0 \neq \phi \in Hom_R(M, M)$.

Consider the R −submodules $Ker\ \phi$ and $Im\ \phi$ of M.

Now, M is a simple R −module.

Therefore, $Ker\ \phi = M$ or $\{0\}$.

Similarly, $Im\ \phi = M$ or $\{0\}$.

If $Ker\ \phi = M$, then $\phi = 0$ but $\phi \neq 0$, therefore, $Ker\ \phi = \{0\}$.

Also, $Im\ \phi = \{0\}$, then $\phi = 0$ but $\phi \neq 0$, therefore, $Im\ \phi = M$.

$Ker\ \phi = \{0\}$ implies ϕ is 1-1.

$Im\ \phi = M$ implies ϕ is onto.

Hence, ϕ is bijective which proves that ϕ is invertible.

So, every non-zero element of $Hom_R(M, M)$ is a unit.

Task:

1. Let M be a completely reducible module and let $K \neq M$ be a submodule of M. Show that M/K is completely reducible.
2. Show that $\frac{Z}{<pq>}$ is a completely reducible Z −module, where p and q are distinct prime numbers.

6.3 Free Modules

Definition 6.3.1: A list –that is, a finite sequence $x_1, x_2, \ldots, x_n$ of elements of an $R-$ module M is called linearly independent if, for any $a_1, a_2, \ldots, a_n \in R, a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$ implies, $a_i = 0\ \forall\ 1 \leq i \leq n$. A finite sequence is called linearly dependent if it is not linearly independent.

A subset S of an R −module M is called linearly independent if every finite sequence of distinct elements of S is linearly independent. Otherwise, it is called linearly dependent.

That is, if S contains at least one sequence of distinct elements which is linearly dependent, then S is linearly dependent.

Examples 6.3.2:

- Let F be a field. Consider F as F −module. Then the set $\{1, x, x^2, x^3, \ldots\}$ is linearly independent in $F[x]$.
- Let F be a field. Consider F as F −module. Then the set $\{1, x, 1 + x, x^2, \ldots\}$ is linearly dependent in $F[x]$.
- Let M be an R −module. The set $\{0\}$ is always linearly dependent if R is the ring with unity.
- Let R be a ring with unity. Let $M = R^n$ be an $R-$ module.

Then the set $\{e_1, e_2, \ldots, e_n\}$ is linearly independent, where e_i is the $n-$tuple with $i-th$

entry 1, all others zero.

- Let F be a field. Then $M = F_2$ is the set of all square matrices of order 2 with entries from F, is a F −module.

Then the set $\left\{\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}, \begin{bmatrix}0 & 1\\0 & 0\end{bmatrix}, \begin{bmatrix}0 & 0\\1 & 0\end{bmatrix}, \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}\right\}$ is a linearly independent set.

Definition 6.3.3:A subset B of an R −module M is called a basis of M if

i. M is generated by B.

ii. B is a linearly independent set.

The set $\{e_1, e_2, \ldots, e_n\}$ is a basis of $M = R^n$, where R is a ring with unity and e_i is the n −tuple with $i - th$ entry 1, all others zero.

Example 6.3.4:

Let R be a ring with unity {1}. Then R −module R has a basis {1} or $\{u\}$, where u is a unit. Let $\alpha \in R$ and u is a unit in R. Then clearly, $\alpha = u(u^{-1}\alpha) \in \ < u >$. Hence, $\{u\}$ generates R.

Again, let $\alpha \in R$ such that $u\alpha = 0$.

Since u is a unit so $u^{-1} \in R$,

Pre-multiplying both sides by u^{-1}, we get,

$$u^{-1}(u\alpha) = 0$$

That is,

$$\alpha = 0$$

This implies $\{u\}$ is linearly independent.

Hence, it is a basis of R −module R.

Remark 6.3.5: Not every module has a basis.

Consider a cyclic group G, regard G as a Z −module.

Claim:G has a basis if and only if it is infinite.

Let $G = \ < a >$ has a basis.

Let ma be any element of the basis of G.

Then $\{ma\}$ must be linearly independent.

That is $\lambda(ma) = 0, \lambda \in Z$ if and only if $\lambda = 0$

If G is finite. That is $O(G) = n$.

Then, $n(ma) = 0; n \neq 0$

So, we arrive at a contradiction.

Hence, G must be infinite.

Conversely,

let $G = \ < a >$ is an infinite cyclic group.

Then clearly,$\{a\}$ is a basis of G as a Z −module.

Definition 6.3.6: An R −module M is called a free module if M admits a basis. In other words, M is free if there exists a subset S of M such that $M = \ < S >$, and S is a linearly independent set. We consider {0} as a free module with empty set as the basis.

Example 6.3.7: The$\mathbb{Z}$ −module $\mathbb{Q}$ is not free.

If possible, let $\mathbb{Q}$ has a basis B.

Let B has more than one element.

Then we can choose $\alpha_1 = \frac{m_1}{n_1}, \alpha_2 = \frac{m_2}{n_2} \in B$ such that $\alpha_1 \neq \alpha_2$, $m_1, n_1, m_2, n_2 \in \mathbb{Z} - \{0\}$.

Now $m_2 n_1 \alpha_1 + (-m_1) n_2 \alpha_2 = 0$

Also, $m_2 n_1$ and $-m_1 n_2$ both are non-zero integers.

This proves that $\{\alpha_1, \alpha_2\}$ is a linearly dependent set. But being a subset of basis B, $\{\alpha_1, \alpha_2\}$ is L. I.

So, we arrive at a contradiction.

That means, B contains only one element.

Now, let $b = \{\alpha\}$

That means $\mathbb{Q} =< \alpha >$

Now, $\alpha \in \mathbb{Q}$

This implies, $\alpha^2 \in \mathbb{Q} =< \alpha >$

That is, $\alpha^2 = k\alpha; k \in \mathbb{Z}$

This implies, $\alpha = k \in \mathbb{Z}$

This means $\mathbb{Q} \subseteq \mathbb{Z}$, which is not true.

That means $\mathbb{Q}$ has no basis over$\mathbb{Z}$.

Hence, it is not a free module.

Example 6.3.8:

A submodule of a free module need not be a free module.

Consider $R = \mathbb{Z}_6$ as R −module.

Then R is free R −module with basis {1}.

Consider $S = 2\mathbb{Z}_6$

Then S is a R −submodule.

If possible, let S has a basis $\{x_1, x_2, \dots, x_n\}$ over R.

Then every element x of S can be expressed as

$x = r_1 x_1 + r_2 x_2 + \cdots + r_n x_n$where $r_i \in R$

Since R contains 6 elements, so, x has 6^n choices.

This implies, S contains 6^n elements for some natural number n.

But we know that S has 3 elements.

So, we arrive at a contradiction. Hence, S is not a free R −module.

Theorem: Let M be a free R −module with a basis $\{e_1, e_2, \dots, e_n\}$. Then $M \cong R^n$.

Proof: Define a mapping $\phi: M \to R^n$ by

$$\phi\left(\sum_{i=1}^{n} r_i e_i\right) = \sum_{i=1}^{n} r_i f_i$$

where, $f_i = (0, 0, \dots, 0, 1, 0, \dots 0) \in R^n$

ϕ is well-defined.

Let

$$\sum_{i=1}^{n} r_i e_i = \sum_{i=1}^{n} r_i' e_i$$

This implies,

$$\sum_{i=1}^{n} r_i e_i - \sum_{i=1}^{n} r_i' e_i = 0$$

That is

$$\sum_{i=1}^{n} (r_i - r_i')e_i = 0$$

Using linear independence of $\{e_1, e_2, \ldots, e_n\}$,

we get that $r_i - r_i' = 0 \; \forall \, i$

Hence, $r_i = r_i' \; \forall \, i$

Therefore, ϕ is well-defined.

Now, we prove that ϕ is R −homomorphism

Let $m = \sum_{i=1}^{n} r_i e_i$,

$$m' = \sum_{i=1}^{n} r_i' e_i$$

and $r \in R$

Consider

$$\phi(m + m') = \phi\left(\sum_{i=1}^{n} r_i e_i + \sum_{i=1}^{n} r_i' e_i\right)$$

$$= \phi\left(\sum_{i=1}^{n} (r_i + r_i')e_i\right)$$

$$= \sum_{i=1}^{n} (r_i + r_i')f_i$$

$$= \sum_{i=1}^{n} r_i f_i + \sum_{i=1}^{n} r_i' f_i$$

$$= \phi(m) + \phi(m')$$

Also,

$$\phi(rm) = \phi\left(r \sum_{i=1}^{n} r_i e_i\right)$$

$$= \phi\left(\sum_{i=1}^{n} r(r_i e_i)\right)$$

$$= \sum_{i=1}^{n} (r r_i) f_i$$

$$= r\sum_{i=1}^{n}(r_i f_i)$$

$$= r\sum_{i=1}^{n}(r_i f_i)$$
$$= r\phi(m)$$

Therefore, ϕ is R −homomorphism.

ϕ is 1-1

Let $\sum_{i=1}^{n} r_i e_i \in Ker\,\phi$

Then $\phi(\sum_{i=1}^{n} r_i e_i) = 0$

That is, $\sum_{i=1}^{n} r_i f_i = 0$

By linear independence of $f_1, f_2, \ldots, f_n$,

we get that $r_i = 0\ \forall\ i$

That is, $\sum_{i=1}^{n} r_i e_i = 0$.

Hence, $Ker\ \phi = \{0\}$ and ϕ is 1-1.

ϕ is onto

Since $\{f_1, f_2, \ldots, f_n\}$ is a basis of R^n, therefore for every $y \in R^n$, there exist unique $r_1, r_2, \ldots, r_n \in R$ such that

$$y = \sum_{i=1}^{n} r_i f_i$$

Consider

$$x = \sum_{i=1}^{n} r_i e_i \in M$$

Then $\phi(x) = y$

Hence, ϕ is onto.

Therefore, $M \cong R^n$.

Theorem 6.3.9: Let M be a finitely generated free module over a commutative ring R. Then all the bases of M are finite.

Proof: Let $B = \{e_i\}$, $i \in \wedge$, be a basis of M, and let $\{x_1, x_2, \ldots, x_n\}$ be a set of generators of M.

Then each x_j can be expressed as

$$x_j = \sum_i \alpha_{ij} e_i\ ; \alpha_{ij} \in R$$

Also, all but finitely many $\alpha_{ij}{'}s$ are zero.

Thus, the set of those $e_i's$ that occur in the expression of all the $x_j's$, $1 \le j \le n$ is finite.

These many $e_i's$ being part of the linearly independent set are linearly independent.

So, finitely many $e_i's$ will become the basis.

Hence, M has a finite basis.

Since B is an arbitrary basis of M, so we can say that every basis of M is finite.

Lemma 6.3.10: if for a commutative ring with unity R, we have $R^n \cong R^m$, then $m = n$.

Proof: Let $R^n \cong R^m$, $m < n$

Let $\phi: R^m \to R^n$ be an R −isomorphism.

Since ϕ is 1-1 and onto, therefore, there exists a $\psi = \phi^{-1}$.

Let $\{e_1, e_2, \ldots, e_m\}$ and $\{f_1, f_2, \ldots, f_n\}$ be ordered bases of R^m and R^n respectively.

Let us write

$$\phi(e_i) = \sum_{j=1}^{n} a_{ji} f_j ; 1 \le i \le m$$

and

$$\Psi(f_j) = \sum_{i=1}^{m} b_{ij} e_i ; 1 \le j \le n$$

Let $A = [a_{ji}]$ and $B = [b_{kj}]$ be $n \times m$ and $m \times n$ matrices.

Then

$$\Psi(\phi(e_i)) = \sum_{k=1}^{m} \sum_{j=1}^{n} b_{kj} a_{ji} e_k , 1 \le i \le m$$

Thus, by the linear independence of the $e_i's$ and by the fact that $\Psi = \phi^{-1}$, we have,

$$\sum_{j=1}^{n} b_{kj} a_{ji} = \delta_{ki}$$

These yields

$$BA = I_m$$

That is the identity matrix of order m.

Similarly, $AB = I_n$

Let us consider the augmented matrices,

$A' = [A \quad 0]$ and $B' = \begin{bmatrix} B \\ 0 \end{bmatrix}$ where each of 0 is a zero matrix of appropriate size.

Then

$$A'B' = I_n, \; B'A' = \begin{bmatrix} I_m & 0 \\ 0 & 0 \end{bmatrix}$$

This implies $\det(A'B') = 1$ and $\det(B'A') = 0$

But A', B' are square matrices of order n over a commutative ring. So $\det(A'B') = \det(B'A')$.

So, we arrive at a contradiction.

Hence, $m \ge n$

By symmetry, $n \ge m$

Hence $n = m$.

Theorem 6.3.11: Let M be a finitely generated free module over a commutative ring R. Then all the bases of M have the same number of elements.

Proof: Let M be a free R −module. Let M has two bases B and B'.

If possible, let the number of elements in B and B' be m and n respectively.

Since B is a basis of M having m elements, therefore, $M \cong R^m$

Also, since B' is a basis of M having n elements, therefore

$$M \cong R^n$$

We know that relation of R −isomorphism is an equivalence relation. Therefore, we get,

$$R^m \cong R^n$$

Using the Lemma, we get,

$$n = m$$

Definition 6.3.12: The number of elements in any basis of a finitely generated free module M over a ring R with unity is called the rank of M, written as $rank\, M$.In particular, if R is a field or division ring then the rank is the same as the dimension defined for vector spaces.

Examples 6.3.13: Every finitely generated module is a homomorphic image of a finitely generated free module.

Proof: Let M be a finitely generated R −module and $\{x_1, x_2, \ldots, x_n\}$ is the set of generators of M.

Let e_i be the n −tuple with all entries 0 except at the $i-th$ place, where the entry is 1.

Then $\{e_1, e_2, \ldots, e_n\}$ are linearly independent over R and generate a free module R^n.

Define a map $\phi: R^n \to M$ by

$$\phi\left(\sum_{i=1}^{n} r_i e_i\right) = \sum_{i=1}^{n} r_i x_i$$

Because each $x \in R^n$ has a unique representation as $\sum_{i=1}^{n} r_i e_i$, therefore, ϕ is well defined.

Further, if $x = \sum_{i=1}^{n} r_i e_i$, $y = \sum_{i=1}^{n} r_i' e_i$ and $r \in R$,

then

$$\phi(x+y) = \phi\left(\sum_{i=1}^{n} r_i e_i + \sum_{i=1}^{n} r_i' e_i\right)$$

$$= \phi\left(\sum_{i=1}^{n} (r_i + r_i') e_i\right)$$

$$= \sum_{i=1}^{n} (r_i + r_i') x_i$$

$$= \sum_{i=1}^{n} r_i x_i + \sum_{i=1}^{n} r_i' x_i$$

$$= \phi(x) + \phi(y)$$

Also,

$$\phi(rx) = \phi\left(r \sum_{i=1}^{n} r_i e_i\right)$$

$$= \phi\left(\sum_{i=1}^{n} r(r_i e_i)\right)$$

$$= \sum_{i=1}^{n} (r r_i) x_i$$

$$= r \sum_{i=1}^{n} (r_i x_i)$$

$$= r\phi(x)$$

Therefore, ϕ is R −homomorphism.

ϕ is onto

Let $y \in M$. Since $\{x_1, x_2, \ldots, x_n\}$ is the set of generators of M.

So, there exist $r_i \in R$ for $1 \leq i \leq n$ such that

$$y = \sum_{i=1}^{n} r_i x_i$$

Since $\{e_1, e_2, \ldots, e_n\}$ is a basis of R^n over R, therefore,

$$x = \sum_{i=1}^{n} r_i e_i \in R^n$$

Note that $\phi(x) = y$

Hence, ϕ is onto

If $K = Ker\ \phi$,

then by the Fundamental Theorem of R −homomorphism, we have,

$$\frac{R^n}{K} \cong M$$

That is, M is isomorphic to homomorphic image R^n/K of a finitely generated free module over R.

Theorem 6.3.14: Let V be a vector space over a field F with a basis $\{e_i\}_{i\in\wedge}$. Then

i. $V = \oplus \sum_{i\in\wedge} Fe_i \cong \oplus \sum_{i\in\wedge} F_i,\ F_i = F$.

ii. V is semi-simple.

iii. If W is a subspace of V, then there exists a subspace W' such that $V = W \oplus W'$.

Proof: Given that $\{e_i\}_{i\in\wedge}$ is a basis of V.

$\forall\ x \in V$, x can be uniquely expressed as $x = \sum_{finite} \alpha_i e_i;\ \alpha_i \in F$

Thus $x \in \sum_{i\in\wedge} Fe_i$

That is $x \in \oplus \sum_{i\in\wedge} Fe_i$

Hence $V = \oplus \sum_{i\in\wedge} Fe_i$

Define a function $\phi: Fe_i \to F$ as $\phi(\alpha e_i) = \alpha\ \forall\ \alpha \in F$

ϕ is one-one, onto, R −homomorphism.

This implies, $Fe_i \cong F\ \forall\ i \in \Lambda$ which proves part i.

For part ii.

V is called semi-simple if $V = \oplus \sum_{i\in\wedge} W_i$; W_i is a simple subspace of V.

From i, $V = \oplus \sum_{i\in\wedge} F_i; F_i = F$ being a field is simple.

Hence, V is semi-simple.

For part iii.

$V = \oplus \sum_{i\in\wedge} Fe_i$ is semi-simple.

W is a subspace of V then there exists $\Lambda' \subset \Lambda$ such that

$$V = W \oplus \left(\oplus \sum_{i\in\wedge'} Fe_i \right)$$

$= W \oplus W'; W' = \oplus \sum_{i\in\wedge'} Fe_i$ is a subspace of V.

Summary

- The method to find the generating set of a given subset S of an R −module M **is explained.**
- the cyclic module is defined, and its structure is observed.
- Generating a set of the sum of R −modules is found by taking their union.
- semi-simple or completely reducible modules are defined.
- proved that an R −submodule and a quotient module of a semi-simple module is semi-simple

- basis of a free moduleis defined, and it has been analyzed that not every module is a free module
- proved that every basis of a free module has the same number of elements
- defined rank of a free module and observed that a vector space is always semi-simple

Keywords

- Generating set of a module
- Cyclic module
- Semi-simple module
- Quotient module
- Free module
- The rank of a free module

Self Assessment

1. Let M be an $R-$module and $x \in R$. Then the smallest $R-$submodule of M containing x is given by

A. $\{rx + nx | r \in R, n \in Z\}$
B. $\{rx | r \in R\}$
C. $\{nx | n \in Z\}$
D. $\{rn + x | r \in R, n \in Z\}$

2. The smallest $R-$submodule of an $R-$module M containing a non-empty subset S of M is obtained by

A. Taking the union of all the $R-$submodules of $R-$module M which contain S
B. Taking intersection of all the $R-$submodules of $R-$module M which contain S
C. Taking the finite sum of all the $R-$submodules of $R-$module M which contain S
D. Taking the product of all the $R-$submodules of $R-$module M which contain S

3. Smallest generating set of the $Z-$module Z consists of … number of elements

A. 0
B. 1
C. 2
D. Infinitely many

4. Let M be a simple $R-$ module then

A. $RM = \{0\}$
B. $RM = \{1\}$
C. $RM = \{0,1\}$
D. $RM \neq \{0\}$

5. The number of proper submodules of a simple module is

A. 0
B. 1
C. 2
D. Infinite

6. Let R be a ring with unity. Then consider the statements

I. M is a cyclic R module
II. M is isomorphic to a quotient module of R given by R/I, where I is left ideal of R

A. I implies II but II does not imply I
B. II implies I but I does not imply II
C. I implies II and II implies I
D. Neither I implies II, nor II implies I

7. Let N and P be submodules of an R module M. Then $M = N \oplus P$ implies that
A. $N \cap P = \{0\}$
B. $N \cap P = \phi$
C. $N \cup P = M$
D. $N \cup P = \{0\}$

8. Consider the statements and choose the correct option
I. Every simple R −module is semi-simple
II. Every semi-simple R −module is simple
A. Statement I is true and II is false
B. Statement II is true, and I is false
C. Statement I and II both are true
D. Statement I and II both are false

9. True/ False Every semi-simple module can be expressed as a direct sum of some of its simple sub-modules
A. True
B. False

10. Let G be a free cyclic module over the ring of integers. Then the number of elements in G is
A. 1
B. 2
C. Any finite number
D. Infinite

11. Choose the correct statement
A. Every Z −module is free
B. Submodule of a free module is always free
C. Z −module Q is not free (Q denotes the ring of rational numbers)
D. A cyclic Z −module is free

12. Let M be a free R −module with a basis having m elements. Then $M \cong R^n$; where n is a natural number
A. $n < m$
B. $n > m$
C. $n \geq m$
D. $n = m$

13. A finitely generated vector space V over a field F, considered as an F −module is always
A. Free module
B. Semi-simple module
C. Isomorphic to $F^n; n \in N$
D. All options are true

14. True/False Let M be a finitely generated free R −module. Then M always has a unique basis.
A. True
B. False

15. Let B and B' be bases of a finitely generated free R −module M having m and n number of elements respectively. Then
A. m and n are both infinite
B. m and n are both finite and $m < n$
C. m and $n$are both finite and $m > n$

D. m and n are both finite and $m = n$

Answers for Self Assessment

1.	**A**	**2.**	**B**	**3.**	**B**	**4.**	**D**	**5.**	**A**
6.	**C**	**7.**	**A**	**8.**	**A**	**9.**	**A**	**10.**	**D**
11.	**C**	**12.**	**D**	**13.**	**D**	**14.**	**B**	**15.**	**D**

Review Questions

1. Let R be a ring with unity Show that R as an $R-$module is completely reducible if and only if each $R-$module M is completely reducible.
2. Let A and B be rings such that A and B are completely reducible modules as $A-$module and $B-$module respectively. Let $R = A \oplus B$ be the ring direct sum of A and B. Show that R is completely reducible as $R-$module.
3. Let R be a commutative ring with unity and let $e \neq 0, 1$ be idempotent. Prove that Re can not be a free $R-$module.
4. Prove that the direct product $M_1 \times M_2 \times ... \times M_k$ of free $R-$modules M_i is again a free $R-$module.
5. Let $\{x_i\}_{i\in\Lambda}$ be a basis of a free $R-$module M. Prove that $M = \oplus \sum_{i\in\Lambda} Rx_i$.

Further Readings

- Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress
- Topics in algebra by I.N. Hartstein, Wiley
- Abstract algebra by David S Dummit and Richard M Foote, Wiley

Weblinks

- https://nptel.ac.in/courses/111/102/111102009/
- https://nptel.ac.in/courses/111/105/111105112/#

Unit 07: Noetherian and Artinian Modules

CONTENTS

Objective

After studying this unit, you will be able to

- define Noetherian and Artinian modules and rings,
- understand Noetherian and Artinian modules and rings with examples,
- understand left and right Noetherian (Artinian) rings,
- prove with examples that a right Noetherian (Artinian) ring may not be left Noetherian (Artinian),
- see the relation between nilpotent and nil ideals in an Artinian or Noetherian ring,
- state and prove Hilbert Basis Theorem,
- analyze that this theorem is not true for Artinian rings,
- prove an important characterization of Noetherian rings in terms of its prime ideals.

Introduction

In this unit, you will be introduced to Noetherian and Artinian rings and modules and understand the concept of Noetherian and Artinian rings and modules with the help of examples. The concept of left and right Noetherian (Artinian) rings is defined. It will be proved that the right (left) Noetherian (Artinian) ring may not be left (right) Noetherian (Artinian). Nil and nilpotent ideals are proved. Hilbert basis theorem is proved.

7.1 Noetherian and Artinian Modules and Rings

Definition 7.1.1: Let $M = \bigoplus \sum_{i=1}^{k} M_i$ be an $R-$module which is a direct sum of $R-$modules M_i.

Then for any $m \in M$, m can be uniquely expressed as

$$m = \sum_{i=1}^{k} m_i \ ; m_i \in M_i$$

In other words, every $m \in M$, is associated with unique $(m_1, m_2, \dots, m_k)$.

For each index j, consider $\lambda_j: M_j \to M$ which takes $m \in M_j$ to the $k-$tuple whose $j-th$ coordinate is m, all others 0.

For example, let $k = 5$, $j = 3$

$$M = \oplus \sum_{i=1}^{5} M_i$$

Then $\lambda_3 : M_3 \to M$ is defined as

$$\lambda_3(m) = (0,\ 0,\ m,\ 0,\ 0)\ \forall\ m \in M_3$$

Now, we define a projection map. Define a map $\pi_j : M \to M_j$ as follows,

For all

$$m \in M = \oplus \sum_{i=1}^{k} M_i\ ,$$

Then for $m = (m_1, m_2, \ldots, m_k)$

Then $\pi_j(m) = m_j$ that is $j-th$ coordinate of m.

For example,

let $k = 5,\ j = 3$

$$M = \oplus \sum_{i=1}^{5} M_i$$

Then $\pi_3 : M \to M_3$ is defined as

$$\begin{aligned} \pi_3(m) &= \pi_3(m_1, m_2, m_3, m_4, m_5)\ \forall\ m \in M \\ &= m_3 \end{aligned}$$

Remarks 7.1.2: Let $M = \oplus \sum_{i=1}^{k} M_i$ be an $R-$module which is the direct sum of $R-$modules M_i. Then

1. The inclusion map $\lambda_j : M_j \to M$ which takes $m \in M_j$ to the $k-$tuple whose $j-th$ coordinate is m, all others 0 is $R-$homomorphism
2. The projection map $\pi_j : M \to M_j$ which takes each element of M to its $j-th$ coordinate when expressed as a sum of elements of M_i.
3. The sum $\sum_{i=1}^{k} \pi_i = 1$; where 1 is identity map on M.
4. The sum $\sum_{i=1}^{k} \lambda_i \pi_i = 1$; where 1 is identity map on M.
5. For some $\phi \in Hom_R(M,\ M)$, $\phi(\lambda_j) = 0$ implies $\phi = 0$.

The inclusion map $\lambda_j : M_j \to M$ which takes $m \in M_j$ to the $k-$tuple whose $j-th$ coordinate is m, all others 0 is $R-$homomorphism

Let $m_j,\ m_j' \in M_j,\ r \in R$,

Then

$$\begin{aligned} \lambda_j(m_j + m_j') &= (0, 0, \ldots, 0, m_j + m_j', 0, \ldots, 0) \\ &= (0, 0, \ldots, 0, m_j, 0, \ldots, 0) + (0, 0, \ldots, 0, m_j', 0, \ldots, 0) \\ &= \lambda_j(m_j) + \lambda_j(m_j') \end{aligned}$$

Again,

$$\begin{aligned} \lambda_j(r m_j) &= (0, 0, \ldots, 0, r m_j, 0, \ldots, 0) \\ &= r(0, 0, \ldots, 0, m_j, 0, \ldots, 0) \end{aligned}$$

$$= r\lambda_j(m_j)$$

Hence, the inclusion map $\lambda_j : M_j \to M$ is $R-$homomorphism

2. The projection map $\pi_j : M \to M_j$ which takes $m \in M$ to the $j-th$ coordinate of m, when expressed as a sum of elements of M_i is $R-$ homomorphism

Let $m, m' \in M, r \in R$

Let $m = (m_1, m_2, \dots, m_k)$ and $m' = (m'_1, m'_2, \dots, m'_k)$

Then

$$\begin{aligned} \pi_j(m+m') &= \pi_j((m_1, m_2, \dots, m_k) + (m'_1, m'_2, \dots, m'_k)) \\ &= \pi_j(m_1 + m'_1, m_2 + m'_2, \dots, m_k + m'_k) \\ &= m_j + m'_j = \pi_j(m) + \pi_j(m') \end{aligned}$$

Again,

$$\begin{aligned} \pi_j(rm) &= \pi_j(r(m_1, m_2, \dots, m_k)) \\ &= \pi_j(rm_1, rm_2, \dots, rm_k) \\ &= rm_j = r\pi_j(m) \end{aligned}$$

Hence, the projection map is $R-$homomorphism.

3. The sum $\sum_{i=1}^{k} \pi_i = 1$; where 1 is identity map on M.

$\pi_i : M \to M_i \ \forall\ i$ is defined as

$$\pi_i(m) = m_i \ \forall\ m = \sum_{i=1}^{k} m_i \in M,$$

$$\sum_{i=1}^{k} \pi_i(m) = \sum_{i=1}^{k} \pi_i(m_1, m_2, \dots, m_k)$$

$$= \sum_{i=1}^{k} m_i = m$$

Hence, $\sum_{i=1}^{k} \pi_i = 1$

Let $k = 5$

$\pi_i : M \to M_i$ as follows,

For $m = (m_1, m_2, m_3, m_4, m_5)$

$$\pi_i(m) = \sum_{i=1}^{5} m_i$$

That is $\pi_1(m) = m_1,\ \pi_2(m) = m_2, \dots,\ \pi_5(m) = m_5$

Then

$$\sum_{i=1}^{5} \pi_i(m) = \sum_{i=1}^{5} m_i = m$$

4. The sum $\sum_{i=1}^{k} \lambda_i \pi_i = 1$; where 1 is identity map on M.

Consider $m = \sum_{i=1}^{k} m_i \in M$

$$\pi_l(m) = \pi_l\left(\sum_{i=1}^{k} m_i\right) = m_l$$

$$\lambda_l\left(\pi_l\left(\sum_{i=1}^{k} m_i\right)\right) = \lambda_l(m_l)$$

$$= (0,\ 0,\ \ldots,\ 0,\ m_l,\ 0 \ldots,0)$$

So,

$$\sum_{l=1}^{k} \lambda_l \pi_l\,(m) = \sum_{l=1}^{k} t_l$$

where t_l is k −tuple with l −the entry m_l, all others 0.

So that

$$\sum_{l=1}^{k} \lambda_l \pi_l\,(m) = \sum_{l=1}^{k} t_l = m.$$

Hence, $\sum_{l=1}^{k} \lambda_l \pi_l = 1$

5. For some $\phi \in Hom_R(M,\ M)$, $\phi(\lambda_j) = 0$ implies $\phi = 0$.

Let $\phi(\lambda_j) = 0$

This implies $\phi(\lambda_j)(m_j) = 0\ \forall\, m_j \in M_j$

That is $\phi(0,\ 0,\ \ldots,0,\ m_j, 0,\ \ldots,\ 0) = 0\ \forall\, m_j \in M_j$, $1 \le j \le k$ ... (1)

Consider $m = (m_1,\ m_2, \ldots \ldots,\ m_k) \in M$

Then

$$m = (m_1, 0, \ldots,0) + (0,\ m_2, 0, \ldots,0) + \cdots + (0,\ 0, \ldots,\ m_k)$$

Consider

$$\begin{aligned}\phi(m) &= \phi\big((m_1, 0, \ldots,0) + (0,\ m_2, 0, \ldots,0) + \cdots + (0,\ 0, \ldots,\ m_k)\big)\\ &= \phi(m_1, 0, \ldots,0) + \phi(0,\ m_2, 0, \ldots,0) + \ldots + \phi(0,\ 0, \ldots,\ m_k)\\ &= 0 + 0 + \cdots 0 \text{ (from (1))}\\ &= 0\end{aligned}$$

Hence, $\phi(m) = 0\ \forall\, m$, hence $\phi = 0$.

Theorem 7.1.3: Let $M = \oplus \sum_{i=1}^{k} M_i$ be a direct sum of R −modules M_i. Then

$$Hom_R(M,\ M) \cong \begin{bmatrix} Hom_R(M_1,\ M_1) & Hom_R(M_2,\ M_1) & \cdots & Hom_R(M_k,\ M_1)\\ Hom_R(M_1,\ M_2) & Hom_R(M_2,\ M_2) & & Hom_R(M_k,\ M_2)\\ \vdots & & \ddots & \vdots\\ Hom_R(M_1,\ M_k) & Hom_R(M_2,\ M_k) & \cdots & Hom_R(M_k,\ M_k)\end{bmatrix}$$

as rings.

(The right side is a ring T, say, of $k \times k$ matrices $f = [f_{ij}]$ under the usual matrix addition and multiplication, where $f_{ij} \in Hom_R(M_j,\ M_i)$.

Proof:

Let $\phi \in Hom_R(M,\ M)$.

Let $\lambda_j : M_j \to M$ and $\pi_i : M \to M_i$ be the natural inclusion and projection mappings, respectively.

Then $\pi_i \phi \lambda_j \in Hom_R(M_j,\ M_i)$.

Define a mapping $\sigma : Hom_R(M, M) \to T$ by setting $\sigma(\phi)$ to be the square matrix of order k, whose ij − th entry is $\pi_i \phi \lambda_j$, where $\phi \in Hom_R(M,M)$.

We proceed to show that σ is an isomorphism.

So let $\phi,\ \Psi \in \mathrm{Hom}_R(M, M)$.

Then

$$\sigma(\phi+\psi) = [\pi_i(\phi+\psi)\lambda_j] = [\pi_i\phi\lambda_j] + [\pi_i\psi\lambda_j] = \sigma(\phi)+\sigma(\psi)$$

Further,

$$\sigma(\phi)\sigma(\psi) = [\pi_i\phi\lambda_l][\pi_l\psi\lambda_j] = \left[\sum_{l=1}^{K} \pi_i\phi\lambda_l\pi_l\psi\lambda_j\right] = \left[\pi_i\phi\left(\sum_{l=1}^{K}\lambda_l\pi_l\right)\psi\lambda_j\right]$$

Since $\sum_{l=1}^{k} \lambda_l\pi_l = 1,$ it follows that

$$\sigma(\phi)\sigma(\psi) = [\pi_i\phi\psi\lambda_j] = \sigma(\phi\psi)$$

Therefore, σ is a homomorphism.

Now, we prove that σ is 1-1. Let $\phi \in Ker\ \sigma$.

That is,

$$\sigma(\phi) = 0$$

But,

$$\sigma(\phi) = [\pi_i\phi\lambda_j]$$

Therefore,

$$\pi_i\phi\lambda_j = 0\ \forall\ i,\ j$$

This implies

$$\sum_{i=1}^{k} \pi_i\phi\lambda_j = 0$$

But since

$$\sum_{i=1}^{k} \pi_i = 1$$

Therefore, we get,

$$\phi\lambda_j = 0\ \forall\ j$$

Similarly, we can show that $\phi = 0$

Hence σ is 1-1.

σ is onto

Let $f = [f_{ij}] \in T$,

Then $f_{ij}: M_j \to M_i$ is an R –homomorphism.

Set $\phi = \sum_{i,j} \lambda_i f_{ij}\pi_j$

Then $\phi \in Hom_R(M,\ M)$

By definition of σ, $\sigma(\phi)$ is the $k \times k$ matrix whose $(s,\ t)$ entry is $\pi_s\left(\sum_{i,j}\lambda_i f_{ij}\pi_j\right)\lambda_t = f_{st}$, Because $\pi_p\lambda_q = \delta_{pq}$. Hence, $\sigma(\phi) = [f_{st}] = f$.

Thus σ is onto.

Hence, we get that σ is the desired isomorphism.

Task:

1. Let $M = M_1 \oplus M_2$ be the direct sum of simple modules M_1 and M_2 such that M_1 is not isomorphic to M_2. Show that the ring $End_R(M)$ is a direct sum of division rings.
2. Let $M = M_1 \oplus M_2$ be the direct sum of isomorphic simple modules M_1 and M_2. Show that $End_R(M) \cong D_2$, the 2×2 matrix ring over a division ring.

Definition 7.1.4: An $R-$module M is called Noetherian if for every ascending sequence of $R-$submodules of M,

$$M_1 \subset M_2 \subset M_3 \ldots.$$

there exists a positive integer k such that

$$M_k = M_{k+1} = M_{k+2} = \cdots$$

If M is Noetherian, then we also say that the ascending chain condition for submodules holds in M, or M has acc.

Definition 7.1.5: An $R-$module M is called Artinian if for every descending sequence of $R-$submodules of M,

$$M_1 \supset M_2 \supset M_3 \supset \cdots$$

there exists a positive integer k such that

$$M_k = M_{k+1} = M_{k+2} = \cdots$$

If M is Artinian, then we also say that the descending chain condition for submodules holds in M, or M has DCC.

Example 7.1.6:

The ring of integers is Noetherian but not Artinian

Consider Z, the ring of integers. Because the ring of integers Z is a principal ideal ring, any ascending chain of ideals of Z is of the form

$$< n > \ \subset \ < n_1 > \ \subset \ < n_2 > \subset \cdots \ldots (1)$$

where $n, n_1, n_2, \ldots \in Z$.

Because $< n_i > \ \subset \ < n_{i+1} >$ implies n_{i+1} divides n_i.

The ascending chain (1) of ideals in Z starting with n can have at most n distinct terms. This shows that Z as a $Z-$module is Noetherian.

But Z as a $Z-$ module has an infinite properly descending chain

$$< 2 > \ \supset \ < 4 > \cdots$$

showing that Z is not Artinian as a $Z-$module.

Before we give more examples, we prove two theorems providing us with criteria for a module to be Noetherian or Artinian.

Theorem 7.1.7: For an $R-$module M, the following are equivalent:

i. M is Noetherian.

ii. Every submodule of M is finitely generated.

iii. Every non-empty set S of submodules of M has a maximal element (that is, there exists a submodule M_0 in S such that for any submodule N_0 in S with $N_0 \supset M_0$, we have $N_0 = M_0$).

Proof:

i implies ii

Let M is Noetherian R −module. Let N be a submodule of M.

Assume that N is not finitely generated.

First, observe that N is infinite.

For any positive integer k,

let $a_1, \ldots, a_k \in N$.

Then $N \neq \ < a_1, a_2, \ldots, a_k >$.

Choose $a_{k+1} \in N$ such that $a_{k+1} \notin \ < a_1, a_2, \ldots, a_k >$. We then obtain an infinite properly ascending chain

$$< a_1 > \sqsubset \ < a_1, a_2 > \sqsubset \ < a_1, a_2, a_3 > \sqsubset \cdots$$

Since M is Noetherian, therefore, every ascending chain of submodules must be finite.

So, we arrive at a contradiction.

Hence, N is finitely generated.

Therefore, every submodule of a Noetherian module is finitely generated.

i implies iii

Let $S = \{M_\alpha | \alpha \in \wedge\}$ is a family of R −submodules of R −module M.

If possible, let S does not contain a maximal element.

Consider $M_{\alpha_1} \in S$.

Since M_{α_1} is not a maximal element, therefore, there exists $M_{\alpha_2} \in S$ such that $M_{\alpha_1} \subset M_{\alpha_2}$

Again, M_{α_2} is not a maximal element, therefore, there exists $M_{\alpha_3} \in S$ such that $M_{\alpha_2} \subset M_{\alpha_3}$

Continuing so on, we get an ascending chain of R −submodules,

$$M_{\alpha_1} \subset M_{\alpha_2} \subset M_{\alpha_3} \subset \cdots$$

Since S does not contain a maximal element, therefore, this chain is infinite

which contradicts the fact that M is Noetherian.

Hence, our supposition was wrong.

That is, every family of R −submodules of R −module M has a maximal element.

ii implies i

From ii, we have, every submodule of M is finitely generated.

In particular, M is finitely generated.

Let $M = \ < S >$ where $S = \{x_1, x_2, \ldots, x_n\}$

Then for any ascending chain of R −submodules,

$$M_1 \subset M_2 \subset M_3 \subset \cdots$$

Since each M_i is generated by a subset of finite set S.

Therefore, it is a finite chain. It cannot have more than n submodules.

Hence, M is Noetherian.

iii implies i

Let us consider an ascending chain of R − submodules,

$$M_1 \subset M_2 \subset M_3 \subset \cdots$$

Consider the family $S = \{M_i\}$ of R −submodules of M

By iii, S has a maximal element.

Let M_k is the maximal element of S.

Let $t \in N, t > k$

Since the chain of submodules is ascending, therefore,

$$M_k \subset M_t \dots (1)$$

Also, M_k is a maximal element of S, implies that

$$M_t \subset M_k \dots (2)$$

From (1) and (2), we get that

$$M_t = M_k \; \forall \; t > k$$

Therefore, every ascending chain of submodules is finite.

Hence, M is Noetherian.

Theorem 7.1.8: Similar result for Artinian modules is given by

For an R −module M, the following are equivalent:

i. M is Artinian.

ii. Every non-empty set S of submodules of M has a minimal element (that is, there exists a submodule M_0 in S such that for any submodule N_0 in S with $N_0 \subset M_0$, we have $N_0 = M_0$).

Theorem 7.1.9: Let R be a ring. Then the following are equivalent

i. R is Noetherian.

ii. Let A be any left ideal of R. Then A is finitely generated.

iii. Every nonempty set S of left ideals of R has a maximal element.

In particular, every principal left ideal ring is a Noetherian ring.

Theorem 7.1.10: Let R be a ring. Then the following are equivalent

i. R is Artinian.

ii. Every nonempty set S of left ideals of R has a minimal element.

Theorem 7.1.11: Let R be a ring. Then the following are equivalent

i. R is Artinian.

ii. Every nonempty set S of left ideals of R has a minimal element.

Examples 7.1.12:

Example of a module which is Noetherian as well as Artinian

Consider a field F. Regard F as an F −module.

Then we know that F is a simple F −module. Hence, it has only two submodules $\{0\}$ and F.

So, only ascending chain of submodules that is,

$$\{0\} \subset F$$

is finite, which implies that F is Noetherian$F$ −module.

Again, the only descending chain of submodules that is,

$$F \supset \{0\}$$

is finite, which implies that F is Artinian$F$ −module.

Remark 7.1.13: As rings also, every field or division ring is Noetherian as well as Artinian ring.

Example 7.1.14:

Let V be an n −dimensional vector space over a field F. Then V is both Noetherian and Artinian.

For, if W is a proper subspace of V, then $\dim W < \dim V = n$.

Consider $W_1, W_2, \dots, W_{n+2}$ be $n + 2$ subspaces of V such that

$$W_1 \subset W_2 \subset \cdots \subset W_{n+1} \subset W_{n+2} \ldots (1)$$

This implies,

$$\dim W_1 < \dim W_2 < \cdots < \dim W_{n+1} < \dim W_{n+2}$$

Since $0 \leq \dim W_i \leq \dim V = n$

So, (1) cannot have $n+2$

There can exist at the most $n+1$ in an ascending chain of subspaces.

Hence, every ascending chain of subspaces is finite which proves that V is Noetherian.

Consider descending chain of subspaces

$$W_1 \supset W_2 \supset W_3 \supset \cdots \supset W_{n+1} \supset W_{n+2} \ldots (2)$$

Then

$$W_{n+2} \subset W_{n+1} \subset W_n \subset \cdots \subset W_2 \subset W_1$$

is ascending chain of subspaces.

As discussed earlier, it can have at the most $n+1$ terms and hence (2) contain at the most $n+1$ subspaces.

Thus, any properly descending chain of subspaces cannot have more than $n+1$ terms hence V is Artinian.

Example 7.1.15:

Example of a module that is Noetherian but not Artinian.

Consider the ring of integers Z as Z −module.

Then we have already proved that

Z is Noetherian but not Artinian.

Example 7.1.16:

Example of a module that is Artinian but not Noetherian

Let p be a prime number, and let

$$R = Z(p^\infty) = \left\{\frac{m}{p^n} \in \mathbb{Q} \middle| 0 \leq \frac{m}{p^n} < 1\right\}$$

be the ring where addition is modulo positive integers, and multiplication is trivial; that is, $ab = 0$ for all $a, b \in R$. Then R is Artinian but not Noetherian.

Proof:

Claim: Each ideal in R is of the form

$$A_k = \left\{\frac{1}{p^k}, \frac{2}{p^k}, \ldots, \frac{p^k - 1}{p^k}, 0\right\}$$

where k is a positive integer.

Let $A \neq \{0\}$ be any ideal of R, and

let k be the smallest positive integer such that for some positive integer m, $m/p^k \notin$ A.

Consider $\frac{n}{p^i}$ with $i \geq k$ and GCD $(n, p) = 1$.

We assert that $n/p^i \notin$ A.

Now if $\frac{n}{p^i} \in A$

Then

$\frac{n}{p^i} \cdot p^{i-k} = \frac{np^{i-k}}{p^i} = \frac{n}{p^k} \in A.$

Also, by choice of $k, \frac{1}{p^{k-1}} \in A$.

Because GCD $(n, p) = 1$, we can find integers a and b such that $an + bp = 1$.

Then from $\frac{n}{p^k}, \frac{1}{p^{k-1}} \in A$, we have that na/p^k (reduced modulo whole numbers) and bp/p^k (reduced modulo whole numbers) lie in A.

Hence, $\frac{na+bp}{p^k} = \frac{1}{p^k} \in A$, we arrive at a contradiction.

Thus, no $\frac{n}{p^i}$, $i \geq k$, $GCD\,(n, p) = 1$ can lie in A.

Hence, $A = \left\{\frac{1}{p^{k-1}}, \frac{2}{p^{k-1}}, \dots, \frac{p^{k-1}-1}{p^{k-1}}, 0\right\}$.

We denote it as A_{k-1} so that

$$A_k = \left\{\frac{1}{p^k}, \frac{2}{p^k}, \dots, \frac{p^k - 1}{p^k}, 0\right\}$$

Because each ideal contains a finite number of elements, each descending chain of ideals must be finite.

Hence, R is Artinian.

Consider $A_k = \left\{\frac{1}{p^k}, \frac{2}{p^k}, \dots, \frac{p^k-1}{p^k}, 0\right\}$

For $\frac{a}{p^k} \in A_k, \frac{a}{p^k} = \frac{ap}{p^{k+1}} \in A_{k+1}$(reduced modulo whole numbers)

Hence, $A_k \subset A_{k+1}\ \forall\ k$

The chain $A_1 \subset A_2 \subset A_3 \subset \cdots$is an infinite properly ascending chain of left ideals, showing that R is not Noetherian.

Note that although each ideal A of R is finite and, hence, finitely generated, R itself is not finitely generated.

Example 7.1.17:

Example of a module that is neither Artinian nor Noetherian.

Let R be the ring of real-valued functions defined on the set of real numbers ($\mathbb{R}$) under the compositions of addition and multiplication defined as

$$(f + g)(x) = f(x) + g(x)$$

and

$$(fg)(x) = f(x)g(x)\ \forall\ x \in \mathbb{R}$$

Let $I_n = \{f \in R | f(x) = 0\ \forall\ x \in (-n, n)\}; n \in \mathbb{N}$.

First, we prove that $\forall\ n \in \mathbb{N}$, $I_n$is an ideal of R.

Let $f, g \in I_n, h \in R$,

Then$\forall\ x \in (-n, n), f(x) = g(x) = 0$

$$(f - g)(x) = f(x) - g(x) = 0 - 0 = 0$$

Again

$$fh(x) = f(x)h(x) = 0h(x) = 0$$

$$hf(x) = h(x)f(x) = h(x)0 = 0$$

Hence, $f - g, fh, hf \in I_n\ \forall\ f, g \in I_n$ and $h \in R$

This proves that I_n is an ideal of R.

Now, we assert that $I_{n+1} \subset I_n$

Let $f \in I_{n+1}$

Then $f(x) = 0\ \forall\ x \in (-(n+1), n+1)$

Let $x \in (-n, n) \subset (-(n+1), n+1)$

$$f(x) = 0 \ \forall \ x \in (-n, n)$$

Hence, $f \in I_n$

That is, $I_1 \supset I_2 \supset I_3 \supset \cdots$ is an infinite descending chain of idealsso, R is not Artinian.

Let $I_n = \{f \in R | f(x) = 0 \ \forall \ x > n\}; n \in \mathbb{N}$.

First, we prove that $\forall \ n \in \mathbb{N}$, I_n is an ideal of R.

Let $f, g \in I_n$, $h \in R$,

Then $\forall \ x > n$, $f(x) = g(x) = 0$

$$(f - g)(x) = f(x) - g(x) = 0 - 0 = 0$$

Again

$$fh(x) = f(x)h(x) = 0h(x) = 0$$

$$hf(x) = h(x)f(x) = h(x)0 = 0$$

Hence, $f - g$, fh, $hf \in I_n \ \forall \ f, g \in I_n$ and $h \in R$

This proves that I_n is an ideal of R.

Now, we assert that $I_n \subset I_{n+1}$

Let $f \in I_n$

Then $f(x) = 0 \ \forall \ x > n$

Let $x > n + 1 > n$

$$f(x) = 0 \ \forall \ x > n + 1$$

Hence, $f \in I_{n+1}$

That is, $I_1 \subset I_2 \subset I_3 \subset \cdots$ is an infinite ascending chain of idealsso, R is not Noetherian.

Theorem: Every submodule of a Noetherian module is Noetherian.

Let M be a Noetherian $R-$module and N be an $R-$submodule of M.

Since M is a Noetherian $R-$module.

We know that an $R-$ submodule is Noetherian if and only if all its submodules are finitely generated.

This implies all the submodules of M are finitely generated.

Let P be a submodule of $R-$module N. Then P is also a submodule of $R-$module M, hence it is finitely generated.

So, all the submodules of N are finitely generated.

Hence, N is Noetherian $R-$module.

This proves that every submodule of a Noetherian module is Noetherian.

Theorem 7.1.18: Every submodule of an Artinian module is Artinian.

Let M be an Artinian $R-$module and N be an $R-$submodule of M.

We know that an $R-$module M is Artinian if and only if every non-empty set S of submodules of M has a minimal element.

Let T be any non-empty set of submodules of N. Since every submodule of N is a submodule of M.

So, T is a non-empty set of submodules of M. M is Artinian implies, T has a minimal element.

Therefore, N is Artinian.

Theorem 7.1.19: Homomorphic image of a Noetherian module is Noetherian.

Proof: Let M be a Noetherian R −module and M' be the homomorphic image of M. Then by the fundamental theorem of R −isomorphism there exists a function $f: M \to M'$ and $M' \cong \frac{M}{N'}$, where $N = Ker\ f$

Claim: M/N is Noetherian R −module.

Consider an ascending chain of submodules of M/N

$$\frac{M_1}{N} \subset \frac{M_2}{N} \subset \frac{M_3}{N} \subset \cdots (1)$$

The submodules of the quotient module M/N are of the form U/N, where U is a submodule of M containing N.

Also, let $m \in M_i$

Then $m + N \in \frac{M_i}{N} \subset \frac{M_{i+1}}{N}$

This implies, $m \in M_{i+1}$

This proves that $M_1 \subset M_2 \subset M_3$ .... is an ascending chain of submodules of M

Since M is Noetherian, therefore, there exists some natural number k, such that $M_k = M_t\ \forall\ t \geq k$

Hence,

$$\frac{M_k}{N} = \frac{M_t}{N} \forall\ t \geq k$$

This proves that (1) is finite. So, M/N is Noetherian and hence M' is Noetherian.

Theorem 7.1.20: Homomorphic image of an Artinian module is Artinian.

Let M be an Artinian R −module and M' be the homomorphic image of M.

Then by the fundamental theorem of R −isomorphism there exists a function $f: M \to M'$ and $M' \cong \frac{M}{N'}$, where $N = Ker\ f$

Claim: M/N is an Artinian R −module.

Consider a descending chain of submodules of M/N

$$\frac{M_1}{N} \supset \frac{M_2}{N} \supset \frac{M_3}{N} \supset \cdots (1)$$

The submodules of the quotient module M/N are of the form U/N, where U is a submodule of M containing N.

Also, let $m \in M_i$

Then $m + N \in \frac{M_i}{N} \subset \frac{M_{i-1}}{N}$

This implies, $m \in M_{i-1}$

This proves that $M_1 \supset M_2 \supset M_3$ .... is a descending chain of submodules of M

Since M is Artinian, therefore, there exists some natural number k, such that $M_k = M_t\ \forall\ t \geq k$

Hence,

$$\frac{M_k}{N} = \frac{M_t}{N} \forall\ t \geq k$$

This proves that (1) is finite. So, M/N is Artinian and hence M' is Artinian.

Remark 7.1.21: If all the submodules of a module are Noetherian, the module need not be Noetherian.

Example 7.1.22:

Let p be a prime number, and let

$$R = Z(p^\infty) = \left\{\frac{m}{p^n} \in \mathbb{Q} | 0 \leq \frac{m}{p^n} < 1\right\}$$

be the ring where addition is modulo positive integers, and multiplication is trivial; that is, $ab = 0$ for all $a, b \in R$.

We have proved that each proper ideal of R is of the form

$$A = \left\{\frac{1}{p^{k-1}}, \frac{2}{p^{k-1}}, \ldots, \frac{p^{k-1}-1}{p^{k-1}}, 0\right\}$$

and hence finite.

So, every proper ideal of R is finitely generated

Hence, every proper ideal of R is Noetherian but we know that R is not Noetherian.

Theorem 7.1.23: Let M be an R −module and let N be an R −submodule of M. Then M is Noetherian if and only if both N and M/N are Noetherian.

Proof:

Let M be a Noetherian R −module and let N be an R −submodule of M. Then we know that every submodule and homomorphic image of M is Noetherian.

Hence, N and M/N are Noetherian.

Conversely,

Let N and M/N be Noetherian and let K be any submodule of M.

Then $\frac{K+N}{N}$ is a submodule of $\frac{M}{N}$, and, hence,

it is finitely generated.

But then $\frac{K+N}{N} \cong \frac{K}{N \cap K}$ implies $\frac{K}{N \cap K}$ is finitely generated, say

$$\frac{K}{N \cap K} = < x_1 + (N \cap K), x_2 + (N \cap K), \ldots, x_m + (N \cap K) >$$

Consider $x \in K$, then $x + (N \cap K) \in \frac{K}{N \cap K}$

Since

$$\frac{K}{N \cap K} = < x_1 + (N \cap K), x_2 + (N \cap K), \ldots, x_m + (N \cap K) >$$

So, there exist $\alpha_1, \alpha_2, \ldots, \alpha_n \in R$ such that

$$x + (N \cap K) = \sum_{i=1}^{m} \alpha_i \left(x_i + (N \cap K)\right)$$

$$= \sum_{i=1}^{m} \alpha_i x_i + (N \cap K)$$

$$x + (N \cap K) = \sum_{i=1}^{m} \alpha_i x_i + (N \cap K)$$

$$x - \sum_{i=1}^{m} \alpha_i x_i \in N \cap K$$

or,

$$x = \sum_{i=1}^{m} \alpha_i x_i + y; \; y \in N \cap K$$

which implies that

$$K = < x_1, x_2, \ldots, x_n > + N \cap K$$

Further, because N is Noetherian, its submodule $N \cap K$ is finitely generated, say by $y_1, y_2, \ldots, y_n$.

This implies for $y \in N \cap K$, there exist $\beta_1, \beta_2, \ldots, \beta_n$ such that

$$y = \sum_{i=1}^{n} \beta_i y_i$$

so that

$$x = \sum_{i=1}^{m} \alpha_i x_i + \sum_{i=1}^{n} \beta_i y_i$$

This implies, $K = < x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_n >$ is finitely generated.

Hence, every submodule of M is finitely generated which proves that M is Northerian.

Theorem 7.1.24: Let M be an R −module and let N be an R −submodule of M. Then M is Artinian if and only if both N and M/N are Artinian.

Proof:

Let M be an Artinian R −module and let N be an R −submodule of M. Then we know that every submodule and homomorphic image of M is Artinian.

Hence, N and M/N are Artinian.

Conversely,

Let N and M/N be Artinian and let K be any submodule of M.

Consider any descending chain of submodules

$M_1 \supset M_2 \supset M_3 \ldots$ (1) of R −module M.

Then

$M_1 \cap N \supset M_2 \cap N \supset M_3 \cap N \ldots$ (2) is descending chain of submodules of Artinian module N.

Therefore, chain (2) is stationary

There exists positive integer m such that $\forall\, n \geq m$

$$M_m \cap N = M_n \cap N$$

Consider the descending chain of submodules of Artinian module M/N

$$\frac{M_1 + N}{N} \supset \frac{M_2 + N}{N} \supset \frac{M_3 + N}{N} \ldots (3)$$

Then since M/N is Artinian, there exists positive integer l such that $\forall\, k \geq l$

$$\frac{M_k + N}{N} = \frac{M_l + N}{N}$$

Let $r = \max(m, l)$

Then $\forall\, i \geq r$

$$M_r \cap N = M_i \cap N$$

and

$$\frac{M_r + N}{N} = \frac{M_i + N}{N}$$

This implies,

$$M_r + N = M_i + N$$

Claim: $\forall\, i \geq r,\ M_i = M_r$

$$\begin{aligned} M_r &= M_r \cap (M_r + N) \\ &= M_r \cap (M_i + N) \\ &= M_i + (M_r \cap N) \end{aligned}$$

This is due to modular law if A, B, and C are three R −submodules of an R − module M, such that $B \subset A$ then $A \cap (B + C) = B + (A \cap C)$

So,

$$\frac{\quad}{M_r} = \frac{\quad}{M_i} + \left(\frac{\quad}{M_r} \cap \frac{\quad}{N}\right)$$

$$= \frac{M_i}{M_i} + \left(\frac{M_r}{M_i} \cap \frac{N}{N}\right)$$

$$= N_i$$

which proves that chain (1) of $R-$ submodules of M is finite.

Since (1) is an arbitrary descending chain of $R-$ submodules of M, hence M satisfies DCC. So, M is Artinian.

Theorem 7.1.25: Let R_i, $1 \leq i \leq n$, be a family of Noetherian (Artinian) rings each with a unity element. Then their direct sum $R = \oplus \sum_{i=1} R_i$ is again Noetherian (Artinian).

Proof:

We know that each left ideal A of R is of the form

$$A_1 \oplus A_2 \oplus A_3 \oplus .. \oplus A_n,$$

where A_i are left ideals in R.

So, if a left ideal

$$B = B_1 \oplus B_2 \oplus B_3 \oplus ... \oplus B_n$$

of R is such that $A \subset B$, then it is clear that $A_i \subset B_i, \forall\, 1 \leq i \leq n$.

Hence, any properly ascending (descending) chain of left ideals in R must be finite because each R_i is Noetherian (Artinian).

Theorem 7.1.26: A subring of a Noetherian (Artinian) ring need not be Noetherian (Artinian)

Proof:

For the Noetherian case, the ring R of 2×2 matrices over the rational numbers Q is a Noetherian ring.

Claim: $\begin{bmatrix} Z & Q \\ 0 & Q \end{bmatrix}$ is a subring of R which is not left Noetherian.

First, we prove that

$$R_1 = \begin{bmatrix} Z & Q \\ 0 & Q \end{bmatrix} = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \middle| a \in Z,\ b, c \in Q \right\}$$

is a subring of R.

Clearly, $\begin{bmatrix} Z & Q \\ 0 & Q \end{bmatrix} \subset R$

Consider $\begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}, \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} \in \begin{bmatrix} Z & Q \\ 0 & Q \end{bmatrix}$

Then $a_1,\ a_2 \in Z$ implies $a_1 - a_2,\ a_1 a_2 \in Z$

Again $b_1,\ b_2,\ c_1,\ c_2 \in Q$ implies $b_1 - b_2,\ c_1 - c_2,\ a_1 b_2 + b_1 c_2,\ c_1 c_2 \in Q$

This implies

$$\begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} - \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} = \begin{bmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & c_1 - c_2 \end{bmatrix} \in R_1$$

and

$$\begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} = \begin{bmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{bmatrix} \in R_1$$

Hence, R_1 is a subring of R.

Consider for fixed k,

$$A_k = \left\{ \begin{bmatrix} 0 & \frac{m}{2^k} \\ 0 & 0 \end{bmatrix} \middle| m \in Z \right\}$$

is a left ideal of R_1.

For $\begin{bmatrix} 0 & \frac{m}{2^k} \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \frac{n}{2^k} \\ 0 & 0 \end{bmatrix} \in A_k$

$$\begin{bmatrix} 0 & \frac{m}{2^k} \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 0 & \frac{n}{2^k} \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & \frac{m-n}{2^k} \\ 0 & 0 \end{bmatrix} \in A_k$$

Again let $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in R_1, \begin{bmatrix} 0 & \frac{n}{2^k} \\ 0 & 0 \end{bmatrix} \in A_k$

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \begin{bmatrix} 0 & \frac{n}{2^k} \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & \frac{an}{2^k} \\ 0 & 0 \end{bmatrix} \in A_k$$

Hence, A_k is a left ideal of R_1.

Also, $A_1 \subset A_2 \subset \cdots$ is an infinite chain of left ideals of R_1, which proves that R_1 is not left Noetherian.

For Artinian, consider the ring of rational numbers Q, being field Q is Artinian.

But its subring, the ring of integers Z is not Artinian.

As

$$< 2 > \supset < 4 > \supset < 8 > \supset \cdots$$

is an infinite descending chain of ideals in the ring of integers.

Definitions 7.1.27:

- A ring is called a right Noetherian (Artinian) ring if it satisfies acc (DCC) on its right ideals.
- A ring is called a left Noetherian (Artinian) ring if it satisfies acc (DCC) on its left ideals.

Note:

A right (left) Noetherian ring may not be left (right) Noetherian.

Example 7.1.28:

A right Noetherian ring may not be left Noetherian

Consider the ring

$$R = \begin{bmatrix} Z & Q \\ 0 & Q \end{bmatrix} = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \middle| a \in Z,\ b,\ c \in Q \right\}$$

Then as proved, R is not left Noetherian.

Now we prove that R is right Noetherian.

Claim: Any right ideal of R is generated by at the most two elements

Let A be a non-zero right ideal of R. Let

$X = \{n \in Z \mid \begin{bmatrix} n & x \\ 0 & y \end{bmatrix} \in A \text{ for some } x,\ y \in Q\}$

Then it is clear that X is an ideal in Z. Hence,

$X = \ < n_0 >$ for some $n_0 \in Z$, because Z is a principal ideal ring.

Case 1. $X \neq \{0\}$.

We claim $A = \begin{bmatrix} n_0 & 1 \\ 0 & 1 \end{bmatrix} R$ or $A = \begin{bmatrix} n_0 & 1 \\ 0 & 0 \end{bmatrix} R$

That is, A is a principal right ideal of R generated by $\begin{bmatrix} n_0 & 1 \\ 0 & 1 \end{bmatrix}$ or $\begin{bmatrix} n_0 & 1 \\ 0 & 0 \end{bmatrix}$

First, let

$$\begin{bmatrix} n_0 & a \\ 0 & b \end{bmatrix} \in A; b \neq 0$$

Then

$$\begin{bmatrix} n_0 & a \\ 0 & b \end{bmatrix}\begin{bmatrix} k & x \\ 0 & y \end{bmatrix} = \begin{bmatrix} n_0 k & n_0 x + ay \\ 0 & by \end{bmatrix} \in A$$

for all $k \in Z, x, y \in Q$.

Taking $k = 1$, $y = \frac{1}{b}$, $x = \frac{1-\frac{a}{b}}{n_0}$, we see that

$$\begin{bmatrix} n_0 & 1 \\ 0 & 1 \end{bmatrix} \in A$$

Next, let $\begin{bmatrix} n_0 m & c \\ 0 & d \end{bmatrix}$ be an arbitrary element of A. Then

$$\begin{bmatrix} n_0 m & c \\ 0 & d \end{bmatrix} = \begin{bmatrix} n_0 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} m & \frac{c-d}{n_0} \\ 0 & d \end{bmatrix}$$

Hence, $A = \begin{bmatrix} n_0 & 1 \\ 0 & 1 \end{bmatrix} R$

In case, (2, 2) entry of each element of A is 0. The general element of A is

$$\begin{bmatrix} n_0 & c \\ 0 & 0 \end{bmatrix}$$

Then

$$\begin{bmatrix} n_0 & c \\ 0 & 0 \end{bmatrix}\begin{bmatrix} k & x \\ 0 & y \end{bmatrix} = \begin{bmatrix} n_0 k & n_0 x + cy \\ 0 & 0 \end{bmatrix} \in A$$

for all $k \in Z, x, y \in Q$.

Taking $k = 1$, $y = 1$, $x = \frac{1-c}{n_0}$, we see that

$$\begin{bmatrix} n_0 & 1 \\ 0 & 0 \end{bmatrix} \in A$$

Next, let $\begin{bmatrix} n_0 m & c \\ 0 & 0 \end{bmatrix}$ be an arbitrary element of A. Then

$$\begin{bmatrix} n_0 m & c \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} n_0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} m & \frac{c-d}{n_0} \\ 0 & d \end{bmatrix}$$

Hence, $A = \begin{bmatrix} n_0 & 1 \\ 0 & 0 \end{bmatrix} R$

So, in case, (2, 2) entry of each element of A is 0. Then

$$A = \begin{bmatrix} n_0 & 1 \\ 0 & 0 \end{bmatrix} R$$

Case 2. $X = \{0\}$

Subcase 1.

Suppose A is the principal right ideal generated by some non-zero element of the form

$$\begin{bmatrix} 0 & \beta \\ 0 & \gamma \end{bmatrix}, \beta, \gamma \in Q.$$

Then

$$A = \begin{bmatrix} 0 & \beta \\ 0 & \gamma \end{bmatrix} R = \left\{\begin{bmatrix} 0 & \beta y \\ 0 & \gamma y \end{bmatrix} | y \in Q\right\}$$

Subcase 2. Suppose A is not the principal right ideal.

Then A contains at least one element

$$\begin{bmatrix} 0 & \beta \\ 0 & \gamma \end{bmatrix}; \beta, \gamma \neq 0$$

Because if $\beta = 0 \; \forall \begin{bmatrix} 0 & \beta \\ 0 & \gamma \end{bmatrix} \in A$, then $A = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} R$ and if $\gamma = 0 \; \forall \begin{bmatrix} 0 & \beta \\ 0 & 0 \end{bmatrix} \in A$, then $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} R$

which is not possible as A is not principal ideal.

Hence,

$A \supset \begin{bmatrix} 0 & \beta \\ 0 & \gamma \end{bmatrix} R = \left\{ \begin{bmatrix} 0 & \beta y \\ 0 & \gamma y \end{bmatrix} | y \in Q \right\}$ and $A \neq \begin{bmatrix} 0 & \beta \\ 0 & \gamma \end{bmatrix} R$

So, we can choose, $\begin{bmatrix} 0 & \beta' \\ 0 & \gamma' \end{bmatrix} \in A$ such that

$$\begin{bmatrix} 0 & \beta' \\ 0 & \gamma' \end{bmatrix} \notin \begin{bmatrix} 0 & \beta \\ 0 & \gamma \end{bmatrix} R$$

That is,there does not exist $y \in Q$ such that

$$\beta' = \beta y,\ \gamma' = \gamma y$$

or,

$\frac{\beta'}{\beta} \neq \frac{\gamma'}{\gamma}$ that is, $\beta'\gamma - \gamma'\beta \neq 0$.

Hence the system of equations

$$p = \beta x + \beta' y,\ q = \gamma x + \gamma' y$$

has a unique solution $x,\ y \in Q$ for arbitrary $p,\ q \in Q$.

Since $p,\ q \in Q$ are arbitrary, therefore,

the matrix $\begin{bmatrix} 0 & p \\ 0 & q \end{bmatrix}$ is a general matrix in A.

Also,

$$\begin{bmatrix} 0 & p \\ 0 & q \end{bmatrix} = \begin{bmatrix} 0 & \beta \\ 0 & \gamma \end{bmatrix} \begin{bmatrix} 0 & x \\ 0 & x \end{bmatrix} + \begin{bmatrix} 0 & \beta' \\ 0 & \gamma' \end{bmatrix} \begin{bmatrix} 0 & y \\ 0 & y \end{bmatrix} \in A$$

Hence, A is generated by e_{12} and e_{22}.

That is, generated by two elements.

So, the claim is established.

We have proved that each right ideal of R is finitely generated hence, R is right Noetherian.

Example 7.1.29:

A right Artinian ring may not be left,Artinian

Consider the ring

$$R_1 = \begin{bmatrix} Q & R \\ 0 & R \end{bmatrix} = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \middle| a \in Q,\ b,\ c \in R \right\}$$

Note that Q denotes the field of rational numbers and R denotes the field of real numbers,

Since R is infinite-dimensional vector space over Q, therefore, there exist infinitely many $\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots$ which are linearly independent over Q.

Let for each positive integer k,

$$A_k = \left\{ \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} \mid a \in \ < \alpha_k, \alpha_{k+1}, \ldots > \right\}$$

Then A_k is a left ideal of R_1 and $A_k \supset A_{k+1}$.

Also,

$\begin{bmatrix} 0 & \alpha_k \\ 0 & 0 \end{bmatrix} \in A_k$ but $\begin{bmatrix} 0 & \alpha_k \\ 0 & 0 \end{bmatrix} \notin A_{k+1}$

Therefore, $A_k \neq A_{k+1}$

We get an infinite descending chain of left ideals, hence R_1 is not left,Artinian.

Now we prove that R_1 is right Artinian.

Let $I_1 \supset I_2,\ I_1 \neq I_2$ be two right ideals of R_1.

Let $\begin{bmatrix} \alpha & \beta \\ 0 & \gamma \end{bmatrix} \in I_2$ where $\alpha \in Q,\ \beta,\ \gamma \in R$

We have two cases

Case 1. $\alpha \neq 0$

Let α be the least positive integer such that

$$\begin{bmatrix} \alpha & \beta \\ 0 & \gamma \end{bmatrix} \in I_2$$

Therefore,

$$\begin{bmatrix} \alpha & \beta \\ 0 & \gamma \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in I_2$$

$$\begin{bmatrix} 0 & \alpha \\ 0 & 0 \end{bmatrix} \in I_2$$

That is,

$$\begin{bmatrix} 0 & \alpha \\ 0 & 0 \end{bmatrix}\left(\frac{1}{\alpha}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\right) \in I_2$$

So,

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in I_2$$

This implies,

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\beta\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \in I_2$$

$$\begin{bmatrix} 0 & \beta \\ 0 & 0 \end{bmatrix} \in I_2$$

Also,

$$\begin{bmatrix} \alpha & \beta \\ 0 & \gamma \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in I_2$$

$$\begin{bmatrix} \alpha & 0 \\ 0 & 0 \end{bmatrix} \in I_2$$

Hence

$$\begin{bmatrix} \alpha & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \beta \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} \alpha & \beta \\ 0 & \gamma \end{bmatrix} \in I_2$$

So,

$$\begin{bmatrix} 0 & 0 \\ 0 & \gamma \end{bmatrix} \in I_2$$

Also, $\alpha \neq 0, \begin{bmatrix} \alpha & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} \alpha^{-1} & 0 \\ 0 & 0 \end{bmatrix} \in I_2$

That is $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in I_2$

Similarly, if $\gamma \neq 0$, then $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \in I_2$

That is, if $\gamma \neq 0$, then $I_2 = R_1$, which is not possible, as I_2 is properly contained in I_1.

Therefore,

$\gamma = 0$, and I_2 is generated by $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$

Let I_3 be any non-zero right ideal of R_1 such that

$$I_1 \supset I_2 \supset I_3, I_1 \neq I_2 \neq I_3$$

Let $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \in I_3$ be any non-zero element.

If $a \neq 0$

Then

$$\left(\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}\right)\begin{bmatrix} \frac{1}{a} & 0 \\ 0 & 0 \end{bmatrix} \in I_3$$

This implies

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in I_3$$

That is, $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in I_3$

This means, $I_2 = I_3$; which is not true.

So, $a = 0 \Rightarrow b \neq 0$

Hence, $\begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & \frac{1}{b} \end{bmatrix} \in I_3$

This implies

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in I_3$$

So, I_3 is generated by $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$

That is, I_3 is the minimal right ideal of R_1.

So, descending chain of right ideals, in this case, is finite. Hence, R_1 is right Artinian.

Case 2. $\alpha = 0$

Here, $\begin{bmatrix} 0 & \beta \\ 0 & \gamma \end{bmatrix} \in I_2$

Subcase 1.

If all other elements of I_2 can be expressed as

$\lambda \begin{bmatrix} 0 & \beta \\ 0 & \gamma \end{bmatrix}$, for some $\lambda \in R$ then $I_2 = \; < \begin{bmatrix} 0 & \beta \\ 0 & \gamma \end{bmatrix} >$

Hence, I_2 is minimal right ideal and chain

$$I_1 \supset I_2 \supset \{0\}$$

is finite. So, R_1 is right Artinian

Subcase 2.

If there exists some $\begin{bmatrix} 0 & b \\ 0 & c \end{bmatrix} \in I_2$ such that

$$\begin{bmatrix} 0 & b \\ 0 & c \end{bmatrix} \neq \lambda \begin{bmatrix} 0 & \beta \\ 0 & \gamma \end{bmatrix},$$

for any $\lambda \in R$ then $\frac{b}{\beta} \neq \frac{c}{\gamma}$.

Now, $\begin{bmatrix} 0 & b \\ 0 & c \end{bmatrix}, \begin{bmatrix} 0 & \beta \\ 0 & \gamma \end{bmatrix} \in I_2$

Therefore, $c\begin{bmatrix} 0 & \beta \\ 0 & \gamma \end{bmatrix} - \gamma \begin{bmatrix} 0 & b \\ 0 & c \end{bmatrix} \in I_2$

That is,

Therefore, $\begin{bmatrix} 0 & \beta c - \gamma b \\ 0 & 0 \end{bmatrix} \in I_2$

This implies,

$$\begin{bmatrix} 0 & \beta c - \gamma b \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & \frac{1}{\beta c - \gamma b} \end{bmatrix} \in I_2$$

That is, $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in I_2$

This further implies,

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & \beta \end{bmatrix} \in I_2$$

That is,

$$\begin{bmatrix} 0 & \beta \\ 0 & 0 \end{bmatrix} \in I_2$$

So, $\begin{bmatrix} 0 & 0 \\ 0 & \gamma \end{bmatrix} \in I_2$

If $\gamma = 0 \ \forall \beta$, then $I_2 = \ < \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} >$

Hence, I_2 is minimal right ideal and chain

$$I_1 \supset I_2 \supset \{0\}$$

is finite. So, R_1 is right Artinian.

If $\gamma \neq 0$, then $\begin{bmatrix} 0 & 0 \\ 0 & \gamma \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & \frac{1}{\gamma} \end{bmatrix} \in I_2$

So, $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \in I_2$.

Hence, I_2 is generated by $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

Let I_3 be any non-zero right ideal of R_1 such that

$$I_1 \supset I_2 \supset I_3, I_1 \neq I_2 \neq I_3$$

Then I_3 is the minimal right ideal generated by $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$

So, descending chain of right ideals, in this case, is finite. Hence, R_1 is right Artinian.

Definition 7.1.30:

- A right (or left) ideal A in a ring R is called nilpotent if $A^n = \{0\}$ for some positive integer n.
- A right (or left) ideal A in a ring R is called a nil ideal if each element of A is nilpotent.

Note:

Every nilpotent right (or left) ideal is nil. However, the converse is not true.

Theorem 7.1.31: If J is nil left ideal in an Artinian ring R. Then J is nilpotent.

Proof:

Let J is nil left ideal in an Artinian ring R such that J is not nilpotent.

This implies, $J^k \neq \{0\}$ for any positive integer k.

Consider a family $\{J, J^2, J^3, \ldots\}$.

Because R is Artinian, this family has a minimal element, say

$$B = J^m$$

Then

$$B^2 = J^{2m} \subset J^m = B$$

($a.a \in I \ \forall \ a \in I$, where I is an ideal of a ring R).

implies $B^2 = B$ (By minimality of B)

Consider another family

$F = \{A | A$ is a left ideal contained in B with $BA \neq \{0\}\}$.

Then

$$F \neq \phi$$

$$B \cdot B = B^2 = B = J^m \neq \{0\}$$

Also, $B \subseteq B$ is a left ideal.

So, $B \in F$, hence $F \neq \phi$

Since R is Artinian, therefore, F has a minimal element say A.

Then $BA \neq \{0\}$.

This implies there exists an element $a \in A$ such that

$Ba \neq \{0\}$.

But $Ba \subset A$ and $B(Ba) = B^2a = Ba \neq \{0\}$.

Thus, $Ba \in F$.

Hence, by minimality of A, $Ba = A$.

This gives that there exists an element $b \in B$ such that $ba = a$.

This implies $b^i a = a$ for all positive integers i. But because b is a nilpotent element,

So, there exists some positive integer k for which $b^k = 0$.

This implies $b^k a = 0$, hence $a = 0$.

But in that case, $Ba = 0$, so we arrive at a contradiction.

Therefore, for some positive integer k, $J^k = (0)$.

Lemma 7.1.32: Let R be a Noetherian ring. Then the sum of nilpotent ideals in R is a nilpotent ideal.

Proof: Let B be the sum of nilpotent ideals in R.

Because R is Noetherian (i.e., left Noetherian), B is finitely generated as a left ideal.

Suppose $B = < x_1, x_2, \ldots, x_m >$. Then each x_i lies in the sum of finitely many $A_i's$.

Hence, B is contained in the sum of a finite number of $A_i's$, say (after reindexing if necessary) $A_1, A_2, \ldots A_n$.

Thus,

$$B = A_1 + A_2 + \ldots + A_n$$

which being finite sum of nilpotent ideals is nilpotent ideal.

which being finite sum of nilpotent ideals is nilpotent ideal.

Definition 7.1.33: If S is any non-empty subset of a ring R, then$l(S) = \{x \in R | xS = 0\}$ is called the left annihilator of S in R.
$l(S)$ is a left ideal of R.

Theorem 7.1.34: Let R be a Noetherian ring having no non-zero nilpotent ideals. Then R has no non-zero nil ideals.

Proof: Let N be a non-zero nil ideal in R.

Let $F = \{l(n) | n \in N, n \neq 0\}$ be a family of left annihilator ideals.

Because R is Noetherian, F has a maximal member, say $l(n)$

Let $x \in R$. Then $nx \in N$. So, there exists a smallest positive integer k such that $(nx)^k = 0$.

Now, let $y \in l(n)$. Then $yn = 0$

$$y(nx)^{k-1} = y(nx)(nx) \ldots (nx) = yn\,(xnxn \ldots xnx) = 0$$

So,$l(n) \subset l((nx)^{k-1})$

Because $(nx)^{k-1} \neq 0$, $l((nx)^{k-1}) \in F$.

But then by maximality of $l(n)$,

$$l(n) \subset l((nx)^{k-1})$$

Now,

$$(nx)^k = 0$$

implies

$$nx \in l((nx)^{k-1}) = l(n)$$

That is, $nxn = 0 \; \forall x \in R$, $n \in N$

Now

$$(RnR)^2 = RnRRnR = RnRnR = 0$$

Therefore, by hypothesis,

$$RnR = 0$$

If $1 \in R$, then

$$1n1 = n = 0,$$

a contradiction. In this case, we are done.

Otherwise,

Consider the ideal generated by n,

$$< n > = nR + Rn + RnR + nZ$$

Set $A = nR + Rn$

Because $nxn = 0 \; \forall x \in R$

$$A^{2^2} = (nR + Rn)^2$$

$$= nRnR + RnRn + nRRn + RnnR$$

$$= n \cdot 0 + 0 \cdot nR + RnRn + nRRn$$

$$n + nRn + Rn^2R$$

$$= 0$$

By hypothesis, $A = \{0\}$

$$< n > = nR + Rn + RnR + nZ$$

$$= nR + Rn + RnR + nZ$$

$$A + RnR + nZ$$

$$= A + RnR + nZ$$

$$A + nZ$$

If $n^k = 0$,

Then we have

$$(A + nZ)^k = \{0\}$$

Therefore, by hypothesis,

$$A + nZ = \{0\}$$

Since $A = \{0\}$, we get, nZ and hence $n = 0$

Again, we arrive at a contradiction.

Hence, R has no non-zero nil ideals.

Remark 7.1.35: Indeed, one can similarly show that R has no nonzero right or left nil ideals.

Next, we show that a nil ideal in a Noetherian ring is nilpotent.

Theorem 7.1.36: Let N be a nil ideal in a Noetherian ring R. Then N is nilpotent.

Proof: Let T be the sum of nilpotent ideals in R.

Then R/T has no non-zero nilpotent ideals,

for if A/T is nilpotent, then $\left(\frac{A}{T}\right)^m = \{0\}$ implies $\frac{A^m}{T} = \{0\}$ so, $A^m \subset T$.

But since T is nilpotent, there exists a positive integer k such that

$$(A^m)^k = \{0\}$$

Hence, A itself is nilpotent, so $A \subset T$.

This implies $\frac{A}{T} = \{0\}$

Consider the nil ideal $\frac{N+T}{T}$ in $\frac{R}{T}$

Since R/T has no non-zero nilpotent ideal, so R/T has no non-zero nil ideal.

This implies,

$$\frac{N+T}{T} = \{0\}$$

This implies, $N \subset T$, which is a nilpotent ideal. Hence, N is nilpotent.

Theorem 7.1.37: A right Artinian ring having more than one element and having no proper zero divisors is a division ring.

Proof:

Let R be the Artinian ring without zero divisors, which has at least two elements.

Then there exists at least one element $a(\neq 0) \in R$.

Now, R is Artinian, so the descending chain of right ideals of R,

$< a > \supset < a^2 > \supset < a^3 > \supset \cdots$ is finite.

That is, there exists $l \in N$ such that $\forall\ k \geq l$,

$$< a^k > = < a^l >$$

In particular,

$$< a^l > = < a^{l+1} >$$

This implies,

$$a^l \in < a^{l+1} >$$

That is,

$$a^l = a^{l+1}r + na^{l+1},\ r \in R,\ n \in Z$$

This implies,

$$a^l = a^l(ar + na)$$

As R is without zero divisors, canceling a^{l-1} on both sides,

$$a = a(ar + na)$$

$$a = ae; e = ar + na \in R$$

This implies,

$$ae = ae^2\ ,$$

that is,

$$e = e^2$$

So, $\forall\ x \in R,\ xe = xe^2$

$$(xe - x)e = 0$$

$$\Rightarrow xe - x = 0$$

$$\Rightarrow xe = x\ \forall\ x \in R$$

Also, $e^2x = ex\ \forall\ x \in R$ gives, $ex = x$

So, e is the unity of R.

Therefore,

$$< a^l > = a^lR$$

and

$$< a^{l+1} > = a^{l+1}R$$

Now,

$$a^le \in a^lR = < a^l > = < a^{l+1} > = a^{l+1}R$$

This implies,

$$a^l e = a^{l+1} s; s \in R$$

That gives,

$$e = as$$

Thus, every non-zero element of R is a unit, hence R is a division ring.

Remarks 7.1.38:

- An Artinian integral domain with at least two elements is a field.
- If R is a commutative Artinian ring with unity, then every prime ideal of R is a maximal ideal.

Proof: Let R be a commutative Artinian ring and P be a prime ideal of R.

Then R/P is also commutative and Artinian ring.

Also, $1 \in R$ implies $1 + P \in \frac{R}{P}$

$P \in \frac{R}{P}$ and $1 + P \in \frac{R}{P}$

If $P = 1 + P$ then $1 \in P$

But in this case, $P = R$

So, $1 + P \neq P$

Therefore, $\frac{R}{P}$ is commutative, with unity, Artinian ring having at least 2 elements $1 + P$ and P.

Hence, $\frac{R}{P}$ is a field that implies, P is the maximal ideal of R.

7.2 Hilbert Basis Theorem

Theorem 7.2.1: Hilbert Basis Theorem: Let R be a Noetherian ring. Then the polynomial ring $R[x]$ is also a Noetherian ring.

Proof: Let F and F' be the families of left ideals of R and $R[x]$, respectively. Let n be a nonnegative integer. Define a mapping $\phi_n: F' \to F$ where$\phi_n(I) = \{a \in R | \exists ax^n + bx^{n-1} + \cdots \in I, a \neq 0\} \cup \{0\}$

Claim 1:$\phi_n(I) \in F$

We need to prove that $\phi_n(I)$ is a left ideal of R.

Let $a_0, a_1 \in \phi_n(I), r \in R$

Then there exist polynomials

$$a_0x^n + b_0x^{n-1} + \cdots \in I$$
$$a_1x^n + b_1x^{n-1} + \cdots \in I$$

Since I is a left ideal of $R[x]$

Therefore,

$$(a_0x^n + b_0x^{n-1} + \cdots) - (a_1x^n + b_1x^{n-1} + \cdots) \in I$$

and

$$r(a_0x^n + b_0x^{n-1} + \cdots) \in I$$

That is,

$$(a_0 - a_1)x^n + (b_0 - b_1)x^{n-1} + \cdots \in I$$

and

$$ra_0x^n + rb_0x^{n-1} + \cdots \in I$$

which implies,

$$a_0 - a_1, ra_0 \in \phi_n(I) \forall a_0, a_1 \in \phi_n(I), r \in R$$

which proves that

$\phi_n(I)$ is a left ideal of R, and hence, $\phi_n(I) \in F$

Claim 2: If $I, J \in F'$ with $I \subset J$ and $\phi_n(I) = \phi_n(J)\ \forall\ n \geq 0$, then $I = J$

Let $0 \neq f(x) \in J$ of degree m.

Because $\phi_m(I) = \phi_m(J)$,

there exists $g_m(x) \in I$ with leading coefficient the same as that of $f(x)$, and $f(x) - g_m(x)$ is either 0 or of degree at most $m - 1$.

Suppose $f(x) - g_m(x) \neq 0$.

Because $f(x) - g_m(x) \subset J$, we can similarly find

$$g_{m-1}(x) \in I$$

such that $f(x) - g_m(x) - g_{m-1}(x) \in J$ and degree is either 0 or of degree at most $m - 2$. Continuing like this, we arrive, after at most m steps, at

$$f(x) - g_m(x) - g_{m-1}(x) - \cdots - g_1(x) = 0$$

Now, $g_i(x) \in I\ \forall\ i$

This implies, $g_m(x) + g_{m-1}(x) + \cdots + g_1(x) \in I$

That is $f(x) \in I$

This implies, $I = J$.

Let $A_1 \subset A_2 \subset A_3 \subset \cdots$ be an ascending sequence of left ideals of $R[x]$.

Then for each non-negative integer n,

$$\phi_n(A_1) \subset \phi_n(A_2) \subset \phi_n(A_3) \subset \cdots$$

is an ascending sequence of left ideals of R;

hence, there exists a positive integer $k(n)$ such that

$$\phi_n(A_{k(n)}) = \phi_n(A_{k(n)+1}) = \phi_n(A_{k(n)+2}) = \cdots$$

Further, because R is Noetherian, the collection of left ideals $\{\phi_n(A_i)\}, n \in N, i \in N$, has a maximal element, say $\phi_p(A_q)$.

Then

$$\phi_p(A_q) = \phi_n(A_q)\ \forall\ n \geq p$$

$$= \phi_n(A_j)\ \forall\ n \geq p,\ j \geq q$$

Therefore, we may choose $k(n) = q$ for all $n \geq p$ in (1).

Moreover, if $s = k(1) \ldots k(p-1)q$, then

$$\phi_n(A_s) = \phi_n(A_{s+1}) = \cdots$$

for all $n \in N$.

Hence, by the result proved in the first paragraph, $A_s = A_{s+1} = \cdots$

Therefore, $R[x]$ is Noetherian.

Remark 7.2.2: Hilbert Basis Theorem does not hold for Artinian rings.

Let F be a field

This implies, F is Artinian.

Since F being a field is an integral domain.

Also, we know that if R is an integral domain, then so is $R[x]$.

Hence, $F[x]$ is an Integral domain.

Also, $0, 1 \in F$

Hence $0, 1 \in F[x]$

So, if $F[x]$ is Artinian, then being an Artinian integral domain, with at least two elements, $R[x]$ is a field.

But $x \in F[x]$ is not a unit.

So, we arrive at a contradiction.

That is, $F[x]$ is not Artinian.

Theorem 7.2.3: Let R be a commutative ring with unity. Let F be the family of all infinitely generated ideals of R. If R is not Noetherian, then F has a prime ideal of R as its maximal element.

Proof: Given that R is not Noetherian. Therefore, there exists some ideal of R which is not finitely generated. That is, $F \neq \phi$

Also, F is partially ordered set under the inclusion $' \subseteq '$. Now if C is a class in F, then the union of all the elements in C will be its upper bound.

By Zorn's Lemma, there exists some maximal element in F, call i: P.

If possible, let P is not the prime ideal of R. This implies, there exist elements $x, y \in R$ such that $xy \in P$ and $x \notin P, y \notin P$.

Consider the set $X = \{r \in R | rx \in P\}$

Claim:X is anideal of R containing P properly.

Since $y \in X, X \neq \phi$

Let $a, b \in X$

$\Rightarrow ax, bx \in P$

$\Rightarrow ax - bx \in P$

$\Rightarrow (a - b)x \in P$

$\Rightarrow a - b \in X$

Let $r \in R, a \in X$

Then $(ra)x = r(ax) \in P$

Therefore, $ra \in X$.

Hence, X is an ideal of R.

Let $a \in P$

$\Rightarrow ax \in P$

$\Rightarrow a \in X$

$\Rightarrow P \subseteq X$

Further, $xy \in P, yx \in P$

$y \in X$ but $y \notin P$ implies $X \neq P$

That is, P is properly contained in X.

Now, $P + < x >$ is an ideal of R containing P.

As $x \notin P, P + < x > \neq P$

Since P is a maximal element of F, $P + < x > \notin F$

This implies $P + < x >$ and X are both finitely generated.

Let $P + < x > = P_0 + < x >$ where $P_0 = < \{p_0, p_1, \dots, p_n\} >, p_i \in P$

Claim: $P = P_0 + xX$

$P_0 \subseteq P$

Again, $p_i \in P \; \forall \; i$

Therefore $\{p_0, p_1, \dots, p_n\} > \subseteq P$, hence $P_0 \subseteq P$

Also, $\forall\, r \in X, rx \in P, xX \in P$

That is, $P_0 + xX \subseteq P$

Let $p \in P$

$P \subseteq P + \langle x \rangle = P_0 + \langle x \rangle$

$\Rightarrow p = p_0 + rx, p_0 \in P_0, r \in R$

$\Rightarrow rx \in P$

$\Rightarrow r \in X$

So, $p = p_0 + rx \in P_0 + xX$

Hence, $P = P_0 + xX$

Since both P_0 and X are finitely generated, P is finitely generated. Hence, P is a prime ideal.

Theorem 7.2.4: Let R be a commutative ring with unity. Then R is Noetherian if and only if every prime ideal of R is finitely generated.

Proof:

Let R be a Noetherian ring. Then by definition, every ideal of R is finitely generated.

Hence, every prime ideal of R is finitely generated.

Conversely, let every prime ideal of R is finitely generated.

If possible, let R is not Noetherian, then by theorem, there exists at least one prime ideal of R which is infinitely generated.

So, we arrive at a contradiction.

That is, R is Noetherian.

Theorem 7.2.5: Let R be a Noetherian ring. Then every ideal of R contains a finite product of prime ideals.

Proof: If possible, let there exists an ideal of a Noetherian ring R which does not contain any product of prime ideals.

Let F be the family of all such ideals.

As per the assumption, $F \neq \phi$

Since R is Noetherian, F has a maximal element M.

$M \in F$, M is not containing any finite product of prime ideals.

This implies, M is not a prime ideal.

That is, there exist A and B, ideals of R such that $AB \subseteq M, A \nsubseteq M, B \nsubseteq M$

Consider, $(A + M)(B + M) \subseteq AB + AM + MB + M^2 \subseteq M$

Since $M \subset A + M, M \subset B + M, M \neq A + M, M \neq B + M$.

As M is an element of F, $A + M, B + M \notin F$

$A + M$ and $B + M$ contain a product of a finite number of prime ideals.

This implies $(A + M)(B + M)$ contains a finite product of prime ideals.

But $(A + M)(B + M) \subseteq M$

Hence, M contains a finite product of prime ideals. That is, $M \notin F$

So, we arrive at a contradiction.

Remark 7.2.6: Converse of Hilbert Basis Theorem

Let R be a commutative ring with unity such that $R[x]$ is Noetherian, then R is also Noetherian.

Consider a function $f: R[x] \to R$ as $f(a_0 + a_1 x + \cdots) = a_0$

Then f is$R$ $-$homomorphism.

$\forall\, a \in R, f(a) = a$, so, f is onto.

By the Fundamental theorem of homomorphism,

$$\frac{R[x]}{Ker\ f} \cong R$$

Since $R[x]$ is Noetherian, $\frac{R[x]}{<x>}$ is Noetherian and hence, R is Noetherian.

Summary

- Noetherian and Artinian modules and rings are defined.
- Noetherian and Artinian modules and rings are explained with the help of examples.
- with the help of examples proved that a right Noetherian (Artinian) ring may not be left Noetherian (Artinian).
- relation between nilpotent and nil ideals in an Artinian or Noetherian ring is elaborated.
- Hilbert Basis Theorem is proved.
- analyzed that this theorem is not true for Artinian rings.
- proved an important characterization of Noetherian rings in terms of its prime ideals.

Keywords

- Noetherian and Artinian Rings
- Noetherian and Artinian Modules
- Right Noetherian ring
- Left Noetherian ring
- Nilpotent ideals
- Nil ideals
- Hilbert basis theorem

Self Assessment

1. Let $M = \oplus \sum_{i=1}^{k} M_i$ be a direct sum of R −modules M_i. Then

A. $Hom_R(M,M)$ is an R −module

B. $Hom_R(M,M)$ is a subring of $Hom\ (M,M)$

C. $Hom_R(M,M)$ is isomorphic to a ring of matrices

D. All options are true

2. Let $M = \oplus \sum_{i=1}^{3} M_i$ be an R −module which is a direct sum of R −modules M_i. Let $\pi_3: M \to M_3$ is projection map and $\lambda_2: M_2 \to M$ be the inclusion map defined as $\pi_3(m_1, m_2,$ $m3=m3$ and $\lambda 2m2=0, m2, 0$ Then $\pi 3\lambda 2$ is

A. A one-one map

B. Onto map

C. Identity map

D. Zero map

3. Which of the following is not an Artinian ring?

A. Z (ring of integers)

B. Q (ring of rational numbers)

C. C (ring of complex numbers)

D. R (ring of real numbers)

4. For a module M over a ring R,

A. M is Artinian if and only if it is Noetherian

B. M is Artinian implies that it is not Noetherian

C. M is Noetherian implies it is not Artinian

D. M may be Noetherian as well as Artinian

5. The module of 2×2 matrices over the field of real numbers is
A. Both Noetherian and Artinian
B. Neither Noetherian nor Artinian
C. Noetherian but not Artinian
D. Artinian but not Noetherian

6. Consider the statements
I. Every vector space is Noetherian as well as Artinian
II. Every field is Noetherian as well as Artinian
A. I and II both are true
B. I is true but II is false
C. II is true but I is false
D. Both I and II are false

7. Which of the following rings is neither Noetherian nor Artinian?
A. The ring of rational numbers
B. The ring of square matrices of order k with entries from rational numbers
C. The ring of real-valued functions defined on the set of real numbers
D. The ring of integers

8. Let M be a Noetherian module. Then
A. Every submodule of M is Artinian
B. Every homomorphic image of M is Artinian
C. Every submodule of M is Noetherian
D. Every submodule of M is finite

9. Let M be a Noetherian module over a ring R. Let $0 \neq x \in M$. Then Rx
A. is always a Noetherian submodule of M
B. is always an Artinian submodule of M
C. is always a proper submodule of M
D. may or may not be a submodule of M

10. A ring R is Noetherian if and only if
A. Each subring of R is Noetherian
B. Each ideal of R is Noetherian
C. Each homomorphic image of R is Noetherian
D. For some ideal I of R, I and R/I both are Noetherian

11. Let R be a Noetherian ring. Then
A. Every subring of R is Noetherian
B. Every ideal of R is Noetherian
C. Every subring of R is Artinian
D. Every ideal of R is Artinian

12. Let R be a Noetherian ring with unity. Then
A. R always has a maximal ideal.
B. R never has a maximal ideal
C. R may or may not has a maximal ideal
D. R always has a non-zero minimal ideal

13. For the ring of integers Z, choose the incorrect statement
A. Z is PID
B. Z is ED
C. Z is Noetherian
D. Z is Artinian

14. Which of the following rings is neither Noetherian nor Artinian?
A. The ring of rational numbers
B. The ring of square matrices of order k with entries from rational numbers
C. The ring of real-valued functions defined on the set of real numbers
D. The ring of integers

15. Let R be a ring with unity. Then choose the correct statement
A. If R is PID then so is $R[x]$
B. If R is ED then so is $R[x]$
C. If R is right Noetherian, then so is $R[x]$
D. If R is right Artinian, then so is $R[x]$

Answers for Self Assessment

1.	D	2.	D	3.	A	4.	D	5.	A
6.	A	7.	C	8.	C	9.	A	10.	D
11.	B	12.	A	13.	D	14.	C	15.	C

Review Questions

1. Let $n \in N$ and $m \mid n \mid < m < n$. Then show that $\overline{m}$ is a zero divisor in Z_n.
2. List all the zero divisors in Z.
3. For which rings with unity will 1 be a zero divisor?
4. Let R be a ring and $a \in R$ be a zero divisor. Then show that every element of the principal ideal Ra is a zero divisor.
5. In a domain, show that the only solutions of the equation $x^2 = x$ are $x = 0$ and $x = 1$.
6. Prove that 0 is the only nilpotent element in a domain.
7. Let $R_1, R_2, \ldots, R_n$ be a family of Noetherian rings. Show that their direct sum $R = R_1 \oplus R_2 \oplus \cdots \oplus R_n$ is again Noetherian.
8. Prove that the intersection of all prime ideals in a Noetherian ring is nilpotent.
9. Show that every principal left ideal ring is a Noetherian ring.
10. Let R be a Noetherian ring. Show that the ring of 3×3 matrices R_3 over R is also Noetherian.
11. Let R be a Noetherian integral domain. Then show that for all $0 \neq c \in R, Rc$ is large.

Further Regarding

- Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress
- Topics in algebra by I.N. Hartstein, Wiley
- Abstract algebra by David S Dummit and Richard M Foote, Wiley

Weblinks

- https://nptel.ac.in/courses/111/102/111102009/
- https://nptel.ac.in/courses/111/105/111105112/#

Unit 08: Uniform and Primary Modules

CONTENTS

Objectives

After studying this unit, you will be able to

- observe that for every non-zero minimal left ideal $\boldsymbol{A}$ in a ring $\boldsymbol{R}$, either $\boldsymbol{A^2 = \{0\}}$ or $\boldsymbol{A = Re; e^2 = e \in R}$,
- state and prove Wedderburn— Artin Theorem,
- see important consequences of Wedderburn— Artin Theorem,
- define uniform and primary modules,
- understand prime ideals associated with a module over a noetherian ring,
- prove that a non-zero finitely generated module over a commutative noetherian ring hasonly a finite number of primes associated with it,
- state and prove Noether-Lasker Theorem.

Introduction

In this unit, you will be introduced to many concepts related to the Wedderburn— Artin Theorem and Noether Lasker theorem. You will understand the statement and proof of these theorems. Uniform and Primary modules will be explained with the help of examples.

8.1 Wedderburn Artin Theorem

Lemma 8.1.1: Let A be a minimal left ideal in a ring R. Then either $A^2 = \{0\}$ or $A = Re$, where e is an idempotent element in R.

Proof: Suppose $A^2 \neq \{0\}$.

Then there exists $a \in A$ such that $Aa \neq \{0\}$.

But $Aa \subset A$, and the minimality of A shows $Aa = A$.

From this, it follows that there exists $e \in A$ such that $ea = a$,

and, clearly,

$e \neq 0$ because $a \neq 0$.

Moreover,

$$e^2a = e(ea) = ea$$

or

$$(e^2 - e)a = 0$$

If $B = \{c \in A | ca = 0\}$,

Claim: B is a left ideal of R

Let $c,\ d \in B,\ r \in R$,

Then

$$(c - d)a = ca - da = 0 - 0 = 0$$

and

$$(rc)a = r(ca) = r0 = 0$$

Hence, $c - d,\ rc \in B\ \forall\, c,\ d \in B,\ r \in R$.

That is, B is a left ideal of R.

Claim: $B \subset A,\ B \neq A$

Let $c \in B = \{c \in A |\ ca = 0\}$

Clearly, $B \subset A$

Also, $a \in A,\ Aa \neq 0$

That is, there exists at least one element $x \in A$ such that $xa \neq 0$

But then $x \notin B$

That is, $A \neq B$

Therefore, we must have $B = \{0\}$. But, then

$$(e^2 - e)a = 0$$

implies

$$e^2 - e \in B = \{0\}$$

Hence,

$$e^2 = e$$

Now $Re \subset A$ and $Re \neq (0)$, because

$$0 \neq e = e^2 \in Re$$

Accordingly, $Re = A$.

Lemma 8.1.2: Let R be left (or right) Artinian ring with unity and no non-zero nilpotent ideals. Let $e \in R$ be an idempotent element. Then for some non-zero idempotent $e_1 \in R(1 - e)$,

(i) $e_1 e = 0$

(ii) Let $e' = e + e_1 - ee_1$; then $e'^2 = e'$ and $e_1 e' \neq 0$

(iii) $R\,(1 - e') \subset R(1 - e)$

(iv) $e_1 \notin R\,(1 - e')$

Proof:

Since

$$e_1 \in R(1 - e)$$

So, $e_1 = r(1 - e)$ for some $r \in R$

Consider, $e_1 e = r(1 - e)e = r(e - e^2) = 0$

So, $e_1 e = 0$ which proves part (i)

Let $e' = e + e_1 - ee_1$

Then

$$e'e' = (e + e_1 - ee_1)(e + e_1 - ee_1)$$
$$= e^2 + ee_1 - e^2e_1 + e_1e + e_1^2 - e_1ee_1 - ee_1e - ee_1^2 + ee_1ee_1$$

Using, the results that

$e^2 = e$, $e_1^2 = e_1$ and $e_1e = 0$,

$$e'e' = e + ee_1 - ee_1 + e_1 - ee_1$$
$$= e + e_1 - ee_1 = e'$$

So, $(e')^2 = e'$

Also,

$$e_1e' = e_1(e + e_1 - ee_1)$$
$$= e_1e + e_1^2 - e_1ee_1$$
$$= e_1 \neq 0$$

For part (iii)

Let $x \in R(1 - e')$

Then

$$x = r(1 - e'); r \in R$$

That is,

$$x = r(1 - e - e_1 + ee_1)$$
$$= r(1 - e_1 - e(1 - e_1))$$
$$= r(1 - e_1)(1 - e)$$
$$\in R(1 - e)$$

which proves part (iii)

For part (iv) Let $e_1 \in R\,(1 - e')$

Then $e_1 = r'(1 - e'); r \in R$

Consider $e_1e' = r'(1 - e')e' = 0$

But $e_1e' \neq 0$

So, $e_1 \notin R\,(1 - e')$

Lemma 8.1.3: Let R be left (or right) Artinian ring with unity and no non-zero nilpotent ideals. Then each non-zero left ideal in R is of the form Re for some idempotent e.

Proof:

Let A be any non-zero left ideal.

If we have a family of non-zero left ideals of R contained in A, then this family of left ideals contains A and hence it is non-empty.

Then since R is left Artinian, this family and hence A contains a minimal left ideal M.

By Lemma 8.1.1, either $M^2 = \{0\}$ or $M = Re$ for some idempotent e.

If $M^2 = \{0\}$,

Since M is left ideal of R, $RM \subset M$.

Hence,

$$(MR)^2 = MRMR \subset M^2R = \{0\}$$

so,

$$(MR)^2 = \{0\}$$

by hypothesis, $MR = \{0\}$

Since R is a ring with unity, so,

$MR = \{0\}$ implies $M = \{0\}$,

So, we arrive at a contradiction.

Hence, $M = Re$

Consider now a family F of left ideals, namely,

$$F = \{R(1-e) \cap A \mid 0 \neq e = e^2, e \in A\}$$

Clearly, F is non-empty.

Because R is left Artinian, F has a minimal member, say $R(1-e) \cap A$.

Claim:

We claim $R(1-e) \cap A = \{0\}$.

Otherwise, there exists a non-zero idempotent

$$e_1 \in R(1-e) \cap A$$

So, $e_1 \in R(1-e)$

By Lemma 8.1.2,

(i) $e_1 e = 0$

(ii) If $e' = e + e_1 - ee_1$ then $e'^2 = e'$ and $e_1 e' \neq 0$

(iii) $R(1-e') \subset R(1-e)$

$$(iv) e_1 \notin R(1-e')$$

This implies,

$$R(1-e') \cap A \subset R(1-e) \cap A$$

Also, If $e_1 \notin R(1-e') \cap A$, $e_1 \in R(1-e) \cap A$

This proves that

$$R(1-e') \cap A \subset R(1-e) \cap A$$

and

$$R(1-e') \cap A \neq R(1-e) \cap A$$

By minimality of $R(1-e) \cap A$,

we get a contradiction.

This establishes our claim, $R(1-e) \cap A = \{0\}$

Next, let $a \in A$.

Then $a(1-e) \in R(1-e) \cap A = \{0\}$

Thus, $a = ae$

Then $A \supset M = Re \supset Ae = A$

This implies, $A = Re$

Lemma 8.1.4: If M and N are two simple$R$ −modules such that M is not isomorphic to N then $Hom_R(M, N) = \{0\}$.

Proof: Let $0 \neq \phi \in Hom_R(M,N)$

$\phi: M \rightarrow N$ is an R − homomorphism.

$Ker\ \phi$ and $Im\ \phi$ are submodules of M and N respectively.

But M and N are simple R −modules.

So, $Ker\ \phi = \{0\}$ or M and $Im\ \phi = \{0\}$ or N

Since $\phi \neq 0$ therefore, $Ker\ \phi \neq M$ and $Im\ \phi \neq \{0\}$

Hence, $Ker\ \phi = \{0\}$ and $Im\ \phi = N$

This implies, ϕ is one-one and onto.

This gives a contradiction to the fact that M and N are not isomorphic.

Our supposition was wrong.

So, $Hom_R(M, N) = \{0\}$.

Lemma 8.1.5: Let $M = \oplus \sum_{i=1}^{k} M_i$ be a direct sum of R −modules M_i. Then

$$Hom_R(M, M) \cong \begin{bmatrix} Hom_R(M_1, M_1) & Hom_R(M_2, M_1) & \cdots & Hom_R(M_k, M_1) \\ Hom_R(M_1, M_2) & Hom_R(M_2, M_2) & & Hom_R(M_k, M_2) \\ \vdots & & \ddots & \vdots \\ Hom_R(M_1, M_k) & Hom_R(M_2, M_k) & \cdots & Hom_R(M_k, M_k) \end{bmatrix}$$

as rings.

(The right side is a ring T, say, of $k \times k$ matrices $f = [f_{ij}]$ under the usual matrix addition and multiplication, where $f_{ij} \in Hom_R(M_j, M_i)$.

The proof is given in Unit 7.

Theorem 8.1.6 (Wedderburn— Artin Theorem): Let R be left (or right) Artinian ring with unity and no non-zero nilpotent ideals. Then R is isomorphic to a finite direct sum of matrix rings over division rings.

Proof: Let A be any non-zero left ideal.

By Lemma 8.1.3, each non-zero left ideal in R is of the form Re for some idempotent e.

This implies, $A = Re$ for some idempotent element $e \in R$.

Let S be the sum of all minimal left ideals in R. Then S is a left ideal of R.

By Lemma 8.1.3, $S = Re$ for some idempotent e.

If $R(1 - e) \neq \{0\}$, then there exists a minimal left ideal A contained in $R(1 - e)$.

A is a minimal left ideal of R and S be the sum of all minimal left ideals in R. So, $A \subset S = Re$

Also, $A \subset R(1 - e)$

This implies, $A \subset Re \cap R(1 - e)$ ...(1)

Let $x \in Re \cap R(1 - e)$

Then $x = re; r \in R$

and $x = r'(1 - e)$

Consider $xe = r'(1 - e)e = 0$

But $xe = (re)e = re^2 = re$

So, $xe = 0$ implies $re = 0$

Hence, $x = 0$

This implies, $Re \cap R(1 - e) = \{0\}$

Then from (1), $A = \{0\}$

So, we arrive at a contradiction

Hence $R(1 - e) = 0$

That is, $R = Re = S$

So, $R = \sum_{i \in \wedge} A_i$; where $\{A_i\}, i \in \wedge$, is the family of all minimal left ideals in R.

So, there exists a subfamily $\{A_i\}, i \in \wedge'$ of the family of the minimal left ideals such that

$$R = \oplus \sum_{i \in \wedge'}{}' A_i;$$

Let

$$1 = e_{i_1} + e_{i_2} + \cdots + e_{i_n}; 0 \neq e_{i_j} \in A_{i_j}; i_j \in \wedge'$$

Then

$$R = Re_{i_1} + Re_{i_2} + \cdots + Re_{i_n}$$

After reindexing, if necessary, we may write

$$R = Re_1 + Re_2 + \cdots + Re_n$$

a direct sum of minimal left ideals.

In the family of minimal left ideals $Re_1, \ldots, Re_n$,

choose the largest subfamily consisting of all minimal left ideals that are not isomorphic to each other as left R-modules.

After renumbering, if necessary, let this subfamily be $Re_1, Re_2, \ldots, Re_k$.

Suppose the number of left ideals in the family $\{Re_i\}$, $1 \leq i \leq n$, that are isomorphic to Re_j is n_j.

Then

$$R = \overbrace{[\text{illegible}]}^{n_1 \, summands} \oplus \overbrace{[\text{illegible}]}^{n_2 \, summands} \oplus \ldots \oplus \overbrace{[\text{illegible}]}^{n_k \, summands}$$

where each set of brackets contains pairwise isomorphic minimal left ideals

and no minimal left ideal in any pair of brackets is isomorphic to a minimal left ideal in another pair.

By Lemma 8.1.4, $Hom_R(Re_i, Re_j) = 0 \; \forall \; i \neq j$

By Schur's Lemma, $Hom_R(Re_i, Re_i) = D_i$ is a division ring.

Using Lemma 8.1.5,

$$Hom_R(R, R) \cong \left[\begin{pmatrix} (D_1)_{n_1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & (D_k)_{n_k} \end{pmatrix} \right]$$

$$= (D_1)_{n_1} \oplus (D_2)_{n_2} \oplus \cdots \oplus (D_k)_{n_k}$$

But since $Hom_R(R, R) \cong R^{op}$ as rings

and the opposite ring of a division ring is a division ring, R is a finite direct sum of matrix rings over division rings.

Remark 8.1.7: Because the matrix rings over division rings are both right and left noetherian and Artinian,

and a finite direct sum of noetherian and Artinian rings is again noetherian and Artinian,

we get, for left (or right) Artinian ring R with unity and no non-zero nilpotent ideals, R is also right and left Artinian (noetherian).

Theorem 8.1.8: Let R be a ring with unity. Then the following are equivalent

i. R is left Artinian with no nonzero nilpotent ideals.

ii. R is left Artinian with no non-zero nil ideals.

iii. R is a finite direct sum of minimal left ideals.

iv. Each left ideal of R is of the form Re, e is idempotent.

v. R is a finite direct sum of matrix rings over division rings.

Proof: (i) implies (ii) R is left Artinian with no non-zero nilpotent ideal. Let I be a non-zero nil ideal in R. Since we know that every nil ideal is nilpotent in an Artinian ring. Hence I is a nilpotent ideal.

Therefore, R contains a non-zero nilpotent ideal which contradicts (i), hence R does not contain any non-zero nil ideal.

(i) implies (iii)Since division rings are simple rings so, by Wedderburn Artin Theorem, the result holds.

(iii) implies (iv) R is a finite sum of minimal left ideals. That is,

$$R = \oplus \sum_{\alpha \in \wedge} I_\alpha ;$$

I_α is a minimal left ideal $\forall\ \alpha \in \wedge$.

I_α is a simple ring. Also, we can choose, $\wedge' \subset \wedge$ such that

$$R = \oplus \sum_{\alpha \in \wedge'} I_\alpha$$

I_α is simple $\forall\ \alpha \in \wedge, I_\alpha \neq \{0\}$

So, $I_\alpha = < e_\alpha >;\ 0 \neq e_\alpha \in M$.

That is, $I_\alpha = Re_\alpha$or Re; $(0 \neq e \in M)$

(iv) implies (v): Let $M = Re$ be a maximal left ideal of $R. e = e^2$

Then $R(1-e)$ is a minimal left ideal.

$$\frac{R}{Re} \cong R(1-e)$$

Being isomorphic to a simple module, it is a simple module. Therefore, if S is the sum of all minimal left ideals of R then $S \neq \{0\}$.

We claim $S = R$

If $S \neq R$ then S is contained in a maximal left ideal $Rf; f = f^2$but $R(1-f)$ is a minimal left ideal which is not contained in S.

$$S \cap R(1-f) \subset Rf \cap R(1-f) = \{0\}$$

So, we arrive at a contradiction. Hence, $S = R$. So, R is a finite sum of matrix rings over division rings.

(v) implies (i): Matrix rings over division rings are both right and left Artinian. Also, a finite sum of left (right) Artinian rings is again left (right) Artinian.

Therefore, from (5), it is left (right) Artinian.

Further, the matrix rings over division rings are simple rings with unity and hence, they have no non-zero nilpotent ideal.

If $R = A_1 \oplus A_2 \oplus \ldots \oplus A_k$ is a finite direct sum of simple rings, each with unity, then any non-zero ideal is of the form

$A_{i_1} \oplus A_{i_2} \oplus \ldots \oplus A_{i_k}$. So, I is not nilpotent.

8.2 Uniform and Primary Modules

Definition 8.2.1: A non-zero module M is called uniform if any two non-zero submodules of M havea nonzero intersection.

That is, M is a uniform module if $N_1 \cap N_2 \neq \{0\}$

for any non-zero submodules N_1 and N_2 of M.

Note:

There exist modules that are never uniform. Remarks 8.2.2 and 8.2.3 prove this statement.

Remark 8.2.2: Direct sum of two uniform modules is never a uniform module.

Proof: Let N_1 and N_2 be two uniform R −modules.

Consider $N = N_1 \oplus N_2$

By the definition of direct sum, $N_1 \cap N_2 = \{0\}$

Both N_1 and N_2 are non-zero R −submodules of N such that their intersection is$\{0\}$

Hence, N is not a uniform module.

Remark 8.2.3: Let N_1 and N_2 be two proper submodules of a uniform R −module M such that neither submodule contains the other. Then $M/(N_1 \cap N_2)$ is never uniform.

Proof: Consider

$$\frac{N_1}{N_1 \cap N_2} \ and \ \frac{N_2}{N_1 \cap N_2}$$

We know that any R −submodule of $\frac{M}{N}$ is of the form $\frac{U}{N}$ where U is a R −submodule of M containing N.

Both $\frac{N_1}{N_1 \cap N_2}$ and $\frac{N_2}{N_1 \cap N_2}$ are R −submodules of $M/(N_1 \cap N_2)$.

Again $N_1 \not\subseteq N_2$ and $N_2 \not\subseteq N_1$

Therefore $\frac{N_1}{N_1 \cap N_2} \neq \{N_1 \cap N_2\}$ and $\frac{N_2}{N_1 \cap N_2} \neq \{N_1 \cap N_2\}$. That is, both the submodules are not equal to zero submodule of $M/(N_1 \cap N_2)$.

Let $x + (N_1 \cap N_2) \in N_1/(N_1 \cap N_2)$

Then $x \in N_1$

If $x \in N_2$ then $x \in N_1 \cap N_2$

That is, $x + (N_1 \cap N_2) = N_1 \cap N_2$, that is zero submodule of $M/(N_1 \cap N_2)$.

Hence, $M/(N_1 \cap N_2)$ is never uniform.

Definition 8.2.4: If U and V are uniform modules, we say U is sub-isomorphic to V and write $U \sim V$ provided U and V contain non-zero isomorphic submodules.

Theorem 8.2.5: The relation defined in Definition 8.2.4 is an equivalence relation.

Proof:

Reflexive: For a uniform module U, $f: U \to U$ defined as $f(x) = x \ \forall x \in U$ is R −isomorphism. Hence $U \sim U$ for every uniform module U.

Symmetric: Let U and V be two uniform R −modules such that $U \sim V$.

This implies, there exist U_1 and V_1 such that U_1 isa submodule of U and V_1 isa submodule of V and U_1 isisomorphic to V_1. Since the relation of isomorphism is an equivalence relation. Therefore V_1 is isomorphic to U_1 and hence $V \sim U$.

Transitive: Let U, V and W be three uniform modules such that $U \sim V$ and $V \sim W$.

Then there exist U_1, V_1 and W_1 submodules of U, V and W respectively such that $U_1 \cong V_1$ and $V_1 \cong W_1$. Again using the fact that isomorphism is an equivalence relation, we get, $U_1 \cong W_1$.

Hence, $U \sim W$.

Therefore, $\sim$ is an equivalence relation.

Definition 8.2.6: A module M is called primary if each non-zero submodule of M has a uniform submodule and any two uniform submodules of M are sub-isomorphic.

A non-zero submodule N of M is called large if $N \cap K \neq \{0\}$ for all non-zero submodules K of M.

Remark 8.2.7: Every uniform module is primary.

Proof: Let M be a uniform module.

Consider $\{0\} \neq N$ be a submodule of M.

Let N_1 and N_2 be two non-zero submodules of N and hence of M.

M is a uniform module so, $N_1 \cap N_2 \neq \{0\}$

So, N is uniform.

Let N_1 and N_2 be two non-zero uniform submodules of N.

Consider $N_1 \cap N_2 \neq \{0\}$

Also, $N_1 \cap N_2$ is an R −submodule of both N_1 and N_2.

So, we have $N_1 \cap N_2$ in both N_1 and N_2 such that $N_1 \cap N_2 \cong N_1 \cap N_2$

Hence $N_1 \sim N_2$

Therefore, M is a primary module.

Example 8.2.8: $\mathbb{Z}$ as a $\mathbb{Z}$ −module is uniform and primary.

Proof: Consider $\mathbb{Z}$ as a $\mathbb{Z}$ −module.

Let I_1 and I_2 be two non-zero submodules of $\mathbb{Z}$.

There exist $n_1, n_2 \in \mathbb{Z}$ such that

$I_1 = < n_1 >$ and $I_2 = < n_2 >$

Since $I_1, I_2 \neq \{0\}, n_1, n_2 \neq 0$

Consider $I = < n_1 n_2 >$

Since $n_1 n_2 \in < n_1 > \cap < n_2 >, I \subseteq I_1 \cap I_2$.

Also, $n_1 n_2 \neq 0$

This implies, $I = < n_1 n_2 > \neq \{0\}$

So, $\mathbb{Z}$ as a $\mathbb{Z}$ −module is uniform as well as primary.

Theorem 8.2.9: Let M be a noetherian module or any module over a noetherian ring R. Then each non-zero submodule of M contains a uniform module

Proof: Let M be a non-zero module. Then there exists at least one $0 \neq x \in M$.

If M is noetherian, xR is a submodule of M, hence it is noetherian.

If R is noetherian then xR being the homomorphic image of ring R is noetherian. Therefore, xR is noetherian.

Let $F = \{K | K$ is a submodule of xR, K is not large$\}$

Clearly, $\{0\} \in F$, hence $F \neq \phi$

Since xR is noetherian, F has a maximal element say K

then K is not large.

So, there exist non-zero submodule U of xR such that $K \cap U = \{0\}$

Claim: U is uniform.

If U is not uniform, then there exist non-zero submodules A and B of U such that $A \cap B = \{0\}$

Let $x \in (K \oplus A) \cap B$

$$x \in K \oplus A, x \in B$$

This implies, $x = k + a; k \in K, a \in A,$ and $x = b; b \in B$

So that, $b = k + a; k = b - a$

$$k \in K, b \in B \subset U; a \in A \subset U$$

Now, $b, a \in U$ and U is submodule implies, $b - a \in U$ hence $k \in U$.

$\Rightarrow k \in K \cap U = \{0\}$

$\Rightarrow k = 0$

$\Rightarrow b - a = 0$

$\Rightarrow b = a$

But then $b \in B, a \in A, a = b$

$\Rightarrow b \in B \cap A = \{0\}$

$\Rightarrow b = a = 0$

$\Rightarrow x = 0$

$(K \oplus A) \cap B = \{0\}$

$K \oplus A$ is not large.

Also, $K \subset K \oplus A$

So, we arrive at a contradiction.

Our assumption was wrong.

Hence, U is uniform.

Definition 8.2.10: If R is a commutative noetherian ring and P is a prime ideal of R, then P is said to be associated with the module M if R/P embeds in M, or equivalently $P = r(x)$ for some $x \in M$, where

$r(x) = \{a \in R | xa = 0\}$ denotes the annihilator of x.

Definition 8.2.11: A module M is called $P-$primary for some prime ideal P if P is the only prime ideal associated with M.

Remark 8.2.12: If R is a commutative noetherian ring and P is a prime ideal of R, then an $R-$module is $P-$primary if and only if each non-zero submodule of M is sub-isomorphic to R/P.

Theorem 8.2.13: Let U be a uniform module over a commutative noetherian ring R. Then U contains a submodule isomorphic to R/P for precisely one prime ideal P, that is, U is sub-isomorphic to R/P for exactly one prime ideal P. (The ideal P in the above theorem is usually called the prime ideal associated with uniform module U)

Proof: Let $F = \{r(x) | 0 \neq x \in U\}$

Since R is noetherian, there exists a maximal ideal in F. Let $r(x) \in F$ is the maximal ideal.

Claim: $P = r(x)$ is a prime ideal.

Let $ab \in P = r(x)$

$\Rightarrow xab = 0 \ldots (1)$

If $a \notin r(x)$

$\Rightarrow xa \neq 0$

Let $y \in r(x)$

$$\Rightarrow xy = 0$$

$\Rightarrow yx = 0$

$\Rightarrow (yx)a = 0$

$\Rightarrow y(xa) = 0$

$\Rightarrow y \in r(xa)$

So, $r(x) \subset r(xa)$

Also, $r(xa) \in F$

By the maximality of $r(x), r(xa) = r(x)$

From (1), $xab = 0$

$\Rightarrow b \in r(xa) = r(x)$

$\Rightarrow b \in r(x)$

$\Rightarrow xb = 0$

So, either $a \in r(x)$ or $b \in r(x)$

Hence $r(x)$ is a prime ideal.

Claim: $xR \cong \frac{R}{r(x)} = \frac{R}{P}$

Define $\phi : xR \to P + r \;\forall\; r \in R$

ϕ is homomorphism:

Let $xr_1, xr_2 \in xR, r \in R$

Consider

$$\begin{aligned} \phi(xr_1 + xr_2) &= \phi(x(r_1 + r_2)) \\ &= P + (r_1 + r_2) \\ &= (P + r_1) + (P + r_2) \\ &= \phi(xr_1) + \phi(xr_2) \end{aligned}$$

Again,

$$\begin{aligned} \phi((xr_1)r) &= \phi(x(r_1 r)) \\ &= P + r_1 r \\ &= (P + r_1) r \\ &= \phi(xr_1) r \end{aligned}$$

Hence, ϕ is $R -$ homomorphism.

Since R is commutative

$$\phi\left(r(xr_1)\right) = r\phi(xr_1)$$

ϕ is one-one

Let $\phi(xr_1) = \phi(xr_2)$

$\Rightarrow P + r_1 = P + r_2$

$\Rightarrow r_1 - r_2 \in P = r(x)$

$\Rightarrow x(r_1 - r_2) = 0$

$\Rightarrow xr_1 = xr_2$

Therefore, ϕ is one-one.

ϕ is onto

Let $P + r \in \frac{R}{P}$ be any element of $\frac{R}{P}$; $r \in R$

Since $r \in R, xr \in xR$

Then $\phi(xr) = P + r$

Hence, ϕ is onto.

$\phi: xR \to R/P$ is an R −isomorphism.

So, $xR \cong \frac{R}{P}$

R/P is embedded in U.

Uniqueness: If for any other prime ideal $Q, U \sim R/Q$ that is, R/Q is embedded in U then

$$\left[\frac{R}{P}\right] = \left[\frac{R}{Q}\right] = [U]$$

So, there exist cyclic submodules xR and yR of R/P and R/Q respectively such that $xR \cong yR$.

but $xR \cong \frac{R}{P}$ and $yR \cong \frac{R}{Q}$

This implies, $\frac{R}{P} \cong \frac{R}{Q}$ and hence $P = Q$.

Definition 8.2.14: We proved that if U is a uniform module over a commutative noetherian ring R. Then U contains a submodule isomorphic to R/P for precisely one prime ideal P. This unique prime ideal is called prime ideal associated with uniform module U.

Theorem 8.2.15: Let M be a non-zero finitely generated module over a commutative noetherian ring R. Then there are only a finite number of primes associated with M.

Proof: Let F be the family of direct sums of cyclic uniform submodules of M. Then $F \neq \phi$.

Define partial order relation $' \leq '$ on F by

$$\oplus \sum_{i \in I} x_i R \leq \oplus \sum_{j \in J} y_j R$$

if and only if $I \subseteq J$ and $x_i R \subseteq y_i R \; \forall \; i \in I$

By Zorn's lemma, F has a maximal element N.

Let

$$N = \oplus \sum_{\lambda \in \Lambda} x_\lambda R$$

Also, M is noetherian, so N is finitely generated.

That is,

$$N = \oplus \sum_{i=1}^{m} x_i R$$

for some positive integer m.

As each $x_i R$ is uniform, there exists $x_i a_i \in x_i R$ such that $P_i = r(x_i a_i)$ is prime ideal associated with $x_i R$.

Let

$$K = \sum_{i=1}^{m} x_i a_i R$$

Claim: If Q is any associated prime ideal of M then $Q = P_i$ for some i; $1 \leq i \leq m$.

Since Q is associated prime, $Q = r(x); x \in M$.

Since N is a maximal member in F.

$N \cap L$ and $K \cap L$ are both non-zero for all non-zero submodules L of M.

Therefore,

$xR \cap K \neq \{0\}$

Let $0 \neq y \in xR \cap K$

$\Rightarrow y = xr; r \in R$ and $y = \sum_{i=1}^{m} x_i a_i r_i$

Let $x_i a_i r_i s = 0$

$\Rightarrow r_i s \in r(x_i a_i) = P_i$

Suppose $x_i a_i r_i \neq 0$

$\Rightarrow r_i \notin P_i$

$\Rightarrow s \in P_i$

Therefore, P_i is prime.

Hence if $x_i a_i r_i \neq 0$ then $r(x_i a_i) = r(x_i a_i r_i)$

Now,

$$r(y) = \bigcap_{i=1}^{m} r(x_i a_i r_i)$$
$$= \bigcap_{i \in \Lambda} r(x_i a_i)$$
$$= \bigcap_{i \in \Lambda} P_i$$

where $i \in \Lambda$ implies, $x_i a_i r_i \neq 0$

Now

$$\frac{R}{Q} \cong xR$$

Therefore, there exist $\theta: \frac{R}{Q} \to xR$ which is one-one, onto, and R −homomorphism.

For $y \in xR$, $\theta^{-1}(yR)$ is a cyclic submodule of $\frac{R}{Q}$, that is, $\theta^{-1}(yR) \cong R/Q$.

Now

$$Q = r(x) = r(y) = \bigcap_{i \in \Lambda} P_i$$

Therefore, $Q \subset P_i \; \forall \, i$

Suppose $P_i \nsubseteq Q \; \forall \, i \in \Lambda$

There exists $x_i \in P_i$ such that $x_i \notin Q \; \forall \, i$.

As

$$\prod_{i \in \Lambda} x_i \in \bigcap P_i = Q$$

and Q is prime

therefore, there exists at least one $x_i \in Q$.

So, we arrive at a contradiction.

Hence, $P_i \subset Q$ for some i.

Therefore, $P_i = Q$ for some $i \in \Lambda$

Task:

1. Prove that a vector space over a field F is uniform if and only if it is one-dimensional.
2. Prove that one-dimensional subspaces of a vector space are always primary.

8.3 Noether Lasker Theorem

Theorem 8.3.1: Noether- Lasker Theorem: Let M be a finitely generated module over a commutative noetherian ring R. Then there exists a finite family $N_1, \ldots, N_t$ of submodules of M such that

a) $\bigcap_{i=1}^{t} N_i = \{0\}$ and $\bigcap_{i=1,\, i\neq i_0}^{t} N_i \neq \{0\}$ for all $1 \leq i_0 \leq t$.

b) Each quotient M/N_i is a P_i −primary module for some prime ideal P_i.

c) The P_i are all distinct, $1 \leq i \leq t$.

d) The primary component N_i is unique if and only if P_i does not contain P_j for any $j \neq i$

Proof: Consider the uniform modules $Rx_i, 1 \leq i \leq m$

Choose Rx_i's such that $[Rx_i] \neq Rx_j]$ for $i \neq j$

After re-indexing, we take

$$U_i = Rx_i, 1 \leq i \leq t$$

Note that $[Rx_i] = Rx_j]$

$\Rightarrow \left[\frac{R}{P_i}\right] = \left[\frac{R}{P_j}\right]$

$\Rightarrow \frac{R}{P_i} \cong \frac{R}{P_j}$

$\Rightarrow P_i = P_j$

Hence the only prime ideals associated with M are $P_1, P_2, \ldots, P_t$ and P_i's are all distinct which proves part (c).

Let F_i be the family of submodules of M which do not contain any submodule sub-isomorphic to U_i, $1 \leq i \leq t$.

Let N_i be the maximal element of F_i.

(a) Suppose

$$\bigcap N_i \neq \{0\}$$

This implies, $\cap N_i$ contains a uniform module U.

Let P be the unique prime associated with U. Then P is the associated prime of M.

Therefore, $P = P_j$ for some $1 \leq j \leq t$.

$$\Rightarrow [U] = \left[\frac{R}{P_j}\right] = U_j]$$

as $U \subseteq N_j$, we arrive at a contradiction.

Claim: Every uniform submodule of $\frac{M}{N_i}$ belongs to $[U_i]$.

Let N be any submodule of M containing N_i.

If N_i is a proper submodule of N. This implies, $N \notin F_i$.

Hence, we can find a uniform submodule U of N such that there exists a one-one map $\theta: U \to U_i$

Restricting θ to $U \cap N_i$, we get a submodule of $U \cap N_i$ in U_i.

By choice of $F_i, U \cap N_i = \{0\}$

Thus, the map

$$\theta^*: \frac{U + N_i}{N_i} \to U_i$$

as $\theta^*(x + N_i) = \theta(x) \; \forall x \notin N_i$ remains an embedding.

Proof of (*a*):Let U be a uniform submodule of M such that $U \in [U_i]$

Then there does not exist any monomorphism from U to $\frac{M}{N_j}$ for $i \neq j$.

Hence $U \cap N_j \neq 0$ for $i \neq j$.

As U is uniform,

$\bigcap_{i \neq j} (U \cap N_j) \neq \{0\}$

$\Rightarrow U \cap \left(\bigcap_{i \neq j} N_j \right) \neq \{0\}$

$\Rightarrow \bigcap_{i \neq j} N_j \neq \{0\}$

*(b)*Let Q be a prime ideal associated with $\frac{N}{N_i}$.

Let U is the submodule of $\frac{M}{N_i}$ such that $U \cong \frac{R}{Q}$.

Then U is a uniform submodule of M/N_i.

Hence, $U \in [U_i]$

$$\left[\frac{R}{Q}\right] = [U] = [U_i].$$

$\Rightarrow Q = P_i$ as P_i is unique prime associated with U_i. Thus M/N_i is P_i −primary.

(*c*) is already proved.

(*d*) AssumeN_i is unique.

Suppose for some $j \neq i, P_j \subseteq P_i$

Let $f: \frac{R}{P_j} \to \frac{R}{P_i}$ is given by $f(r + P_j) = r + P_i$.

Then if $r \in P_j, r \in P_i$, so f is well defined.

Since $f(1 + P_j) \neq P_i$ that is, non-zero.

Therefore, f is non-zero R −homomorphism.

Let U and V be uniform submodules of U_j and U_i respectively such that $U \cong R/P_j$ and $V \cong R/P_i$.

Hence, there exists a non-zero homomorphism

$$g: U \to \frac{R}{P_j} \to \frac{R}{P_i} \to V.$$

Let $x \in U$ such that $g(x) \neq 0$

Claim:$rx = 0 \Leftrightarrow r\left(x - \left(g(x)\right)\right) = 0$

Suppose $rx = 0$

Then $g(rx) = 0$

$\Rightarrow rg(x) = 0$

$\Rightarrow r(x - g(x)) - rx - rg(x) = 0$

Conversely, let $r(x - g(x)) = 0$

$\Rightarrow r(x) = rg(x) \in U \cap V$

As $U \in [U_j]$ and $V = [U_i]$

$U \cap V = \{0\}$

$\Rightarrow rx = 0$

$Rx \cong \frac{R}{r(x)}$

$\cong R(x - g(x))$

As $U \in [U_j]$, $U \in F_i$

$\Rightarrow Rx \in F_i$ and hence $R(x - g(x)) \in F_i$

Let N_0 and N_0^* be maximal elements of F_i containing Rx and $R(x - g(x))$ respectively.

As maximal element of F_i is unique.

Hence $N_0 = N_0^*$.

$\Rightarrow Rx + R(x - g(x)) \in F_i$

$\Rightarrow Rg(x) \in F_i$

But $g(x) \in V$ and $[V] = [U_i]$

So, we arrive at a contradiction.

That is, $P_j \not\subseteq P_i \; \forall j \neq i$

$\Rightarrow$ there does not exist any non-zero R −homomorphism from R/P_j to R/P_i.

Let N and L be two maximal elements of F_i.

Then $N \not\subseteq L$ and $L \not\subseteq N$ if $N \neq L$

$\Rightarrow$ The map $M \rightarrow \frac{M}{N}$ gives a non-zero homomorphism $\theta: L \rightarrow \frac{M}{N}$

Every uniform submodule of $\frac{M}{N}$ belongs to $[U_i]$.

Hence P_i is the prime ideal associated with $\frac{N}{N}$.

Let U be the uniform submodule of M/N isomorphic to R/P_i. Restricting θ to V, the pre-image of U under θ, we get a homomorphism from V to R/P_i.

As $V \in F_i$, P_j is a prime associated with V for some $j \neq i$.

Consequently, we get a non-zero homomorphism from $\frac{R}{P_j}$ to $\frac{R}{P_i}$, which is a contradiction. Hence, F_i has a unique maximal element.

Summary

- observed that for every non-zero minimal left ideal $\boldsymbol{A}$ in a ring $\boldsymbol{R}$, either $\boldsymbol{A^2} = \{\boldsymbol{0}\}$ or $\boldsymbol{A} = \boldsymbol{Re}; \boldsymbol{e^2} = \boldsymbol{e} \in \boldsymbol{R}$.
- Wedderburn— Artin Theorem is proved.
- Important consequences of Wedderburn— Artin Theorem are explained.
- Uniform and primary modules are defined.
- Prime ideals associated with a module over a noetherian ring are explained.
- Noether-Lasker Theorem is proved.

Keywords

- Wedderburn Artin Theorem

- Uniform Modules
- Primary Modules
- Prime ideals
- Noether Lasker Theorem

Self Assessment

1. Let A be a minimal left ideal in a ring R such that $A^2 \neq \{0\}$. Then

A. $A = Re$ where $e = e^2 \in R$

B. $A = Re$ where e is the unity of R

C. $A = \{e\}$ where e is the unity of R

D. $A = R$

2. Let A is the minimal left ideal of a ring R and B is any left ideal of R. Then

A. B is contained in A

B. B contains A

C. If B is contained in$A$, then $B = A$

D. If B contains A, then $B = A$

3. Let M be a simple R −module. Let f be an R −endomorphism on M. Then

A. f is always 1-1

B. f is 1-1 if and only if $f \neq 0$

C. f is 1-1 if and only if $f = 0$

D. f is never 1-1

4. Let M be a simple R −module. Let f be an R −endomorphism on M. Then

A. f is always onto

B. f is onto if and only if $f \neq 0$

C. f is onto if and only if $f = 0$

D. f is never onto

5. Let R be a left Artinian ring with unity and no nonzero nilpotent ideals

A. All ideals of R are nil ideals

B. R has no nil ideal

C. $R = \{0\}$

D. R has no non-zero nil ideal

6. Let R be a left Artinian ring with unity and no non-zero nilpotent ideals. Then each non-zero left ideal of R is of the form Re, where e is

A. Additive identity of R

B. Multiplicative identity of R

C. Any element of R

D. An idempotent element of R

7. Let R be a left Artinian ring with unity and no non-zero nilpotent ideals. If S is the sum of all minimal left ideals in R, then

A. S is a minimal left ideal of R

B. S is a left ideal of R

C. S is the maximal left ideal of R

D. S may or may not be a left ideal of R

8. True/False Let R be a left Artinian ring with unity and no non-zero nilpotent ideal. Then R is always right Artinian

A. True
B. False

9. Let M be a non-zero uniform module and I and J are two non-zero submodules of M then
A. $I \cup J = M$
B. $I \oplus J = M$
C. $I \cap J \neq \{0\}$
D. $I \cap J = \{0\}$

10. True/False Two uniform submodules of the Z −module Z are sub-isomorphic.
A. True
B. False

11. True/ False Each non-zero submodule of a noetherian module contains a uniform module.
A. True
B. False

12. Let P be a prime ideal of R and M be an P −primary R −module. Then the number of prime ideals associated with M is
A. 0
B. 1
C. 2
D. Infinite

13. Let M be an R module. Then
A. M is primary if and only if it is uniform
B. M is uniform implies it is primary
C. M is primary implies it is uniform
D. If M is not uniform, it cannot be prime

14. Let M be a non-zero finitely generated noetherian module over a commutative ring R. Let there are n primes associated with M. Then
A. $n = 0$
B. $n = 1$
C. n is a finite number
D. n may be infinite

15. Let U is a uniform module over a commutative noetherian ring R. Then the unique prime ideal P for which U contains a submodule isomorphic to R/P is called …… ideal associated with uniform module U.
A. prime
B. Irreducible
C. Maximal
D. Zero

Answers for Self Assessment

1. A	2. C	3. B	4. B	5. D
6. D	7. B	8. A	9. C	10. A

11. A 12. B 13. B 14. C 15. A

Review Questions

1. Let R be a left Artinian ring with unity and no non-zero nilpotent ideals. Then show that for each ideal I of R, R/I is also left Artinian with no non-zero nilpotent ideals.
2. Let R be a prime left Artinian ring with unity. Show that R is isomorphic to the $n \times n$ matrix over a division ring. Hence, show that a prime ideal in an Artinian ring is maximal.
3. Let R be an Artinian ring. Then show that the following sets are equal ideals:
   N = sum of nil ideals
   U = sum of all nilpotent left ideals
   V =sum of all nilpotent right ideals
4. Let N, U, and V be as defined in question 3, show that R/N has no non-zero nil ideals.
5. Let R be a finite-dimensional algebra over an algebraically closed field F. Suppose R has no non-zero nil ideals. Show that R is isomorphic to the direct sum of matrix rings over F.

Further Readings

- Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress
- Topics in algebra by I.N. Hartstein, Wiley
- Abstract algebra by David S Dummit and Richard M Foote, Wiley

Weblinks

- https://nptel.ac.in/courses/111/102/111102009/
- https://nptel.ac.in/courses/111/105/111105112/#

Unit 09: Smith Normal Form

CONTENTS

Objective

After studying this unit, you will be able to

- find Smith Normal Form of an $m \times n$ matrix over a PID R,
- understand the Smith Normal Form with the help of examples,
- define row module, column module and rank of a matrix,
- prove that for a matrix A over a PID, row rank of A is equal to column rank of A,
- express a finitely generated module over a PID as a direct sum of R −modules,
- define torsion module and understand results about torsion modules,
- important result on Fundamental theorem (Structure theorem) of finitely generated module over a PID,
- explain the applications of Structure theorem with the help of examples.

Introduction

In this unit, you will be able to understand Smith Normal form of an $m \times n$ matrix over a PID R with the help of examples. Further, row module, column module and rank of module will be defined. Torsion modules will be defined and Fundamental theorem of finitely generated module over a PID will be proven.

9.1 Smith Normal form over a PID

Definition 9.1.1: Let A be an $m \times n$ matrix over R. The following three types of operations on the rows (columns) of A are called elementary row (column) operations.

Interchanging two rows (columns): We denote by $R_i \leftrightarrow R_j$, $(C_i \leftrightarrow C_j)$, the operation of interchanging the $i-th$ and $j-th$ rows (columns).

Multiplying the elements of one row (column) by a non-zero element of R. We denote by αR_j, (αC_j) the operation of multiplying the $j-th$ row (column) by $\alpha \in R$.

Adding to the elements of one row (column) α times the corresponding elements of a different row (column), where $\alpha \in R$. We denote by $R_i + \alpha R_j$ $(C_i + \alpha C_j)$ the operation of adding to the elements of the $i - th$ row (column) α times the corresponding elements of the $j - th$ row (column).

Example 9.1.2:

Consider the 4×4 matrix over the field of real numbers given by

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

Then Applying first operation on A, $R_2 \leftrightarrow R_1$, we get,

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

Applying second operation on A, $R_1 \to 3R_1$, we get,

$$\begin{bmatrix} 1 & 0 & 2 & 3 \\ -1 & 2 & 1 & 2 \\ 2 & 0 & 0 & 1 \\ 3 & -1 & 1 & 1 \end{bmatrix} \sim \begin{bmatrix} 3 & 0 & 6 & 9 \\ -1 & 2 & 1 & 2 \\ 2 & 0 & 0 & 1 \\ 3 & -1 & 1 & 1 \end{bmatrix}$$

Applying third operation on A, $R_2 \to R_2 + 3R_1$, we get,

$$\begin{bmatrix} 1 & 0 & 2 & 3 \\ -1 & 2 & 1 & 2 \\ 2 & 0 & 0 & 1 \\ 3 & -1 & 1 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 2 & 3 \\ 2 & 2 & 7 & 11 \\ 2 & 0 & 0 & 1 \\ 3 & -1 & 1 & 1 \end{bmatrix}$$

Similarly, we can apply operations on columns.

Notation: We denote e_{ij}, $1 \le i, j \le n$, the $n \times n$ matrix units. That is, e_{ij} is square matrix of order n with $(i, j)th$ entry 1, all other entries 0.

For example, e_{32} of 4×4 order is

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

Remarks 9.1.3: We show that

$$e_{ij}e_{jl} = e_{il}$$

and

$$e_{ij}e_{kl} = 0 \; \forall \; j \ne k$$

Let us denote $(p, q)th$ entries of e_{ij} and e_{jl} as a_{pq} and b_{pq} respectively.

Then

$(i, l) - th$ entry of $e_{ij}e_{jl} = \sum_{k=1}^{n} a_{ik} b_{kl}$

Now, $a_{iq} = 1$ if and only if $q = j$, otherwise $a_{iq} = 0$

So, $\sum_{k=1}^{n} a_{ik} b_{kl} = a_{ij} b_{jl} = b_{jl} = 1$

Again consider $p \ne i$ or $q \ne l$,

$(p, q) - th$ entry of $e_{ij}e_{jl} = \sum_{k=1}^{n} a_{pk} b_{kq}$

Since $p \ne i$, $a_{pk} = 0 \; \forall \; k$

Hence, $(p, q) - th$ entry of $e_{ij}e_{jl} = 0 \; \forall \; p \ne i, q \ne l$

Therefore, only (i, l) the entry of $e_{ij}e_{jl} = 1$, all others 0.

That is, $e_{ij}e_{jl} = e_{il}$

Remarks 9.1.4: Now we prove

$$e_{ij}e_{kl} = 0 \ \forall\ j \neq k$$

Let us denote $(p, q)th$ entries of e_{ij} and e_{kl} as a_{pq} and b_{pq} respectively.

Then

$(p,\ q) - th$ entry of $e_{ij}e_{kl} = \sum_{n=1}^{n} a_{pm}b_{mq}$

If $m \neq j$, then $a_{pm} = 0$

So, $\sum_{n=1}^{n} a_{pm}b_{mq} = a_{pj}b_{jq}$

$a_{pj} = 1$ if and only if $p = i$, otherwise it is equal to 0.

Then

$(p,\ q) - th$ entry of $e_{ij}e_{kl} = b_{jq}$ if $p = i$, otherwise it is 0.

But $b_{kl} = 1$, $b_{jq} = 0 \ \forall\ j \neq k, \forall q$

This implies, $b_{jq} = 0$

Hence, $e_{ij}e_{kl} = 0 \ \forall\ j \neq k$

Therefore, we can say that $e_{ij}e_{kl} = \delta_{jk}e_{il}$ where δ_{jk} is the Kronecker delta.

Theorem: Let A be an $m \times n$ matrix over R.

(i) If $E_{ij} = 1 - e_{ii} - e_{jj} + e_{ij} + e_{ji}$,

then $E_{ij}A(AE_{ij})$ is the matrix obtained from A by interchanging the $i - th$ and the $j - th$ rows (columns).

Also, $E_{ij}^{-1} = E_{ij}$

(ii) *If* $L_i(\alpha) = 1 + (\alpha - 1)e_{ii}$ *and* α *is an invertible element in* R,

then $L_i(\alpha)A\ [AL_i(\alpha)]$ *is the matrix obtained from* A *by multiplying the* $i - th$ *row (column) by* α.

Also, $L_i^{-1}(\alpha) = 1 + (\alpha^{-1} - 1)e_{ii}$.

(iii) *If* $M_{ij}(\alpha) = 1 + \alpha e_{ij}$,

then $M_{ij}(\alpha)A\ [AM_{ij}(\alpha)]$ is the matrix obtained from A by multiplying the $j - th$ row (column) by α and adding it to the $i - th$ row (column).

Also, $M_{ij}^{-1}(\alpha) = 1 - (\alpha)e_{ij}$.

Proof:

Let $(p,\ q)th$ entry of e_{ij} and A is b_{pq} and a_{pq} respectively.

Then $(p,\ q)th$ entry of $e_{ij}A$ is given by $\sum_{k=1}^{n} b_{pk}a_{kq}$

But by the definition of e_{ij}, $b_{ij} = 1$, $b_{pq} = 0$ *if* $p \neq i$ or $q \neq j$.

In particular, $b_{pk} = 0 \ \forall\ k \neq j$

Hence, $(p,\ q)th$ entry of $e_{ij}A$ is given by $b_{pj}a_{jq}$.

Also, $b_{ij}a_{jq} = a_{jq}$ if $p = i$

Otherwise, 0

Which clearly implies that,

$e_{ij}A$ is the matrix whose $i - th$ row is the $j - th$ row of A, and all other rows are zero.

Taking $i = j$, we get that $e_{ii}A$ is the matrix whose $i - th$ row is the same as that of A, and all other rows are zero.

Then

$$E_{ij}A = (1 - e_{ii} - e_{jj} + e_{ij} + e_{ji})A$$

$$= A - e_{ii}A - e_{jj}A + e_{ij}A + e_{ji}A$$

This expression has no change on any row of A except the $i-th$ and $j-th$ row.

The complete expression on right side thus interchanges the $i-th$ and $j-th$ rows of A.

Moreover,

E_{ij} interchanges the $i-th$ and $j-th$ rows of A.

Again, applying E_{ij}, we are again interchanging the $i-th$ and $j-th$ rows and thus getting them at their original place back.

That is,

$$E_{ij}^2 = I$$

or,

$$E_{ij}^{-1} = E_{ij}$$

For part (ii)

Consider $L_i(\alpha) = 1 + (\alpha - 1)e_{ii}$ and α is an invertible element in R,

then $L_i(\alpha)A = (1 + (\alpha - 1)e_{ii})A$

$$= A + (\alpha - 1)e_{ii}A$$

Note that in $e_{ii}A$, all rows except the $i-th$ row are zero and $i-th$ is same as that of A

So, for $c \in R, ce_{ii}A$ has all rows except the $i-th$ row are zero and $i-th$ is c times the $i-th$ row of A.

That is, $i-th$ row of $(\alpha-1)e_{ii}A$ is $\alpha - 1$ times $i-th$ row of A and hence $i-th$ row of $A + (\alpha - 1)e_{ii}A$ is $(1 + \alpha - 1)$ times that is, α times the $i-th$ row of A.

Also, for any $j \neq i$, since $j-th$ row of $(\alpha - 1)e_{ii}A$ is 0, so, $j-th$ row of $A + (\alpha - 1)e_{ii}A$ is same as the $j-th$ row of A.

So, $L_i(\alpha)A$ denotes the matrix obtained from A by multiplying the $i-th$ row (column) by α.

Further, consider

$$(1 + (\alpha - 1)e_{ii})(1 + (\alpha^{-1} - 1)e_{ii}) = 1 + (\alpha^{-1} - 1 + \alpha - 1)e_{ii} + (1 - \alpha - \alpha^{-1} + 1)e_{ii}^2$$

Since $e_{ii}^2 = e_{ii}$

So, we get,

$$(1 + (\alpha - 1)e_{ii})(1 + (\alpha^{-1} - 1)e_{ii}) = 1$$

Hence,

$$L_i^{-1}(\alpha) = 1 + (\alpha^{-1} - 1)e_{ii}$$

Part $(iii) M_{ij}(\alpha) = 1 + \alpha e_{ij}$.

The matrix $e_{ij}A$ is the matrix whose $i-th$ row is the $j-th$ row of A, and all other rows are zero.

Hence, the matrix $\alpha e_{ij}A$ is the matrix whose $i-th$ row is α times the $j-th$ row of A, and all other rows are zero.

The matrix $M_{ij}(\alpha)A = A + \alpha e_{ij}A$ is the matrix with $i-th$ row as sum of $i-th$ row of A and α times the $j-th$ row of A, all other rows are same as that of matrix A.

Moreover,

Consider

$$(1 + \alpha e_{ij})(1 - \alpha e_{ij}) = 1 + \alpha e_{ij} - \alpha e_{ij} - \alpha^2 e_{ij}^2$$

$$= 1 - \alpha^2 e_{ij}^2$$

Note that e_{ij} is the matrix with $(i, j)th$ entry 1, all other entries 0.

So, $e_{ij}^2 = 0$

Hence, $(1 + \alpha e_{ij})(1 - \alpha e_{ij}) = 1$

Definition 9.1.5: The matrices E_{ij}, $L_i(\alpha)$ and $M_{ij}(\alpha)$ are known as elementary matrices.

Note:

An elementary matrix is the result of performing a single elementary row or column operation on an identity matrix.

Precisely,

E^{ij} = the matrix obtained from the identity matrix by interchanging the $i-th$ and $j-th$ rows (equivalently, interchanging the $i-th$ and $j-th$ columns).

$L^i(\alpha)$ = the matrix obtained from the identity matrix by multiplying the $i-th$ row by a non-zero $\alpha \in R$ (equivalently, by multiplying the $i-th$ column by by a non-zero $\alpha \in R$)

$M^{ij}(\alpha)$ = the matrix obtained from the identity matrix by adding to the elements of the $i-th$ row α times the corresponding elements of the $j-th$ row, where $\alpha \in R$ (It is also the matrix obtained from the identity matrix by adding to the elements of the $i-th$ column α times the corresponding elements of the $j-th$ column]

In addition to these three elementary rows (column) operations, we apply a non-elementary operation to the rows and columns of A:

that is, multiplication by matrices of the form

$$\begin{bmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & \ddots & & & & \\ & & & \begin{bmatrix} u & s \\ v & t \end{bmatrix} & & & \\ & & & & \ddots & & \\ & & & & & 1 & \\ & & & & & & 1 \end{bmatrix}$$

where $\begin{bmatrix} u & s \\ v & t \end{bmatrix}$ is invertible in R_2, the ring of square matrices of order 2 over R.

Multiplying A on the right (left) by a suitable matrix of the above form has the effect of replacing two of the entries on a given row (column) by their greatest common divisor and 0, respectively.

Definition 9.1.6: Consider two $m \times n$ matrices A and B over R. Then A is said to be equivalent to B if there exists an invertible matrix $P \in R_m$ and an invertible matrix $Q \in R_n$, such that $B = PAQ$.

Now we see that "being equivalent" defines an equivalence relation in the set of $m \times n$ matrices with entries in R.

Theorem 9.1.7: Being equivalent is an equivalence relation on the set of $m \times n$ matrices.

Every matrix A of order $m \times n$ can be written as

$$A = I_m A I_n$$

where I_k is the identity matrix of order k.

So, this relation is reflexive.

Consider, two matrices A and B of order $m \times n$,

such that A is equivalent to B.

That is, there exists an invertible matrix $P \in R_m$ and an invertible matrix $Q \in R_n$, such that $B = PAQ$.

P and Q are both invertible. So, pre-multiplying both sides by P^{-1} and post- multiplying both sides by Q^{-1}, we get, $P^{-1}BQ^{-1} = A$

So, B is equivalent to A.

That is, the relation of equivalence of matrices of order $m \times n$ is symmetric.

Consider, three matrices A, B and C of order $m \times n$,

such that A is equivalent to B and B is equivalent to C.

That is, there exist invertible matrix $P_1, P_2 \in R_m$ and an $Q_1, Q_2 \in R_n$, such that $B = P_1AQ_1$ and $C = P_2BQ_2$.

$$C = P_2BQ_2 = P_2P_1AQ_1Q_2$$

Being product of two invertible matrices, P_2P_1 and Q_1Q_2 are both invertible.

So, A is equivalent to C.

That is, the relation of equivalence of matrices of order $m \times n$ is transitive and hence, an equivalence relation.

Theorem 9.1.8: If A is an $m \times n$ matrix over a principal ideal domain R, then A is equivalent to a matrix that has the "diagonal" form

$$\begin{bmatrix} a_1 & & & & & & & \\ & a_2 & & & & & & \\ & & \ddots & & & & & \\ & & & a_r & & & & \\ & & & & 0 & & & \\ & & & & & 0 & & \\ & & & & & & \ddots & \\ & & & & & & & 0 \end{bmatrix}$$

where $a_i \neq 0$, $a_1|a_2|a_3|\cdots|a_r$

Proof:

We define the length $l(a)$ of $a \neq 0$ to be the number of prime factors occurring in the factorization, $a = p_1p_2 \dots p_r$, where p_i are all primes (not necessarily distinct). We use the convention that $l(u) = 0$ if u is a unit.

If $A = 0$, then there is nothing to prove. Otherwise, let a_{ij} be a non-zero element of A with minimal length $l(a_{ij})$. Elementary row and column operations bring this element to the (1,1) position.

We may then assume that the non-zero element of A with smallest length is at the (1,1) position.

Let a_{11} does not divide a_{1k}.

Interchanging the second and the $k-th$ columns, we may assume a_{11} does not divide a_{12}.

Let $d = (a_{11}, a_{12})$ be the greatest common divisor of a_{11} and a_{12}.

Then $l(d) < l(a_{11})$. There exist elements $u, v \in R$ such that $a_{11}u + a_{12}v = d$

Because $d = (a_{11}, a_{12})$ be the greatest common divisor of a_{11} and a_{12}, there exist $s, t \in R$ such that

$$a_{11} = ds,\ a_{12} = dt$$

Also,

$$a_{11}u + a_{12}v = d$$
$$dsu + dtv = d$$

so that,

$$us + vt = 1$$

It can be verified that

$$\begin{bmatrix} u & t \\ v & -s \end{bmatrix}\begin{bmatrix} s & t \\ v & -u \end{bmatrix} = \begin{bmatrix} us + tv & ut - ut \\ vs - vs & vt + us \end{bmatrix}$$
$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

which implies that $\begin{bmatrix} u & t \\ v & -s \end{bmatrix}$ is invertible. Multiplying A on the right by

$$\begin{bmatrix} \begin{bmatrix} u & s \\ v & t \end{bmatrix} & & & & & & \\ & 1 & & & & & \\ & & \ddots & & & & \\ & & & 1 & & & \\ & & & & \ddots & & \\ & & & & & 1 & \\ & & & & & & 1 \end{bmatrix}$$

We obtain the matrix whose first row is

$$(d \quad 0 \quad b_{13} \quad \dots \quad b_{1n})$$

where $l(d) < l(a_{11})$.

Continuing this process yields an equivalent matrix whose first row has all entries 0, except the (1,1) entry.

Similarly, appropriate elementary row operations (i)— (iii) and the non-elementary operation of multiplying on the left by the matrix of the form given in (iv) reduce the elements in the first column after the (1,1) position to 0 and either keep the elements in the first row unaltered (i.e., all apart from (1,1) entry are zero) or reduce the length of the (1,1) entry.

In the second case, we repeat the process by which all the elements in the first row except the one at the (1,1) position are reduced to 0. Because $l(a_{11})$ is finite, this process (of alternately reducing the first row and the first column) must come to an end. When it does, we have reduced A to the form

$$P_1AQ_1 = \begin{bmatrix} a_1 & 0 & 0 & \dots & 0 \\ 0 & & & & \\ 0 & & A_1 & & \\ \vdots & & & & \\ 0 & & & & \end{bmatrix}$$

where A_1 is an $(m-1) \times (n-1)$ matrix, and P_1 and Q_1 are $m \times m$ and $n \times n$ invertible matrices respectively.

Similarly, there exist invertible matrices P_2' and Q_2' of orders $(m-1) \times (m-1)$ and $(n-1) \times (n-1)$, respectively such that,

$$P_2'A_1Q_2' = \begin{bmatrix} a_2 & 0 & 0 & \dots & 0 \\ 0 & & & & \\ 0 & & A_2 & & \\ \vdots & & & & \\ 0 & & & & \end{bmatrix}$$

where A_2 is an $(m-2) \times (n-2)$ matrix.

Let

$$P_2 = \begin{bmatrix} 1 & 0 \\ 0 & P_2' \end{bmatrix} \text{ and } Q_2 = \begin{bmatrix} 1 & 0 \\ 0 & Q_2' \end{bmatrix}$$

be, respectively, $m \times m$ and $n \times n$ invertible matrices. Then

$$P_2P_1AQ_1Q_2 = \begin{bmatrix} a_1 & 0 & 0 & \dots & 0 \\ 0 & a_2 & 0 & \dots & 0 \\ 0 & & & & \\ 0 & & A_2 & & \\ \vdots & & & & \\ 0 & & & & \end{bmatrix}$$

Continuing like this (or by induction on $m+n$), we obtain

$$PAQ = diag\,(a_1, a_2, \dots, a_r, 0, \dots, 0)$$

Finally, we show that we can reduce PAQ further such that $a_1|a_2| \dots |a_r$.

Assume a_1 does not divide a_2.

Add the second row to the first row.

The first row then becomes

$$(a_1 \quad a_2 \quad \cdots \quad a_r \quad 0 \quad \dots \quad 0)$$

By performing these operations, we can reduce the length of a_1.

Thus, by further reduction, we may assume $a_1|a_2$, and, similarly, $a_1|a_i$, $i = 3, 4, \dots, r$.

By repeating this procedure for a_2 in place of a_1, and so on,

we finally reach a situation where $a_i | a_{i+1}$, $i = 1, \ldots, r-1$.

Definition 9.1.9: The non-zero diagonal elements of the matrix having the diagonal form given in theorem are called the invariant factors of A.

That is, the non-zero $a_1, a_2, \ldots, a_r$ found such that $a_1 | a_2 | \ldots | a_r$ are invariant factors of A.

The invariant factors are unique up to unit multipliers.

Result 9.1.10: Two $m \times n$ matrices are equivalent if and only if they have the same invariant factors.

Let two matrices of order $m \times n$ are equivalent.

Let invariant factors of A are $a_1, a_2, \ldots, a_r$.

Then A is equivalent to the matrix A', where A' is given by

$$A' = \begin{bmatrix} a_1 & & & & & & & \\ & a_2 & & & & & & \\ & & \ddots & & & & & \\ & & & a_r & & & & \\ & & & & 0 & & & \\ & & & & & 0 & & \\ & & & & & & \ddots & \\ & & & & & & & 0 \end{bmatrix}$$

Since relation of equivalence matrices is an equivalence relation, therefore, B is equivalent to A'. Further by uniqueness of invariant factors, we get that B has same invariant factors as that of A.

Conversely, let B and A have same invariant factors $a_1, a_2, \ldots, a_r$.

Then B and A both are equivalent to A'.

Since relation of equivalence matrices is an equivalence relation,

therefore, B is equivalent to A.

Example 9.1.11:

Obtain the Smith normal form and rank for the matrix with integral entries

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 0 \end{bmatrix}$$

Solution: Let $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 0 \end{bmatrix}$

$R_2 \to R_2 - 4R_1$

$\sim \begin{bmatrix} 1 & 2 & 3 \\ 0 & -3 & -12 \end{bmatrix}$

$C_2 \to C_2 - 2C_1, C_3 \to C_3 - 3C_1$

$\sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & -3 & -12 \end{bmatrix}$

$C_3 \to C_3 - 4C_2$

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

$R_2 \to (-1)R_2$

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

Invariant factors are 1 and 3. Hence, rank $A = 2$.

Example 9.1.12:

Obtain the Smith normal form and rank for the matrix with integral entries

$$\begin{bmatrix} 0 & 2 & -1 \\ -3 & 8 & 3 \\ 2 & -4 & -1 \end{bmatrix}$$

over the ring of integers. Also find the rank.

Solution:

$$A = \begin{bmatrix} 0 & 2 & -1 \\ -3 & 8 & 3 \\ 2 & -4 & -1 \end{bmatrix}$$

$C_1 \leftrightarrow C_3$

$$\sim \begin{bmatrix} -1 & 2 & 0 \\ 3 & 8 & -3 \\ -1 & -4 & 2 \end{bmatrix}$$

$C_1 \to (-1)C_1$

$$\sim \begin{bmatrix} 1 & 2 & 0 \\ -3 & 8 & -3 \\ 1 & -4 & 2 \end{bmatrix}$$

$C_2 \to C_2 - 2C_1$

$$\sim \begin{bmatrix} 1 & 0 & 0 \\ -3 & 14 & -3 \\ 1 & -6 & 2 \end{bmatrix}$$

$R_2 \to R_2 + 3R_1$

$$\sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 14 & -3 \\ 1 & -6 & 2 \end{bmatrix}$$

$R_3 \to R_3 - R_1$

$$\sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 14 & -3 \\ 0 & -6 & 2 \end{bmatrix}$$

$C_2 \leftrightarrow C_3$

$$\sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & -3 & 14 \\ 0 & 2 & -6 \end{bmatrix}$$

Now since we are in the ring of integers, so we need to apply non-elementary operations.

We need to post-multiply it with a matrix $\begin{bmatrix} 1 & 0 & 0 \\ 0 & u & t \\ 0 & v & -s \end{bmatrix}$.

Now $GCD\,(-3, 14) = 1$

$-3u + 14v = 1; u = 9, v = 2$

Also, $-3 = -3(1),\ 14 = 14(1)$

That is, $s = -3, t = 14$

So, we post-multiply it by the matrix $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 9 & 14 \\ 0 & 2 & 3 \end{bmatrix}$

Then $\begin{bmatrix} 1 & 0 & 0 \\ 0 & -3 & 14 \\ 0 & 2 & -6 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & -3 & 14 \\ 0 & 2 & -6 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 9 & 14 \\ 0 & 2 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 6 & 10 \end{bmatrix}$

$R_3 \to R_3 - 6R_2$

$$\sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 10 \end{bmatrix}$$

So, rank $A = 3$.

9.2 Row Module, Column Module and Rank

Lemma 9.2.1: Let R be a principal ideal domain and let F be a free R −module with a basis consisting of n elements. Then any submodule K of F is also free with a basis consisting of m elements, such that $m \leq n$.

Proof:

Since F is a free R −module with a basis consisting of n elements, therefore, $F \cong R^n$ as R-modules.

To prove the theorem, we use induction on n.

R° is interpreted as a {0} module, and this is free on the empty set. Therefore, we may assume that $n > 0$, and let us identify the copy of K in R^n (under the isomorphism $F \cong R^n$) with K itself. Let $\pi: K \to R$ be the mapping defined by

$$\pi(x_1, x_2, \ldots, x_n) = x_1$$

If $\pi = 0$, then $K = Ker\ \pi \subset R^{n-1}$, and the theorem follows by induction on n.

If $\pi \neq 0$, its image is a non-zero ideal Ra in R;

that is, $\pi(K) = Ra$, $a \neq 0$.

Choose $k \in K$ such that $\pi(k) = a$.

We assert

$$K = Rk \oplus Ker\ \pi$$

For, let $x \in K$,

Write $\pi(x) = ba$, $b \in R$.

Then $\pi(x - bk) = \pi(x) - b\pi(k) = ba - ba = 0$

Hence,

$$x = bk + (x - bk)$$

implies that $x \in Rk + \ker \pi$.

Thus, $K = Rk + Ker\ \pi$.

To prove that the sum is direct, let

$$ck \in Rk \cap Ker\ \pi,\ c \in R.$$

Then $0 = \pi(ck) = ca$

Since $a \neq 0$, therefore, we have $c = 0$.

This proves our assertion that $K = Rk \oplus Ker\ \pi$.

It is easy to check that the mapping $r \to rk$ of R onto Rk is an R −isomorphism.

Further, $Ker\ \pi = \{(0, x_2, \ldots, x_n) | x_i \in R\}$.

Thus, $Ker\ \pi$ is embedded in R^{n-1}.

Hence, by induction, $Ker\ \pi$ is free, with a basis consisting of at most $n - 1$ generators. Therefore,

$$K = Rk \oplus Ker\ \pi$$

$$\cong R \oplus R^m,\ m \leq n - 1$$

So, $K \cong R^{m+1}$, $m + 1 \leq n$

Notations: Let A be an $m \times n$ matrix over R. The rows (columns) of A are the elements of the R −module $R^{1\times n}$ ($R^{m\times 1}$) consisting of the $1 \times n$ ($m \times 1$) matrices over R.

Generally, we write $R^{1\times n}$ (and $R^{m\times 1}$) as R^n (and R^m).

Using the notation R^n to denote rows as well as columns never creates any confusion because context always makes the meaning clear.

Definition 9.2.2: Let A be an $m \times n$ matrix over R. The submodule of R^n generated by the m rows of A is called the row module of A: and the submodule of R^m generated by the n columns of A is called the column module of A.

$R(A)$ and $C(A)$, respectively, denote the row module and the column module of the matrix A. If the ring R is a field, $R(A)$ and $C(A)$ are, respectively, called the row space and column space of matrix A.

Note:
$R(A)$ and $C(A)$ are finitely generated submodules of free modules R^n and R^n respectively. Thus, by Lemma, both $R(A)$ and $C(A)$ are free modules. Let A be an $m \times n$ matrix over R. The rank of the module $R(A)[C(A)]$ is called the row rank (column rank), of A.

Theorem 9.2.3:Let A be an $m \times n$ matrix over R. Let P and Q, respectively, be $m \times m$ and $n \times n$ invertible matrices over R. Then

row (column) rank (PAQ) = row (column) rank (A).

Since P and Q are invertible matrices, therefore, PAQ is equivalent to A. Hence, both PAQ and A have same invariant factors.

This proves that row (column) rank (PAQ) = row (column) rank (A).

Theorem 9.2.4: Let A be an $m \times n$ matrix over a PID R. Then

row rank A = column rank A.

Proof:

Choose P and Q invertible matrices of suitable sizes such that PAQ is in Smith normal form. Then

row rank A = row rank $PAQ = r$

Also, column rank PAQ = column rank A.

But being a diagonal matrix row rank of PAQ =column rank of PAQ

which proves thatrow rank A = column rank A.

The common value of row rank and column rank of a matrix A over a PID R is known as rank.

9.3 Fundamental Theorem for Finitely Generated Modules over a Principal Ideal Domain

Theorem 9.3.1 (Structure Theorem): Let R be a principal ideal domain and let M be any finitely generated R −module. Then

$$M \cong R^s \oplus \frac{R}{Ra_1} \oplus \frac{R}{Ra_2} \oplus \dots \oplus \frac{R}{Ra_r}$$

a direct sum of cyclic modules, where the a_i are non-zero non-units and $a_i | a_{i+1}$, $i = 1, \dots, r-1$

Proof:

Because M is a finitely generated R −module, so, it is isomorphic to a homomorphic image of a free module. That is,$M \cong R^n/K$.

Again, let M is generated by m elements, so,$M \cong R^m; m \leq n$

Let ϕ be this isomorphism from R^m to K.

Thus,

$$K = \phi(R^m)$$

Let $\{e_1, e_2, \dots, e_m\}$ be a basis of R^m.

For $1 \leq i \leq m$,

$$\phi(e_i) \in K \subset R^n$$

$$\phi(e_1) = \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ \vdots \\ a_{n1} \end{bmatrix} \in R^n$$

$$\phi(e_2) = \begin{bmatrix} a_{12} \\ a_{22} \\ \vdots \\ \vdots \\ a_{n2} \end{bmatrix} \in R^n$$

$$\vdots$$

$$\vdots$$

$$\phi(e_m) = \begin{bmatrix} a_{1m} \\ a_{2m} \\ \vdots \\ \vdots \\ a_{nm} \end{bmatrix} \in R^n$$

Then $\phi(R^m) = AR^m$, where $A = [a_{ij}]$ is an $n \times m$ matrix.

Choose invertible matrices P and Q of order $n \times n$ and $m \times m$, respectively, such that

$$PAQ = diag(a_1, a_2, \ldots, a_k, 0, 0, \ldots, 0),$$

where $a_1|a_2| \ldots |a_k$. Then

$$M \cong \frac{R^n}{K} \cong \frac{R^n}{\phi(R^m)} = \frac{R^n}{AR^m} \cong \frac{PR^n}{PAQR^m}$$

$$M \cong \frac{PR^n}{PAQR^m} = \frac{R^n}{\begin{bmatrix} a_1 & & & & & & & \\ & a_2 & & & & & & \\ & & \ddots & & & & & \\ & & & a_k & & & & \\ & & & & 0 & & & \\ & & & & & 0 & & \\ & & & & & & \ddots & \\ & & & & & & & 0 \end{bmatrix} \begin{bmatrix} R \\ R \\ \vdots \\ \vdots \\ R \\ R \end{bmatrix}}$$

$$= \frac{R \oplus R \oplus \ldots \oplus R}{Ra_1 \oplus Ra_2 \oplus \ldots \oplus Ra_k}$$

$$M \cong \frac{R \oplus R \oplus \ldots \oplus R}{Ra_1 \oplus Ra_2 \oplus \ldots \oplus Ra_k}$$

$$\cong \frac{R}{Ra_1} \oplus \frac{R}{Ra_2} \oplus \ldots \oplus \frac{R}{Ra_k} \oplus \overbrace{R \oplus \cdots \oplus R}^{n-k\ copies}$$

By deleting the zero terms if any, corresponding to those $a_i's$ that are units.

$$M \cong \frac{R}{Ra_u} \oplus \ldots \oplus \frac{R}{Ra_k} \oplus R^s$$

By re-numbering, if necessary, we get

$$M \cong \frac{R}{Ra_1} \oplus \ldots \oplus \frac{R}{Ra_r} \oplus R^s$$

Because for any ideal I, including {0}, R/I is a cyclic $R-$module.

Therefore, M is a direct sum of cyclic modules, where the a_i are non-zero non-units and $a_i|a_{i+1}$, $i = 1, \ldots, r-1$

Definition 9.3.2: An element x of an $R-$module M is called a torsion element if there exists a non-zero element $r \in R$ such that $rx = 0$. A non-zero element x of an $R-$module M is called a torsion-free element if $rx = 0$, $r \in R$, implies $r = 0$.

Theorem 9.3.3: Let R be a principal ideal domain and let M be an $R-$module. Then

$Tor\ M = \{x \in M | x \text{ is torsion}\}$ is a submodule of M.

Proof:

Consider $0 \in M$

Then $r0 = 0 \; \forall \; r \in R$

Therefore, $0 \in Tor\ M$

So, $Tor\ M \neq \phi$

Consider $a, \; b \in Tor\ M, \; r \in R$

This implies, there exist non-zero elements $r_1, \; r_2 \in R$, such that $r_1 a = 0, \; r_2 b = 0$

Consider $r_1 r_2 (a - b) = r_1 r_2 a - r_1 r_2 b$

$$= 0 - 0 = 0$$

This implies, $a - b \in Tor\ M$

Again,

$$r_1(ra) = r(r_1 a) = 0$$

So, $ra \in Tor\ M$

This implies,

$$a - b, \; ra \in Tor\ M \; \forall \; a, \; b \in Tor\ M, \; r \in R$$

Hence, $Tor\ M$ is a submodule of R −module M.

Definition 9.3.4: A module is said to be torsion module if every element is a torsion element. A module having no-nonzero torsion element is called a torsion free module. The set of all torsion elements of a module M (over a commutative ring) form a submodule, called torsion part of M, it is denoted as M_t.

Remark 9.3.5: Every non-zero element of M is linearly independent if and only if M is torsion free module.

Proof:

Let every non-zero element of M is linearly independent.

This implies, $\forall \; 0 \neq x \in M$ and $r \in R$,

If $rx = 0$ then $r = 0$

Therefore, x is torsion free element.

Conversely,

Let M is torsion free module.

Let x be a non-zero element of M.

Since M is torsion free module,

therefore, x is torsion free element.

This implies $rx = 0$ if and only if $r = 0$

So, x is linearly independent.

Remarks 9.3.6:

1. M_t is the largest torsion submodule of M.
2. M is torsion free if and only if $M_t = \{0\}$

Proof: Let N be any torsion submodule of M.

This implies all the elements of N are torsion elements.

If $x \in N$, then x is torsion element.

Since M_t is the set of all torsion elements.

$$\Rightarrow x \in M_t \Rightarrow N \subset M_t$$

Therefore, every torsion submodule of M is contained in M_t. Hence, M_t is the largest torsion submodule of M.

Next, let M is torsion free.

$\Leftrightarrow$ 0 is the only torsion element of M.

$$\Leftrightarrow M_t = \{0\}$$

Theorem 9.3.7: For any module M over a commutative integral domain, the quotient M/M_t is torsion free.

Proof: To prove that M/M_t is torsion free,

we will prove that if $\bar{x}$ is torsion element of M/M_t then $\bar{x} = \bar{0}$, that is, $\bar{x} = M_t$.

Let $\bar{x} = x + M_t, x \in M$ be a torsion element of M/M_t.

$\Rightarrow r\bar{x} = \bar{0}$ for some $0 \neq r \in R$

$\Rightarrow r(x + M_t) = M_t$

$\Rightarrow rx + M_t = M_t$

$\Rightarrow rx \in M_t$

$\Rightarrow$there exists $r_1 \neq 0, r_1 \in R$ such that

$r_1(rx) = 0$

$\Rightarrow (r_1 r)x = 0$

Since r, r_1 are both non-zero elements of an integral domain R and integral domains are without proper zero divisors, therefore, $r_1 r \neq 0$

$\Rightarrow bx = 0$ where $b = r_1 r \neq 0$

$\Rightarrow x$ is torsion element of M.

$\Rightarrow x \in M_t$

$\Rightarrow x + M_t = M_t$

So, $\bar{x} = \bar{0}$

Therefore, M/M_t has no non-zero torsion element and hence it is torsion free.

Example 9.3.8:

Every torsion free module need not be free

Proof: We have already proved that $Z-$module Q is not free.

Let $R - Z$, $M = (Q, +)$

Since $\forall\, 0 \neq r \in R$ and $x \in Q$

$rx = 0$ only if $x = 0$

$\Rightarrow M_t = \{0\}$ and hence M is torsion free.

Theorem 9.3.9:A finitely generated torsion free module over a PID is free.

Proof: Let M be a finitely generated torsion free module.

Let $M =< X >$ where $X = \{x_1, x_2, \ldots, x_n\}$

$M \neq \{0\}$ implies at least one of the $x_i's \neq 0$

If X is linearly dependent, we can choose a subset of X which is linearly independent, and it is possible since M is torsion free module.

Let $B = \{x_1, x_2, \ldots, x_m\}$ be the maximal linearly independent subset.

Let linear span of $B = F$

Since M is non-zero and B generates M.

M contains at least one non-zero element implies

That $B \neq \phi$ and $m \geq 1$

Also, M is torsion free.

Consider $1 \leq i \leq n$, then if some x_i is not in the submodule generated by B.

Then $B \cup \{x_i\}$ is linearly independent subset of X, which contradicts to the maximality of B.

So, it is not possible that is, $\forall\ 1 \leq i \leq n,\ x_i$ is in the submodule generated by B.

Choose $x_i \notin B,\ x_i$ is in the submodule generated by B implies $B \cup \{x_i\}$ is linearly dependent.

Therefore, there exist scalars, a_i, a_{ij} (not all zero)

such that

$$a_i x_i + \sum_{j=1}^{m} a_{ij} x_j = 0 \ldots (1)$$

If $a_i = 0$

Then (1) becomes,

$$\sum_{j=1}^{m} a_{ij} x_j = 0$$

Note that on the left side, we have a linear combination of elements of linearly independent set B.

Hence $a_{ij} = 0\ \forall\ j$

But a_i, a_{ij} are not all zero.

So, our supposition was wrong.

That is, $a_i \neq 0\ \forall\ 1 \leq i \leq n$

Let $a = a_1 a_2 \ldots a_n$

Since M is torsion free so, $a \neq 0$

From (1)

$$a_i x_i = -\sum_{j=1}^{m} a_{ij} x_j$$

is a linear combination of elements of B

Hence, $a_i x_i \in F\ \forall\ i$

Consider

$$\begin{aligned} a x_i &= a_1 a_2 \ldots a_n x_i \\ &= (a_1 a_2 \ldots a_{i-1} a_{i+1} \ldots a_n) a_i x_i \\ &\in F \\ a x_i &\in F\ \forall\ i \end{aligned}$$

Let $x \in M$

M is generated by X. So, there exist $\alpha_i \in R$ such that

$$x = \sum_{i=1}^{n} \alpha_i x_i\ ; \alpha_i \in R$$

So,

$$ax = a\left(\sum_{i=1}^{n} \alpha_i x_i\right)$$

$$= \sum_{i=1}^{n} a(\alpha_i x_i) = \sum_{i=1}^{n} \alpha_i (a x_i) \in F$$

Hence,

$$aM \subset F$$

Consider the map $f: M \to F$ as $f(x) = ax$ then

f is R −homomorphism

Let $x, y \in M, r \in R$

$$f(x+y) = a(x+y) = ax + ay = f(x) + f(y)$$

and

$$f(rx) = a(rx) = r(ax) = rf(x)$$

f is one-one

Let $x \in Ker\ f$

$$\Rightarrow f(x) = 0$$

$$\Rightarrow ax = 0$$

Since $a \neq 0$, x is torsion element

But M is torsion free implies $x = 0$

So, $Ker\ f = \{0\}$

Hence $M \cong f(M)$

$f(M)$ being submodule of free module F is a free module.

Being isomorphic to a free module, M is a free module.

Task:

1. List all the torsion elements of the ring of integers considering it as a module over itself.
2. List all the torsion elements of the ring Z_4 considering it as a Z −module.
3. List all the torsion elements of the ring Z_5 considering it as a Z −module.

Theorem 9.3.10: Let M be a finitely generated module over a principal ideal domain R. Then

$$M = F \oplus Tor\ M$$

where,

(i) $F \cong R^s$ for some non-negative integer s, and

(ii) $Tor\ M \cong \frac{R}{Ra_1} \oplus \dots \oplus \frac{R}{Ra_r}$, where a_i are non-zero non-unit elements in R such that $a_1 | a_2 | \dots | a_r$

Proof:

By the structure theorem for finitely generated modules over a PID,

$$M \cong R^s \oplus \frac{R}{Ra_1} \oplus \frac{R}{Ra_2} \oplus \dots \oplus \frac{R}{Ra_r}$$

a direct sum of cyclic modules, where the a_i are non-zero non-units and $a_i | a_{i+1}$, $i = 1, \dots, r-1$

It then follows that

$$M = F \oplus T$$

where $F \cong R^s$ and

$$T \cong \frac{R}{Ra_1} \oplus \frac{R}{Ra_2} \oplus \dots \oplus \frac{R}{Ra_r} \quad \dots (1)$$

Claim: $a_r T = 0$

Let $x \in T$

Let ϕ be the isomorphism between T and

$$\frac{R}{Ra_1} \oplus \frac{R}{Ra_2} \oplus \dots \oplus \frac{R}{Ra_r}$$

Then

$$\phi(x) \in \frac{R}{Ra_1} \oplus \frac{R}{Ra_2} \oplus \dots \oplus \frac{R}{Ra_r}$$

That is,

$$\phi(x) = \sum_{i=1}^{r} \overline{x_i}\, ; \overline{x_i} \in \frac{R}{Ra_i}\ \forall\, 1 \le i \le r$$

Now

$$\overline{x_i} \in \frac{R}{Ra_i}$$

Implies,

$$\overline{x_i} = x_i + Ra_i,\ x_i \in R \dots (2)$$

Also,

$$a_i | a_r\ \forall\, 1 \le i \le r$$

This implies

$$a_r = a_i r_i ; r_i \in R \dots (3)$$

From (2)

$$\overline{x_i} = x_i + Ra_i,$$
$$a_r \overline{x_i} = a_r(x_i + Ra_i),$$
$$= a_i r_i (x_i + Ra_i) [\text{From } (3)]$$

As, R is commutative

$$a_r(x_i + Ra_i) = r_i a_i (x_i + Ra_i)$$

Now,

$$r_i a_i \in Ra_i$$
$$r_i a_i x_i \in Ra_i$$

Therefore,

$$r_i a_i x_i + Ra_i = Ra_i$$

This implies,

$$a_r(x_i + Ra_i) = Ra_i$$
$$a_r \overline{x_i} = \overline{0} \dots (4)$$
$$a_r \phi(x) = a_r \overline{x_1} + a_r \overline{x_2} + \dots + a_r \overline{x_r}$$
$$= \overline{0} + \overline{0} + \dots + \overline{0} = \overline{0}$$

Since ϕ is R −isomorphism

So, $\phi(a_r x) = \overline{0}$ implies $a_r x = 0$

Since $a_r \neq 0$, $x \in Tor\ M$

So, $\phi(a_r x) = \overline{0}$ implies $a_r x = 0$

This implies, $x \in Tor\ M$

So, $T \subset Tor\ M \dots (5)$

Next let $x \in Tor\ M \subset M \simeq F \oplus T$

$$x = x_1 + x_2,\ x_1 \in F,\ x_2 \in T$$

Because $x \in Tor\ M$, $x_2 \in T \subset Tor\ M$

Consider

$$x_1 = x - x_2 \in Tor\ M$$

This implies, there exists non-zero $r \in R$ such that

$$rx_1 = 0$$

Since $F \cong R^s$

Therefore, there exists $\psi: F \to R^s$ such that ψ is R −isomorphism.

$$x_1 \in F$$

so,

$$\psi(x_1) \in R^s$$

Let

$$\psi(x_1) = (y_1, y_2, \dots, y_s)$$

Since $rx_1 = 0$

$$\Rightarrow \psi(rx_1) = \psi(0) = 0$$

$$\Rightarrow (ry_1, ry_2, \dots, ry_s) = 0$$

$$\Rightarrow ry_i = 0\ \forall\ 1 \le i \le s$$

Since $r \neq 0$

$r, y_i \in R$ and R is an integral domain, hence without zero divisors

$$\Rightarrow y_i = 0\ \forall\ 1 \le i \le s$$

$$\Rightarrow \psi(x_1) = 0$$

But ψ is one-one implies, $x_1 = 0$

Then $x = x_1 + x_2 = x_2 \in T$

Therefore, $x \in T$

$$\Rightarrow Tor\ M \subset T \dots (6)$$

From (5) and (6), we get

$$T = Tor\ M$$

Theorem 9.3.11: Let R be a principal ideal domain and let M be a finitely generated R −module. Suppose

$$M \cong R^s \oplus \frac{R}{Ra_1} \oplus \frac{R}{Ra_2} \oplus \dots \oplus \frac{R}{Ra_u} \dots (1)$$

where a_i are non-zero non-unit elements in R such that $a_1|a_2| \dots |a_u$

$$M \cong R^t \oplus \frac{R}{Rb_1} \oplus \frac{R}{Rb_2} \oplus \dots \oplus \frac{R}{Rb_v} \dots (2),$$

where b_i are non-zero non-unit elements in R such that $b_1|b_2| \dots |b_v$, and

Then $s = t,\ u = v,\ Ra_i = Rb_i,\ 1 \le i \le u$

Proof:

From the Structure theorem, we have,

$M = F \oplus Tor\ M$ and $M = F' \oplus Tor\ M$

where $F \cong R^s$, $F' \cong R^t$

$$T = Tor\ M \cong \frac{R}{Ra_1} \oplus \frac{R}{Ra_2} \oplus \dots \oplus \frac{R}{Ra_u}$$

and

$$T = Tor\ M \cong \frac{R}{Rb_1} \oplus \frac{R}{Rb_2} \oplus \ldots \oplus \frac{R}{Rb_v}$$

First, we prove that $s = t$

$$F \cong R^s,\ F' \cong R^t$$

$$\frac{M}{Tor\ M} = \frac{F \oplus Tor\ M}{Tor\ M}$$

$$\cong \frac{F}{F \cap Tor\ M} = F$$

Also,

$$\frac{M}{Tor\ M} = \frac{F' \oplus Tor\ M}{Tor\ M}$$

$$\cong \frac{F'}{F' \cap Tor\ M} = F'$$

This implies,

$$F \cong F'$$

But $F \cong R^s$, $F' \cong R^t$

$$\Rightarrow R^s \cong R^t \Rightarrow s = t$$

Next, we prove that $u = v$ and $Ra_i = Rb_i\ \forall\ 1 \le i \le u$

If X is any R –module, p is any prime number

Define $X_p = \{x \in X |\ px = 0\}$

Clearly, $p \neq 0$ and $\forall\ x \in X_p$, $px = 0$

Since $px = 0$, $p \neq 0$

$$\Rightarrow x \in Tor\ M$$

Therefore, $X_p\ \subset Tor\ M\ \forall\ R$ –module X.

For $X = T$,

$$T_p = \{x \in T | px = 0\}$$

Since

$$T \cong \oplus \sum_{i=1}^{u} R/R\,a_i$$

Therefore,

$$T_p \cong \oplus\ \sum_{i=1}^{u} \left(\frac{R}{Ra_i}\right)_p \ldots (3)$$

Claim 1:

$$\left(\frac{R}{Ra_i}\right)_p = \begin{cases} \dfrac{R\left(\frac{a_i}{p}\right)}{Ra_i} & if\ p|a_i \\ 0 & otherwise \end{cases}$$

If $p|a_i$

$a_i = pr_i$ for some $r_i \in R$

$$x + Ra_i \in \left(\frac{R}{Ra_i}\right)_p$$

$\Leftrightarrow\ p(x + Ra_i) = Ra_i \Leftrightarrow px + Ra_i = Ra_i$

$\Leftrightarrow px \in Ra_i \Rightarrow x \in R\left(\dfrac{a_i}{p}\right)$

$\Leftrightarrow x + Ra_i \in \frac{R\left(\frac{a_i}{p}\right)}{Ra_i}$

$\Rightarrow R\left(\frac{a_i}{p}\right)_p = \frac{R\left(\frac{a_i}{p}\right)}{Ra_i}$

If p does not divide a_i

For $\bar{x} \in \left(\frac{R}{Ra_i}\right)_p$

$\Rightarrow p\bar{x} = \bar{0}$

$\Rightarrow p(x + Ra_i) = Ra_i$

$\Rightarrow px \in Ra_i$

$\Rightarrow px = r_i a_i,\ r_i \in R$

If $x \neq 0$, $p|r_i a_i$

Since p does not divide a_i

$\Rightarrow p|r_i\ \forall r_i \in R$

$\Rightarrow R = < p >$ which is not possible.

Therefore, $x = 0$ and

hence

$$\left(\frac{R}{Ra_i}\right)_p = 0$$

So, the claim is established.

$$\left(\frac{R}{Ra_i}\right)_p = \begin{cases} \frac{R\left(\frac{a_i}{p}\right)}{Ra_i} & if\ p|a_i \\ 0 & otherwise \end{cases}$$

R is principal ideal domain. This implies, $< p >$ is maximal ideal of R.

So, $\frac{R}{<p>}$ is a field.

That is $\frac{R}{Rp}$ is a field.

Consider $V = \frac{R\left(\frac{a_i}{p}\right)}{Ra_i}$ as a vector space over the field $F = \frac{R}{Rp}$.

Let $\bar{x} \in V$

$\bar{x} = \bar{\alpha}\left(\left(\frac{a_i}{p}\right) + Ra_i\right)$ where $\bar{\alpha} \in \frac{R}{Rp}$

Since $\bar{x} \in V = \frac{R\left(\frac{a_i}{p}\right)}{Ra_i}$

$\Rightarrow \bar{x} = x + Ra_i$ where $x \in R\left(\frac{a_i}{p}\right)$

That is, $x = \frac{x_i a_i}{p}$ for some $x_i \in R$

$$\Rightarrow \bar{x} = x + Ra_i$$

$$= \frac{x_i a_i}{p} + Ra_i$$

$$= x_i\left(\frac{a_i}{p} + Ra_i\right) \in \ < \frac{a_i}{p} + Ra_i >$$

Then $\frac{R\left(\frac{a_i}{p}\right)}{Ra_i}$ is generated by a single element $\left(\frac{a_i}{p}\right) + Ra_i$.

That is, $\frac{R\left(\frac{a_i}{p}\right)}{Ra_i}$ is one dimensional vector space over $\frac{R}{Rp}$.

From (3), T_p is a vector space over $\frac{R}{R_p}$ with dimension equal to number of terms $\frac{R}{Ra_i}$ such that $p|a_i$.

Suppose $p|a_1$ Since $a_1|a_2| \dots |a_u$

This implies $p|a_i \ \forall\ 1 \le i \le u$

Again,

$$T \cong \frac{R}{Rb_1} \oplus \frac{R}{Rb_2} \oplus \dots \oplus \frac{R}{Rb_v} \dots (4)$$

Since $p|a_i \ \forall\ 1 \le i \le u$

In this case, dim $T_p = u$

Hence from decomposition (4) and the fact that $dim\, T_p = u$, we get,

$$dim\left(\frac{R}{Rb_1} \oplus \frac{R}{Rb_2} \oplus \dots \oplus \frac{R}{Rb_v}\right) = u$$

This implies, $p|b_j$ for at least u number of $b_j's$.

$$\Rightarrow u \le v$$

Similarly, we can show that $v \le u$

This implies, $u = v$

$$\Rightarrow T \cong \frac{R}{Ra_1} \oplus \frac{R}{Ra_2} \oplus \dots \oplus \frac{R}{Ra_u} \dots \ (5)$$

and

$$T \cong \frac{R}{Rb_1} \oplus \frac{R}{Rb_2} \oplus \dots \oplus \frac{R}{Rb_u} \dots (6)$$

First, we prove that $Ra_u = Rb_u$

Since $a_u T = 0$

From (4), $Ra_u \subset Rb_u$

Also, $b_u T = 0$ implies, $Rb_u \subset Ra_u$

Hence, $Ra_u = Rb_u$

Now assume $Ra_i = Rb_i \ \forall\ k \le i \le u$

We show $Ra_{k-1} = Rb_{k-1}$

Let p be a prime element in R such that $p^{\alpha}|a_{k-1}$, $p^{\alpha+1}$does not divide a_{k-1}

Also,$p^{\beta}|b_{k-1}$, $p^{\beta+1}$does not divide b_{k-1}.

If $\alpha = \beta$ for each prime p, $Ra_{k-1} = Rb_{k-1}$

Otherwise, let $\alpha > \beta$

Put $x = \frac{p^{\alpha-1}a_u}{p^{\theta}} \in R$

where $p^{\theta}|a_u$,$p^{\theta+1}$does not divide a_u.

Then

$$xT = x\left(\frac{R}{Ra_1} \oplus \frac{R}{Ra_2} \oplus \dots \oplus \frac{R}{Ra_u}\right)$$
$$= \frac{Rx + Ra_1}{Ra_1} \oplus \frac{Rx + Ra_2}{Ra_2} \oplus \dots \oplus \frac{Rx + Ra_u}{Ra_u} \dots (7)$$

Putting $x = \frac{p^{\alpha-1}a_u}{p^{\theta}}$ and since $p^{\alpha}|a_{k-1}$, $a_{k-1} = p^{\alpha}a'_{k-1}$

We get,

The $(k-1)th$ summand is

$$\frac{Rx + Ra_{k-1}}{Ra_{k-1}} = \frac{\frac{Rp^{\alpha-1}a_u}{p^\theta} + Rp^\alpha a'_{k-1}}{Rp^\alpha a'_{k-1}}$$

$$= \frac{Rd}{Rp^\alpha a'_{k-1}}$$

where $d = \left(\frac{p^{\alpha-1}a_u}{p^\theta}, p^\alpha a'_{k-1}\right)$, the greatest common divisor of $\frac{p^{\alpha-1}a_u}{p^\theta}, p^\alpha a'_{k-1}$.

But

$$a_{k-1} | a_u$$

This implies,

$$a'_{k-1} = \frac{a_{k-1}}{p^\alpha} | \frac{a_u}{p^\theta}$$

$$\Rightarrow GCD\left(\frac{p^{\alpha-1}a_u}{p^\theta}, p^\alpha a'_{k-1}\right) = p^{\alpha-1}a'_{k-1}$$

Therefore, $d = p^{\alpha-1}a'_{k-1}$

Thus, the $(k-1)th$ summand in (7) is

$$\frac{Rp^{\alpha-1}a'_{k-1}}{Rp^\alpha a'_{k-1}} \cong \frac{R}{Rp}$$

Because in any integral domain,

$$\frac{Ra}{Rab} \cong \frac{R}{Rb}, \ 0 \neq a, b \in R$$

Similarly, we can show that any summand preceding the $(k-1)th$ summand is either $\frac{R}{Rp}$ or $\{0\}$.

Also, indeed if any summand is {0} then all the preceding ones are also zero.

Therefore, (7) can be written as,

$$xT \cong \overbrace{\{0\} \oplus \{0\} \oplus \ldots \oplus \{0\}}^{s\ terms} \oplus \overbrace{\frac{R}{Rp} \oplus \ldots \oplus \frac{R}{Rp}}^{t\ terms} \oplus \frac{R}{Rp^{\lambda_k}} \oplus \ldots \oplus \frac{R}{Rp^{\lambda_u}} \quad \ldots (8)$$

where $s, t \geq 0$, $s + t = k - 2$

Again from (6)

$$xT = x\left(\frac{R}{Rb_1} \oplus \frac{R}{Rb_2} \oplus \ldots \oplus \frac{R}{Rb_u}\right)$$

and its $(k-1)th$ summand is

$$\frac{Rx + Rb_{k-1}}{Rb_{k-1}} = \frac{\frac{Rp^{\alpha-1}b_u}{p^\theta} + Rp^\beta b'_{k-1}}{Rp^\beta b'_{k-1}}$$

where $GCD\,(b'_{k-1}, p) = 1$

Because $\alpha > \beta$ and $b_{k-1} | b_u$

Therefore,

$$b'_{k-1} = \frac{\frac{b_{k-1}}{p^\beta}}{\frac{b_u}{p^\theta}}$$

This implies,

$$p^\beta b'_{k-1} | \frac{p^{\alpha-1}b_u}{p^\theta}$$

Hence,

$$\frac{Rx + Rb_{k-1}}{Rb_{k-1}} = \frac{Rp^\beta b'_{k-1}}{Rp^\beta b'_{k-1}} = \{0\}$$

That is, zero of Rx/Rb_{k-1} that is, Rb_{k-1}.

Therefore,

$$Rx \subset Rb_{k-1}$$

Because $Rb_{k-1} \subset Rb_{k-2} \subset \cdots \subset Rb_1$, it follows that the first $k-1$ summands are all zero.

Therefore, the decomposition of xT may be written as

$$xT = \overbrace{\{0\} \oplus \cdots \oplus \{0\}}^{k-1 \text{ terms}} \oplus \frac{R}{Rp^{\lambda_k}} \oplus \ldots \oplus \frac{R}{Rp^{\lambda_u}} \ldots (9)$$

Comparing (8) and (9), we arrive at a contradiction.

Because any two such decompositions of a module over a PID must have equal number of non-zero summands

Therefore,

$$\alpha \le \beta$$

Similarly, we can show that

$$\beta \le \alpha$$

This implies,

$$\alpha = \beta$$

Hence $Ra_{k-1} = Rb_{k-1}$

which implies, $Ra_i = Rb_i \ \forall\ 1 \le i \le u$

Task:

Let V be a vector space. Let W_1 and W_2 are two subspaces of V such that V is a direct sum of W_1 and W_2. Then prove that $dim\ (V) = dim\ W_1 + dim\ W_2$.

9.4 Application of Fundamental Theorem for Finitely Generated to Finitely Generated Abelian Groups

Remark 9.4.1: Because the ring of integers Z is a PID

and any abelian group is a $Z-$module,

an immediate application of the theorem gives an alternative proof of the decomposition theorem for a finitely generated abelian group.

Theorem 9.4.2: Let A be a finitely generated abelian group. Then

$$A \cong Z^s \oplus \frac{Z}{a_1 Z} \oplus \ldots \oplus \frac{Z}{a_r Z}$$

where s is a non-negative integer and a_i are non-zero non-units in Z, such that $a_1 | a_2 | \ldots | a_r$

Further, the decomposition of A subject to the given condition is unique. (Z^0 is interpreted as $\{0\}$.)

If A is generated by $\{x_1, x_2, \ldots, x_n\}$ subject to

$$\sum_{j=1}^{n} a_{ij} x_j = 0\,,\ 1 \le i \le m,$$

Then

$$A \cong Z \times Z \times \ldots \times Z \times \frac{Z}{a_1 Z} \times \ldots \times \frac{Z}{a_r Z},$$

Where $a_1, a_2, \ldots, a_r$ are the invariant factors of $m \times n$ matrix A.

Example 9.4.3:

The abelian group generated by x_1 and x_2 subject to

$$2x_1 = 0$$

and

$$3x_2 = 0$$

Then we prove that this group is isomorphic to Z_6.

Solution: Coefficient matrix is given by $A = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$

Note that A is in diagonal form, but not in Smith normal form as 2 does not divide 3.

$$A = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$$

$$R_1 \to R_1 + R_2$$

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

Pre-multiply by $\begin{bmatrix} u & t \\ v & -s \end{bmatrix}$ where u, v, s, t are given by,

$2u + 3v = 1, 3 = t(1)$ and $2 = s(1)$

So that, $u = -1, v = 1, t = 3, s = 2$

$$A \sim \begin{bmatrix} 2 & 3 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} -1 & 3 \\ 1 & -2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -6 \end{bmatrix}$$

Applying, $R_2 \to (-1)R_2$, we get,

$$A \sim \begin{bmatrix} 1 & 0 \\ 0 & 6 \end{bmatrix}$$

Thus, the required abelian group is isomorphic to Z_6.

Example 9.4.4:

Find the abelian group generated by $\{x_1, x_2, x_3\}$ subject to

$$5x_1 + 9x_2 + 5x_3 = 0$$

$$2x_1 + 4x_2 + 2x_3 = 0$$

$$x_1 + x_2 - 3x_3 = 0$$

Solution: The coefficient matrix is given by

$$A = \begin{bmatrix} 5 & 9 & 5 \\ 2 & 4 & 2 \\ 1 & 1 & -3 \end{bmatrix}$$

$$R_1 \leftrightarrow R_3$$

$$\sim \begin{bmatrix} 1 & 1 & -3 \\ 2 & 4 & 2 \\ 5 & 9 & 5 \end{bmatrix}$$

$$R_2 \to R_2 - 2R_1, R_3 \to R_3 - 5R$$

$$\sim \begin{bmatrix} 1 & 1 & -3 \\ 0 & 2 & 8 \\ 0 & 4 & 20 \end{bmatrix}$$

$$C_2 \to C_2 - C_1, C_3 \to C_3 + 3C_1$$

$$\sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 8 \\ 0 & 4 & 20 \end{bmatrix}$$

$$R_3 \to R_3 - 2R_2$$

$$\sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 8 \\ 0 & 0 & 4 \end{bmatrix}$$

$$C_3 \to C_3 - 4C_2$$

$$\sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{bmatrix}$$

Since 1|2|4 so, it is the smith normal form.

Hence, the required group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$.

Example 9.4.5: Compute the invariants and find the structures of the abelian groups with generators x_1, x_2, x_3 subject to the following relations

$$3x_1 - 2x_2 = 0$$

$$x_1 + x_3 = 0$$

$$-x_1 + 3x_2 + 2x_3 = 0$$

Solution: The coefficient matrix is given by

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

$$R_1 \leftrightarrow R_2$$

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

$$R_2 \to R_2 - 3R_1, R_3 \to R_3 + R_1$$

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

$$R_2 \leftrightarrow R_3$$

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

Pre-multiply with the matrix $\begin{bmatrix} 1 & 0 & 0 \\ 0 & u & v \\ 0 & t & -s \end{bmatrix}$

$$3u - 2v = 1, u = 1, v = 1, t = 2, s = -3$$

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

Hence, the required group is isomorphic to $\mathbb{Z}_3$.

Example 9.4.6:

Compute the invariants and find the structures of the abelian groups with generators x_1, x_2 subject to the following relations

$$x_1 + x_2 = 0$$

Solution: The coefficient matrix is

$$A = [1 \quad 1]$$

$$C_2 \to C_2 - C_1$$

$$A \sim [1 \quad 0]$$

So, the group is isomorphic to $\mathbb{Z}$.

Summary

- Smith Normal Form of an $m \times n$ matrix over a PID R is explained with the help of examples.
- Row module, column module and rank of a matrix are defined.
- A finitely generated module over a PID is expressed as a direct sum of R −modules.
- Torsion module is defined and results about torsion modules are proved.
- Important result on Fundamental theorem (Structure theorem) of finitely generated module over a PID are discussed.
- The applications of Structure theoremare explained with the help of examples.

Keywords

- Smith Normal Form over a PID
- Row module
- Column module
- Rank of a matrix over a PID
- Structure Theorem
- Torsion elements

Self Assessment

1. Let e_{22} be a matrix of order 4. Then e_{22} is

A. a scalar matrix
B. a diagonal matrix
C. zero matrix
D. non-singular matrix

2. The operator $E_{ij}A$ applied on a matrix A

A. interchanges $i-th$ and $j-th$ rows
B. interchanges $i-th$ and $j-th$ columns
C. add $i-th$ and $j-th$ row
D. add $i-th$ and $j-th$ column

3. The matrix $e_{ij}e_{kl}$ =

A. Identity matrix
B. Identity matrix if $i = l$
C. The matrix e_{il} if $j \neq k$
D. The matrix e_{il} if $j = k$

4. In the ring of integers, length of 120 is

A. 5
B. 4
C. 3
D. 2

5. Rank of the matrix $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 0 \end{bmatrix}$ is

A. 0
B. 1
C. 2
D. 3

6. Length of a unit in a Principal Integral Domain is

A. 0
B. 1
C. Infinite
D. Not defined

7. Let R be a principal ideal domain and let F be a free R −module with a basis consisting of n elements. Let K be an R −submodule of F. Then
A. K may or may not be free
B. K is always free and rank $K < n$
C. K is always free and rank $K > n$
D. K is always free and rank $K \leq n$

8. Consider the map $\pi: F^3 \to F$ as $\pi(x, y, z) = y$ then $Ker\pi$ is
A. a subspace of F^3 of dimension 3
B. a subspace of F^3 of dimension 2
C. a subspace of F^3 of dimension 1
D. not a subspace of F^3

9. Let A be an $m \times n$ matrix over a PID R. Let row rank $A = k$ and column rank $A = l$. Then
A. $k < l < \min\{m, n\}$
B. $k > l > \min\{m, n\}$
C. $k = l = \min\{m, n\}$
D. $k = l \leq \min\{m, n\}$

10. An element x of an R- module M is torsion element then
A. There exists a unique element $r \in R$ such that $rx = 0$
B. There exists a non-zero element $r \in R$ such that $rx = 0$
C. $rx \neq 0$ for all $r \in R$
D. $rx = 0$ for all $r \in R$

11. Let $M = Z_6$ be the additive group of integers under addition modulo 6. Consider M as Z-module. Then the set of torsion element(s) of M is given by
A. $\{2\}$
B. $\{3\}$
C. $\{2, 3\}$
D. Z_6

12. M is torsion free R module. Then torsion part of M denoted by Tor M is
A. Equal to M
B. Equal to {0} where 0 is additive identity of module M
C. Equal to R
D. Equal to {0} where 0 is the additive identity of ring R

13. True/False Let M be a finitely generated module over a principal ideal domain R such that $M = F \oplus Tor\ M$. Then F is a free module over R.
A. True
B. False

14. The non-zero, non-unit elements obtained in the structure theorem are called
A. Units
B. Unity
C. Invariant Factors
D. Multipliers

15. Invariant factors of the matrix $\begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$ over the ring of integers Z are

A. 2 and 3
B. 1 and 6
C. 1 and 3
D. 1and 4

Answers for Self Assessment

1. B	2. A	3. D	4. A	5. C
6. A	7. D	8. B	9. D	10. B
11. D	12. B	13. A	14. C	15. B

Review Questions

1. Find the invariant factors of the following matrix over $Q[x]$:
$$\begin{bmatrix} 5-x & 1 & -2 & 4 \\ 0 & 5-x & 2 & 2 \\ 0 & 0 & 5-x & 3 \\ 0 & 0 & 0 & 4 \end{bmatrix}$$
2. Find the rank of the subgroup of Z^4 generated by the elements $\{(3,6,9,0),(-4,-8,-12,0)\}$.
3. Find the rank of the subgroup of Z^4 generated by the elements $\{(2,3,1,4),(1,2,3,0),(1,1,1,4)\}$
4. Compute the invariants and write down the structures of the abelian groups with generators x_1, x_2, x_3 subject to the following relations:
$$3x_1 - 2x_2 = 0, x_1 + x_3 = 0, -x_1 + 3x_2 + 2x_3 = 0$$
5. Compute the invariants and write down the structures of the abelian groups with generators x_1, x_2, x_3 subject to the following relations:
$$2x_2 - x_3 = 0, -3x_1 + 8x_2 + 3x_3 = 0, 2x_1 - 4x_2 - x_3 = 0$$

Further Readings

- Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress
- Topics in algebra by I.N. Hartstein, Wiley
- Abstract algebra by David S Dummit and Richard M Foote, Wiley

Weblinks

- https://nptel.ac.in/courses/111/102/111102009/
- https://nptel.ac.in/courses/111/105/111105112/#

Dr. Isha Garg, Lovely Professional University

Unit 10: Characteristic Values and Diagonal Canonical Form

CONTENTS

Objective

After studying this unit, you will be able to

- define characteristic value and characteristic vector of a linear operator on a finite-dimensional vector space V over F,
- define annihilating polynomial of a linear operator T on a finite-dimensional vector space V over a field F,
- prove that the set of annihilating polynomials is an ideal of $F[x]$,
- show the existence and uniqueness of minimal polynomial,
- state and prove the Cayley Hamilton Theorem,
- understand how to find minimal and annihilating polynomials of a linear operator,
- define diagonalizable operator on a finite-dimensional vector space,
- Corresponding to a diagonalizable operator T, find the basis B of underlying space such that $[T]_B$ is a diagonal matrix.

Introduction

In this unit, you will be introduced to characteristic values and characteristic vectors of a linear operator on a finite-dimensional vector space V over F. Annihilating polynomials will be defined. It will be proved that the set of annihilating polynomials is an ideal of $F[x]$. Further, the relation between annihilating, minimal and characteristic polynomial will be explained with the help of examples. Diagonal canonical forms are defined, and the operators are classified in terms of diagonalizable or not.

10.1 Characteristic Values

Definition 10.1.1: Let V be a vector space over the field F and let T be a linear operator on V.A characteristic value of T is a scalar c in F such thatthere is a non-zero vector $\alpha \in V$ with $T\alpha = c\alpha$.

If c is a characteristic value of T, then we can observe the following points:

(a) any non-zero vector α such that $T\alpha = c\alpha$ is called a characteristic vector of T associated with the characteristic value c;

(b) the collection of all α such that $T\alpha = c\alpha$ is called the characteristic space associated with c.

Characteristic values are often called characteristic roots, latent roots, eigenvalues, proper values, or spectral values.

We shall use only the name 'characteristic values.'

Theorem 10.1.2: If T is any linear operator and c is any scalar, the set of vectors α such that $T\alpha = c\alpha$ is a subspace of V.

Proof: Let $S = \{\alpha | T\alpha = c\alpha\}$

Since $T(0) = 0 = c0$, $0 \in S$

Hence, $S \neq \phi$

Let α, $\beta \in S$, $a \in F$

Then since T is a linear operator

$$T(a\alpha + \beta) = aT(\alpha) + T(\beta)$$

Also, α, $\beta \in S$ imply $T\alpha = c\alpha$ and $T\beta = c\beta$

So,

$$\begin{aligned} T(a\alpha + \beta) &= aT(\alpha) + T(\beta) \\ &= ac\alpha + c\beta \\ &= c(a\alpha + \beta) \end{aligned}$$

Therefore, $a\alpha + \beta \in S$ $\forall \alpha$, $\beta \in S$, $a \in F$

Hence, S is a subspace of V.

Note:

From this result, it is clear that if α is a characteristic vector of a linear operator T corresponding to the characteristic value c, then $k\alpha; k \in F$ is also a characteristic vector of a linear operator T corresponding to the same characteristic value c. Hence, there exist infinitely many characteristic vectors corresponding to one characteristic value c. However, S is a subspace of finite-dimensional vector space V. So, dim S is finite. This implies the number of linearly independent characteristic vectors corresponding to the characteristic value c is always finite. This finite number is called the geometric multiplicity of c.

Theorem 10.1.3: Let T be a linear operator on an n –dimensional vector space V over a field F.

If c is a characteristic value of T and α is the corresponding characteristic vector. Then for any positive integer n, c^n is a characteristic value of T^n and α is the corresponding characteristic vector. Since c is a characteristic value of T and α is the corresponding characteristic vector. Then, $T\alpha = c\alpha$

First, we prove the result for $n = 2$,

$$\begin{aligned} T^2(\alpha) &= T(T(\alpha)) \\ &= T(c\alpha) \\ &= cT(\alpha) \\ &= c(c\alpha) = c^2\alpha \end{aligned}$$

We assume that the result is true for $n - 1$.

So, $T^{n-1}(\alpha) = c^{n-1}\alpha$

Now we prove for n,

$$
\begin{aligned}
T^n(\alpha) &= T(T^{n-1}(\alpha)) \\
&= T(c^{n-1}\alpha) \\
&= c^{n-1}T(\alpha) \\
&= c^{n-1}c\alpha \\
&= c^n\alpha
\end{aligned}
$$

So, the result is true for all natural numbers.

Theorem 10.1.4: Let T be a linear operator on an n −dimensional vector space V over a field F.If c is a characteristic value of T and α is the corresponding characteristic vector.Then for any polynomial$f(x)$,
$f(c)$ is a characteristic value of $f(T)$ and α is the corresponding characteristic vector.

Proof: Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ be a polynomial of order n.

Consider

$$
\begin{aligned}
f(T)\alpha &= (a_0I + a_1T + a_2T^2 + \cdots + a_nT^n)\alpha \\
&= a_0\alpha + a_1T(\alpha) + a_2T^2(\alpha) + \cdots + a_nT^n(\alpha)
\end{aligned}
$$

Using the result that, for every positive integer k, c^k is a characteristic value of T^k and α is the corresponding characteristic vector.

We get, $T^k(\alpha) = c^k\alpha \ \forall \ k$

So,

$$
\begin{aligned}
f(T)\alpha &= a_0\alpha + a_1T(\alpha) + a_2T^2(\alpha) + \cdots + a_nT^n(\alpha) \\
&= a_0\alpha + a_1c\alpha + a_2c^2\alpha + \cdots + a_nc^n\alpha \\
&= (a_0 + a_1c + a_2c^2 + \cdots + a_nc^n)\alpha \\
&= f(c)\alpha
\end{aligned}
$$

So, $f(c)$ is a characteristic value of $f(T)$ and α is the corresponding characteristic vector.

Example 10.1.5:

Consider the identity linear operator T on the vector space R^2.Then with respect to the standard basis of R^2, the corresponding matrix is the identity matrix of order 2. Apparently, for any vector $(x, y) \in R^2$

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix}$$

So, every non-zero vector in R^2 is a characteristic vector of T corresponding to the characteristic value 1.But we also know that in R^2, a set containing more than 2 elements is linearly dependent.So, any linearly independent set of characteristic vectors of T must contain at the most two elements.So, the number of linearly independent characteristic vectors is 2.

Note:

From the fact that, if T is any linear operator and c is any scalar, then $T - cI$ is also a linear operator on V. Note that the set of vectors α such that $T\alpha = c\alpha$ is the same as the null space of operator $T - cI$.Again, the null space of operator $T - cI$ is non-zero if and only if $T - cI$ is not a one-one operator.

Because of these points, we have the next result

Theorem 10.1.6: 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) $\det T - cI = 0$.

(i) implies (ii)

c is the characteristic value of T. So, there exists a non-zero vector $\alpha \in V$ such that $T\alpha = c\alpha$

$$\Rightarrow T\alpha - c\alpha = 0$$

$$\Rightarrow (T - cI)\alpha = 0$$

$\Rightarrow \alpha \in$ Null space of $T - cI$

Since $\alpha \neq 0$, Null space of $T - cI \neq \{0\}$

Therefore, $T - cI$ is not one-one and hence not invertible.

(ii) implies (iii)

$T - cI$ is not invertible.

So, for any basis of $T - cI$, $[T - cI]_B$ has determinant 0.

$\Rightarrow \det(T - cI) = 0$

(iii) Implies (i)

det $(T - cI) = 0$

This implies $(T - cI)\alpha = 0$ has a non-trivial solution.

So, c is the characteristic value of T.

Note:

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. In other words, If B is an ordered basis for V and $A = [T]_B$, then $T - cI$ is invertible if and only if the matrix $A - cI$ is invertible.

Definition 10.1.7: 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). So, c is a characteristic value of A if and only if $det\ (A - cI) = 0$, or equivalently if and only if $det\ (cI - A) = 0$.

We form the matrix $xI - A$ with polynomial entries, consider the polynomial $f(x) = \det(xI - A)$.

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 that has degree exactly n.

Lemma 10.1.8: Similar matrices have the same characteristic polynomials.

Proof: Let A and B are two similar matrices of order $n \times n$.

This implies, there exists an invertible matrix P such that

$$B = P^{-1}AP$$

The characteristic polynomial of B $= \det(xI - B)$

$= \det(xP^{-1}P - P^{-1}AP)$

$= \det(P^{-1}(xI - A)P)$

$= \det P^{-1} \det(xI - A) \det P$

$= \det(xI - A)$

= Characteristic polynomial of A

So, similar matrices have the same characteristic polynomials.

Notes:

- We know that matrices of a linear operator on a vector space $V(F)$ corresponding to two distinct ordered bases of V are always similar.
- This implies that matrices of a linear operator corresponding to any bases of the vector space have the same characteristic polynomial and hence the same characteristic values.
- Also, since a linear operator on an $n-$dimensional vector space gives rise to a square matrix of order n and its characteristic polynomial is of degree n. Hence, it can not have more than n roots in F.
- There exist operators with no characteristic value, with less than n characteristic values, and with exactly n characteristic values.

Definition 10.1.9:

- The set of all characteristic values of T is called the spectrum of T.
- The number of times a characteristic value appears as a root of a characteristic polynomial is called the algebraic multiplicity of the characteristic value.
- The dimension of the eigenspace of T corresponding to the characteristic value c is called geometric multiplicity of c.

Example 10.1.10:

Example of a linear operator with no characteristic value. Let T be a linear operator on R^2 which is represented in the standard ordered basis by the matrix

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

Put $\det(xI - A) = 0$

We get,

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

This implies, $x^2 + 1 = 0$

Since this polynomial has no roots in R. So, T has no characteristic values.

Example 10.1.11:

Example of a linear operator with two characteristic values. Let T be a linear operator on C^2 which is represented in the standard ordered basis by the matrix

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

The characteristic polynomial of A is given by $x^2 + 1$ which has two roots i and $-i$ in C.So, A has two characteristic values i and $-i$.

Corresponding to $\lambda = i$

$(A - iI)X = 0$

$\Rightarrow \left(\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} - \begin{bmatrix} i & 0 \\ 0 & i \end{bmatrix} \right) \begin{bmatrix} x \\ y \end{bmatrix} = 0$

$\Rightarrow \begin{bmatrix} -i & -1 \\ 1 & -i \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = 0$

$\Rightarrow x - iy = 0$

$\Rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} iy \\ y \end{bmatrix} = y \begin{bmatrix} i \\ 1 \end{bmatrix}$

So, the characteristic vector is $\begin{bmatrix} i \\ 1 \end{bmatrix}$

Corresponding to $\lambda = -i$

$(A + iI)X = 0$

$\Rightarrow \left(\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} i & 0 \\ 0 & i \end{bmatrix} \right) \begin{bmatrix} x \\ y \end{bmatrix} = 0$

$\Rightarrow \begin{bmatrix} i & -1 \\ 1 & i \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = o$

$\Rightarrow x + iy = 0$

$\Rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -iy \\ y \end{bmatrix} = y \begin{bmatrix} -i \\ 1 \end{bmatrix}$

So, the characteristic vector is $\begin{bmatrix} -i \\ 1 \end{bmatrix}$

Example 10.1.12:

Let T be a linear operator on R^3 which is represented in the standard ordered basis by the matrix

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

We find characteristic values and characteristic vectors of T. Also, find the algebraic and geometric multiplicity of each characteristic value.

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

To find the characteristic polynomial,

put $|A - \lambda I| = 0$

$$\begin{vmatrix} 3-\lambda & 1 & -1 \\ 2 & 2-\lambda & -1 \\ 2 & 2 & 0-\lambda \end{vmatrix} = 0$$

$\Rightarrow (-1) \begin{vmatrix} 2 & 2-\lambda \\ 2 & 2 \end{vmatrix} - (-1) \begin{vmatrix} 3-\lambda & 1 \\ 2 & 2 \end{vmatrix} + (-\lambda) \begin{vmatrix} 3-\lambda & 1 \\ 2 & 2-\lambda \end{vmatrix} = 0$

$\Rightarrow -\big(4 - 2(2-\lambda)\big) + 1\big(2(3-\lambda) - 2\big) - \lambda\,\big((3-\lambda)(2-\lambda) - 2\big) = 0$

$\Rightarrow -2\lambda + 4 - 2\lambda - \lambda\,(4 + \lambda^2 - 5\lambda) = 0$

$\Rightarrow \lambda^3 - 5\lambda^2 + 8\lambda - 4 = 0$

$\Rightarrow (\lambda - 1)(\lambda^2 - 4\lambda + 4) = 0$

$\Rightarrow \lambda = 1,\ \lambda^2 - 4\lambda + 4 = 0$

$\Rightarrow \lambda = 1,\ 2,\ 2$

Since $\lambda = 1$ is appearing once as a root of the characteristic polynomial. Hence its algebraic multiplicity is 1.

Since $\lambda = 2$ is appearing twice as a root of the characteristic polynomial. Hence its algebraic multiplicity is 2.

For $\lambda = 1$, let $X = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$ be the corresponding characteristic vector

$$(A - I)X = 0$$

Implies,

$$\begin{bmatrix}2 & 1 & -1\\ 2 & 1 & -1\\ 2 & 2 & -1\end{bmatrix}\begin{bmatrix}x\\ y\\ z\end{bmatrix}=\begin{bmatrix}0\\ 0\\ 0\end{bmatrix}$$

Applying $R_2 \to R_2 - R_1, R_3 \to R_3 - R_1$

$$\begin{bmatrix}2 & 1 & -1\\ 0 & 0 & 0\\ 0 & 1 & 0\end{bmatrix}\begin{bmatrix}x\\ y\\ z\end{bmatrix}=\begin{bmatrix}0\\ 0\\ 0\end{bmatrix}$$

We get,

$$2x + y - z = 0,\ y = 0$$

That is, $2x - z = 0,\ y = 0$

$$\begin{bmatrix}x\\ y\\ z\end{bmatrix}=\begin{bmatrix}x\\ 0\\ 2x\end{bmatrix}=x\begin{bmatrix}1\\ 0\\ 2\end{bmatrix}$$

The only linearly independent characteristic vector corresponding to $\lambda = 1$ is $\begin{bmatrix}1\\ 0\\ 2\end{bmatrix}$. Therefore, its geometric multiplicity is 1.

For $\lambda = 2$, let $X = \begin{bmatrix}x\\ y\\ z\end{bmatrix}$ be the corresponding characteristic vector

$$(A - 2I)X = 0$$

That is,

$$\begin{bmatrix}1 & 1 & -1\\ 2 & 0 & -1\\ 2 & 2 & -2\end{bmatrix}\begin{bmatrix}x\\ y\\ z\end{bmatrix}=\begin{bmatrix}0\\ 0\\ 0\end{bmatrix}$$

Applying $R_2 \to R_2 - 2R_1,\ R_3 \to R_3 - 2R_1$

$$\begin{bmatrix}1 & 1 & -1\\ 0 & -2 & -1\\ 0 & 0 & 0\end{bmatrix}\begin{bmatrix}x\\ y\\ z\end{bmatrix}=\begin{bmatrix}0\\ 0\\ 0\end{bmatrix}$$

We get, $x + y - z = 0,\ -2y - z = 0$

Or $z = 2y,\ x = y$

That is,

$$\begin{bmatrix}x\\ y\\ z\end{bmatrix}=\begin{bmatrix}y\\ y\\ 2y\end{bmatrix}=y\begin{bmatrix}1\\ 1\\ 2\end{bmatrix}$$

The only linearly independent characteristic vector corresponding to $\lambda = 2$ is $\begin{bmatrix}1\\ 1\\ 2\end{bmatrix}$. Therefore, its geometric multiplicity is 1.

Task:

1. Consider any matrix A of order 2×2 over the field of real numbers. Then observe that the characteristic polynomial of A is $x^2 - (trace\ A)x + \det A$.
2. Let A be the identity matrix of order 3 over the field of real numbers. Then prove that A has exactly 3 linearly independent characteristic vectors.

10.2 Annihilating Polynomials

Definition 10.2.1: Let T be a linear operator on a finite-dimensional vector space V over a field F.

Then a polynomial $f(x) \in F[x]$ is said to be annihilating polynomial of T if $f(T) = 0$. For example, annihilating polynomial of identity operator on V is given by $f(x) = x$.

Example 10.2.2:

Let T be an operator on R^2 given by $T(x,\ y) = (x,\ 0)$. Find the annihilating polynomial for T.

Sol: $T: R^2 \to R^2$ is defined as

$T(x, y) = (x, 0)$

$T(T(x, y)) = T(x, 0) = (x, 0)$

Therefore, $T\left(T(x, y)\right) = T(x, y)$

Hence, $T^2 = T$

Consider $f(x) = x^2 - x$,

then clearly,

$f(T) = T^2 - T = 0$

So, $f(x)$ is annihilating polynomial for the linear operator T.

Example 10.2.3:

Let T be an operator on R^3 given by $T(x, y, z) = (0, x, y)$. Find the annihilating polynomial for T.

Sol:

$T(x, y, z) = (0, x, y)$

$T(T(x, y, z)) = T(0, x, y) = (0, 0, x)$

$T^2(x, y, z) = (0, 0, x)$

Again,

$T(T^2(x, y, z)) = T(0, 0, x) = (0, 0, 0)$

Hence, $T^3 = 0$

Consider $f(x) = x^3$,

then clearly,

$f(T) = T^3 = 0$

So, $f(x)$ is annihilating polynomial for the linear operator T.

Theorem 10.2.4: 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 $F[x]$ is a ring under the compositions

$$(p + q)(T) = p(T) + q(T)$$
$$(pq)(T) = p(T)q(T)$$

The collection S of polynomials p which annihilate T is an ideal in the polynomial algebra $F[x]$.

Note that, zero polynomial is annihilating polynomial for all the matrices. So, zero polynomial is in S.

Hence, $S \neq \phi$

Let $f, g \in S, h \in F[x]$ so that $f(T) = 0$ and $g(T) = 0$

Then,

$$(f - g)(T) = f(T) - g(T) = 0 - 0 = 0$$

and

$$fh(T) = f(T)h(T) = 0h(T) = 0$$
$$hf(T) = h(T)f(T) = h(T)0 = 0$$

So,

$$f - g, fh, hf \in S \;\forall f, g \in S, h \in F[x]$$

So, S is an ideal of $F[x]$.

Note:

In general, it is possible that for a linear operator T on a vector space V over a field F there is only one annihilating polynomial that is, zero polynomial. Now we prove that in case V is finite-dimensional, there exists at least one non-zero polynomial f that annihilates T.

Suppose $\dim V = n$

Then dimension of the space of linear operators on vector space V is n^2.

So, the $n^2 + 1$ powers of T given by

$$I, T, T^2, \ldots, T^{n^2}$$

is linearly dependent.

Therefore, there exist scalars $c_0, c_1, \ldots, c_{n^2}$ (not all zero) such that

$$c_0 I + c_1 T + \cdots + c_{n^2} T^{n^2} = 0$$

Consider

$$f(x) = c_0 + c_1 x + \cdots + c_{n^2} x^{n^2}$$

Since $c_i's$ are not all zero. So, $f(x) \neq 0$ and $(T) = 0$

That is, T has non-zero annihilating polynomial.

Remark 10.2.5: For every field F, $F[x]$ is a PID. So, every ideal is generated by a single element. Let T be a linear operator on a finite-dimensional vector space V over F. Then set S of annihilating polynomials of T, being an ideal of $F[x]$ is generated by a single element f. Generators of S may not be unique but there always exists a unique monic polynomial that generates S.

Let $f(x)$ be a generator of S.

Then for any $g(x) \in S$, there exists $h(x) \in F[x]$ such that $g(x) = f(x)h(x)$

Let α be the leading coefficient of $f(x)$.

Then $\alpha \neq 0$, $\alpha \in F$

So, $\alpha^{-1} \in F$

Consider $p(x) = \alpha^{-1} f(x)$

Then $p(x)$ is monic polynomial.

Also, $p(T) = \alpha^{-1} f(T) = \alpha^{-1} 0 = 0$

That is, p annihilates T

So, $p(x) \in S$

Also, for any $g(x) \in S$, there exists $h(x) \in F[x]$ such that $g(x) = f(x)h(x)$

That is the same as,

$$g(x) = (\alpha^{-1} f(x))(\alpha h(x))$$
$$= (\alpha^{-1} f(x))l(x)$$

where $l(x) \in F[x]$. This implies, $p(x)$ is a monic generator of S.

If possible, let $q(x)$ be another monic generator of S.

Since $p(x)$ is the generator of S and $q(x) \in S$, therefore, $p(x) | q(x)$

Similarly,

$$q(x) | p(x)$$

This implies,

$$p(x) = cq(x); c \in F$$

Comparing the leading coefficients on both sides, we get $c = 1$

Hence, $p(x) = q(x)$ which proves uniqueness.

Definition 10.2.6: 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 Fwhich annihilate T. The name 'minimal polynomial' stems from the fact that the 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 a smaller degree than p has.

Note:

If A is 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 annihilates 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 thebasis by the matrix $f(A)$, so that $f(T) = 0$ if and only if $f(A) = 0$.

Result 10.2.7: Let$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$. Then $f(P^{-1}AP) = P^{-1}f(A)P$ where P is an invertible matrix.

Proof:

$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$

$f(P^{-1}AP) = a_0 I + a_1(P^{-1}AP) + a_2(P^{-1}AP)^2 + \ldots + a_n(P^{-1}AP)^n$

$$\text{Note that}(P^{-1}AP)^2 = P^{-1}APP^{-1}AP = P^{-1}AIAP = P^{-1}A^2P$$

Similarly, $(P^{-1}AP)^k = P^{-1}A^kP \; \forall \, k$.

Then,

$$\begin{aligned} f(P^{-1}AP) &= a_0 I + a_1(P^{-1}AP) + a_2 P^{-1}A^2P + \ldots + a_n P^{-1}A^nP \\ &= P^{-1}(a_0 I + a_1 A + a_2 A^2 + \ldots + a_n A^n)P \\ &= P^{-1}f(A)P \end{aligned}$$

So, for every polynomial f,

$$f(P^{-1}AP) = P^{-1}f(A)P$$

Theorem 10.2.8: Similar matrices have the same minimal polynomial.

Let A and B are similar matrices.So, there exists an invertible matrix P such that

$$B = P^{-1}AP$$

Let $p(x)$ and $q(x)$ be the minimal polynomials of A and B respectively.Then $p(A) = 0$implies,

$$p(P^{-1}AP) = P^{-1}p(A)P = 0$$

So,

$$p(B) = 0$$

Therefore, $q(x)|p(x)$

Similarly, we can show that $p(x)|q(x)$

Since both are monic polynomials so, $p(x) = q(x)$

Remark 10.2.9: Suppose that A is an $n \times n$ matrix with entries in the field F.

Suppose that F_1 is a field that contains F as a subfield.

(For example, A might be a matrix with rational entries, while F_1 is the field of real 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, we might obtain two different minimal polynomials for A. Fortunately, that is not the case. Now we see why?

According to 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 given by

$$f = x^k + \sum_{j=0}^{k-1} a_j x^j \text{ ... (1)}$$

Then $f(A) = 0$ implies,

$$A^k + a_{k-1}A^{k-1} + \cdots + a_1 A + a_0 I = 0 \text{ ... (2)}$$

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 of A. Furthermore, by the uniqueness of the minimal polynomial, there is for that k one and only one relation of this form i.e., once the minimal k is determined, there are unique scalars $a_0, \ldots, a_{k-1}$ in F such that (2) holds. They are the coefficients of the minimal polynomial. Now (for each k) we have in (2), a system of n^2 linear equations for the unknowns $a_0, \ldots, a_{k-1}$. 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 $a_0, a_1, \ldots, a_{k-1}$ in F_1, it has a solution with $a_0, a_1, \ldots, a_{k-1}$ in F. It should now be clear that the two minimal polynomials are the same.

Theorem 10.2.10: 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.

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

$$\begin{aligned} 0 &= p(T)\beta \\ &= (T - cI)q(T)\beta \\ &= (T - cI)\alpha \end{aligned}$$

Thus, c is a characteristic value of T.

Conversely, suppose that c is a characteristic value of T,

that is, there exists non-zero α such that $T\alpha = c\alpha$

We know that if α is a characteristic vector of T corresponding to the characteristic value c, then α is a characteristic vector of $f(T)$ corresponding to the characteristic value $f(c)$.

So,

$$p(T)\alpha = p(c)\alpha$$

Since $p(T) = 0$, $\alpha \neq 0$,

So, $p(c) = 0$

Therefore, the roots of characteristic and minimal polynomials are the same.

Theorem 10.2.11: 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: Let K be the commutative ring with identity consisting of all polynomials in T.

of course, K is a commutative algebra with identity over the scalar field.

Choose an ordered basis $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ for V, and

let A be the matrix that represents T in the given basis.

Then

$$T\alpha_i = \sum_{j=1}^{n} A_{ji}\alpha_j\,,\ 1 \leq i \leq n$$

These equations may be written in the equivalent form

$$\sum_{j=1}^{n} (\delta_{ij}T - A_{ji}I)\alpha_j = 0;\ 1 \leq i \leq n$$

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

$$\det B = (T - A_{11}I)(T - A_{22}I) - A_{12}A_{21}I$$
$$= T^2 - (A_{11} + A_{22})T + (A_{11}A_{22} - A_{12}A_{21})I$$
$$= f(T)$$

where f is the characteristic polynomial $f = x^2 - (trace\ A)x + \det A$

For the case $n > 2$, it is also clear that $\det B = f(T)$

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 $f(T) = 0$.

For $f(T)$ be the zero operator, it is necessary and sufficient that $(\det B)\,\alpha_k = 0$ for $1 \leq k \leq n$

By the definition of B, the vectors $\alpha_1, \ldots, \alpha_n$ satisfy the condition

$$\sum_{j=1}^{n} B_{ij}\alpha_j = 0,\ 1 \leq i \leq n$$

When $n = 2$, we can write the above sum 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, we have,

$$\sum_{j=1}^{n} \tilde{B}_{ki}B_{ij}\alpha_j = 0$$

For each pair k, i and summing on i, we have

$$
\begin{aligned}
0 &= \sum_{i,j=1}^{n} \tilde{B}_{ki}B_{ij}\alpha_j\\
&= \sum_{j=1}^{n}\left(\sum_{i=1}^{n} \tilde{B}_{ki}B_{ij}\right)\alpha_j
\end{aligned}
$$

Now $\tilde{B}B = (\det B)\, I$, so that

$$\sum_{i,j=1}^{n} \tilde{B}_{ki}B_{ij} = \delta_{kj} \det B$$

Therefore,

$$
\begin{aligned}
0 &= \sum_{j=1}^{n} \delta_{kj}\,(\det B)\,\alpha_j\\
&= (\det B)\,\alpha_k,\quad 1 \le k \le n
\end{aligned}
$$

This proves the result that $f(T) = 0$ where f is the characteristic polynomial of T.

That is, characteristic polynomial of T is annihilating polynomial of T.

Therefore,

$$
\begin{aligned}
0 &= \sum_{j=1}^{n} \delta_{kj}\,(\det B)\,\alpha_j\\
&= (\det B)\,\alpha_k,\quad 1 \le k \le n
\end{aligned}
$$

This proves the result that $f(T) = 0$ where f is the characteristic polynomial of T.

That is, characteristic polynomial of T is annihilating polynomial of T.

Remark 10.2.12: By Cayley Hamilton Theorem, we have if the characteristic polynomial is

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

Then the minimal polynomial is given by

$$g(x) = (x - c_1)^{e_1}(x - c_2)^{e_2} \ldots (x - c_k)^{e_k}$$

where $1 \le e_i \le d_i$

So, it narrows down the search for minimal polynomials of various operators.

Note:

If a linear operator has all characteristic values distinct, that is no repeated characteristic value, then

$$d_i = 1\ \forall i$$

Since,

$$1 \le e_i \le d_i = 1$$

Therefore, $e_i = 1\ \forall\ i$.

Hence, its characteristic and minimal polynomials are the same.

Example 10.2.13:

Let A be the 4×4 (rational) matrix

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

Find the annihilating polynomial, minimal polynomial, and characteristic polynomial of A.

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

Squaring we get,

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

Again,

$$A^3 = \begin{bmatrix} 0 & 4 & 0 & 4 \\ 4 & 0 & 4 & 0 \\ 0 & 4 & 0 & 4 \\ 4 & 0 & 4 & 0 \end{bmatrix} = 4A$$

Consider $f(x) = x^3 - 4x$

Then $f(A) = A^3 - 4A = 0$

Therefore, $f(x) = x^3 - 4x$ is the annihilating polynomial for A.

$$f(x) = x^3 - 4x$$
$$= x(x^2 - 4)$$
$$= x(x - 2)(x + 2)$$

Let $p(x)$ be the minimal polynomial of A.

$$p(x) \mid f(x)$$

So, choices of $p(x)$ are

$$p(x) = x,\ x - 2,\ x + 2,\ x(x - 2),\ x(x + 2),\ x(x^2 - 4)$$

If $\deg p(x) = 1$

Let $p(x) = Cx + D,\ C, D \in F$

Now $p(A) = 0$

$\Rightarrow CA + DI = 0,\ C \neq 0$

$\Rightarrow A = -\frac{D}{C} I$, scalar multiple of identity

But A is not a scalar multiple of identity.

So, $\deg p(x) \neq 1$

If $\deg p(x) = 2$

Let $p(x) = x^2 + Dx + E$,

So, $A^2 + DA + E = 0$

$A^2 = -DA - E$

$$\Rightarrow \begin{bmatrix} 2 & 0 & 2 & 0 \\ 0 & 2 & 0 & 2 \\ 2 & 0 & 2 & 0 \\ 0 & 2 & 0 & 2 \end{bmatrix} = \begin{bmatrix} 0 & -D & 0 & -D \\ -D & 0 & -D & 0 \\ 0 & -D & 0 & -D \\ -D & 0 & -D & 0 \end{bmatrix} - \begin{bmatrix} E & 0 & E & 0 \\ 0 & E & 0 & E \\ E & 0 & E & 0 \\ 0 & E & 0 & E \end{bmatrix}$$

Comparing entry in 2nd row, 1st column, we get,

$0 = -D - 0$ that is, $D = 0$

$\Rightarrow A^2 = -EI$, scalar multiple of identity.

But A^2 is not a scalar multiple of identity.

Hence $\deg p(x) \neq 2$

Therefore, $\deg p(x) = 3$

So, $p(x) = x(x-2)(x+2)$ is the minimal polynomial of A.

Since roots of minimal polynomial and characteristic polynomials are same, therefore, characteristic polynomial of A has roots $0,\ 2$, and -2.

Now, A is a matrix of order 4. Therefore, there is one more root say x.

Then $0 + 2 + (-2) + x = trace\ A$

That is $x = trace\ A = 0$

So, four characteristic values of A are $0,\ 0,\ 2$, and -2.

Hence characteristic polynomial is $x^2(x^2 - 4)$.

Example 10.2.14: Let a, b and c be elements of a field F, let A be the following matrix

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

Find the characteristic and minimal polynomial for A.

Sol: $A = \begin{bmatrix} 0 & 0 & c \\ 1 & 0 & b \\ 0 & 1 & a \end{bmatrix}$

For characteristic polynomial, put $|xI - A| = 0$

$$\Rightarrow \begin{vmatrix} x & 0 & -c \\ -1 & x & -b \\ 0 & -1 & x-a \end{vmatrix} = 0$$

$\Rightarrow x^2(x-a) - bx - c = 0$

$\Rightarrow x^3 - ax^2 - bx - c = 0$

The characteristic polynomial of A is $x^3 - ax^2 - bx - c$.

Since A is not a scalar matrix.

Therefore, the degree of its minimal polynomial is not equal to 1.

If the degree of the minimal polynomial is 2.

Let $p(x) = x^2 + dx + e$ be the minimal polynomial.

Then $A^2 + dA + eI = 0$

So, $A^2 = -dA - eI \ldots (1)$

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

Then $A^2 = \begin{bmatrix} 0 & c & ca \\ 0 & b & c+ba \\ 1 & a & b+a^2 \end{bmatrix}$

Put in (1),

$$\begin{bmatrix} 0 & c & ca \\ 0 & b & c+ba \\ 1 & a & b+a^2 \end{bmatrix} = \begin{bmatrix} 0 & 0 & -dc \\ -d & 0 & -bd \\ 0 & -d & -ad \end{bmatrix} - \begin{bmatrix} e & 0 & 0 \\ 0 & e & 0 \\ 0 & 0 & e \end{bmatrix}$$

$$\begin{bmatrix} 0 & c & ca \\ 0 & b & c+ba \\ 1 & a & b+a^2 \end{bmatrix} = \begin{bmatrix} -e & 0 & -dc \\ -d & -e & -bd \\ 0 & -d & -ad-e \end{bmatrix}$$

Comparing entry at $(2, 1)$ place,

$0 = -d,\ d = 0$

Then $A^2 = -eI$

But A^2 is not a scalar multiple of identity.

So, $\deg p(x) \neq 2$

Therefore, $\deg p(x) = 3 =$ degree of the characteristic polynomial

Since minimal polynomial divides characteristic polynomial, minimal polynomial and characteristic polynomial are same that is $x^3 - ax^2 - bx - c$.

Task:

1. Find a linear operator which has annihilating polynomial x^2.
2. Prove that for a square matrix of order n, we can always find an annihilating polynomial of degree less than or equal to n.

10.3 Diagonal Canonical Form

Definition 10.3.1: 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. That is, there exists a basis $B = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ of V such that all the $\alpha_i's$ are characteristic vectors of T.

Theorem 10.3.2: Let V be an n-dimensional vector space over a field F. Let $T: V \to V$ is a linear operator on V. Then T is diagonalizable if and only if there exists a basis B of V such that $[T]_B$ is a diagonal matrix.

Proof: Let T is a diagonalizable linear operator on V. So, there exists a basis $B = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ of V such that all the $\alpha_i's$ are characteristic vectors of T. Since, α_i is a characteristic vector of $T \forall\ 1 \le i \le n$.

Therefore, there exist $c_i \in F,\ 1 \le i \le n$ such that $T\alpha_i = c_i\alpha_i$

Now we find the matrix of T with respect to basis B.

$$T(\alpha_1) = c_1\alpha_1 = c_1\alpha_1 + 0\alpha_2 + \dots + 0\alpha_n$$
$$T(\alpha_2) = c_2\alpha_2 = 0\alpha_1 + c_2\alpha_2 + \dots + 0\alpha_n$$
$$\vdots$$
$$T(\alpha_n) = c_n\alpha_n = 0\alpha_1 + 0\alpha_2 + \dots + c_n\alpha_n$$

Hence, the matrix of T with respect to basis B is

$$[T]_B = \begin{bmatrix} c_1 & 0 & \dots & 0 \\ 0 & c_2 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & c_n \end{bmatrix}$$

which is a diagonal matrix.

Conversely, let $B = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ is a basis of V such that the matrix of T with respect to basis B is a diagonal matrix D.

Let

$$D = \begin{bmatrix} c_1 & 0 & \dots & 0 \\ 0 & c_2 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & c_n \end{bmatrix}$$

Then clearly,

$$T(\alpha_1) = c_1\alpha_1 + 0\alpha_2 + \cdots + 0\alpha_n = c_1\alpha_1$$
$$T(\alpha_2) = 0\alpha_1 + c_2\alpha_2 + \cdots + 0\alpha_n = c_2\alpha_2$$
$$\vdots$$
$$T(\alpha_n) = 0\alpha_1 + 0\alpha_2 + \cdots + c_n\alpha_n = c_n\alpha_n$$

That is,

$$T(\alpha_i) = c_i\alpha_i \ \forall\ 1 \le i \le n$$

Also, since $\alpha_i \in B \ \forall\ i$

Since B being the basis of V is linearly independent and any set consisting of 0 is linearly dependent. This implies, $\alpha_i \neq 0 \ \forall\ i$. Hence, $T(\alpha_i) = c_i\alpha_i \ \forall\ 1 \le i \le n$ and $\alpha_i \neq 0$.So, each α_i is an eigenvector of T.

B is a basis of V consisting of eigenvectors of T.So, T is diagonalizable.

Theorem 10.3.3: Characteristic vectors corresponding to distinct characteristic values are always linearly independent.

Proof: Let T be a linear operator on an n −dimensional vector space V over a field F.

First, we prove this result for $n = 2$.

Let α, β are characteristic vectors corresponding to distinct characteristic values c_1 and c_2 of T.

That is, $T(\alpha) = c_1\alpha$ and $T(\beta) = c_2\beta$

Consider $a, b \in F$ such that

$$a\alpha + b\beta = 0$$

Then

$$T(a\alpha + b\beta) = T(0) = 0$$

That is,

$$aT(\alpha) + bT(\beta) = 0$$

Or,

$$ac_1\alpha + bc_2\beta = 0$$

Multiply $a\alpha + b\beta = 0$ by c_1 and subtract from $ac_1\alpha + bc_2\beta = 0$, we get,

$$b(c_1 - c_2)\beta = 0$$

Note that β being a characteristic vector is non-zero and $c_1 \neq c_2$ implies $b = 0$

Put $b = 0$ in $a\alpha + b\beta = 0$,

using the fact that α being a characteristic vector is non-zero, we get, $a = 0$

Therefore, α and β are linearly independent.

So, the result is true for $n = 2$.

Let the result is true for $n - 1$.

Now we prove the result for n.

Let $c_1, c_2, \dots, c_n$ be n distinct characteristic values and $x_1, x_2, \dots, x_n$ be the corresponding characteristic vectors.Consider $a_1, a_2, \dots, a_n \in F$ such that

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0 \dots (1)$$

This implies,

$$T(a_1x_1 + a_2x_2 + \cdots + a_nx_n) = T(0) = 0$$

That is,

$$a_1T(x_1) + a_2T(x_2) + \cdots + a_nT(x_n) = 0$$

Using $T(x_i) = c_ix_i$, we get,

$$a_1c_1x_1 + a_2c_2x_2 + \cdots + a_nc_nx_n = 0 \ldots (2)$$

Multiply (1) by c_n and subtract from (2), we get,

$$\sum_{i=1}^{n-1} a_i(c_n - c_i)x_i = 0$$

The left side is a linear combination of $n-1$ characteristic vectors corresponding to distinct characteristic values.

So, by the induction hypothesis,

$$a_i(c_n - c_i) = 0 \; \forall \; 1 \leq i \leq n-1$$

Note that $c_n \neq c_i \; \forall \; i \neq n$

Hence, $a_i = 0 \; \forall \; 1 \leq i \leq n-1$

Putting in (1), we get, $a_n = 0$

Hence, $x_1, x_2, \ldots, x_n$ are linearly independent.

So, characteristic vectors corresponding to distinct characteristic values are always linearly independent.

Theorem 10.3.4: Characteristic polynomial of a diagonalizable linear operator is a product of linear factors.

Proof: Let T be a diagonalizable linear operator on a finite-dimensional vector space V over a field F.

Let $c_1, \ldots, c_k$ be the distinct characteristic values of T.

Then there is an ordered basis B in which T is represented by a diagonal matrix which has 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

$$[T]_B = \begin{bmatrix} c_1I_1 & & & \\ & c_2I_2 & & \\ & & \ddots & \\ & & & c_kI_k \end{bmatrix}$$

where I_t is the identity matrix of order d_t.

The matrix $[T]_B$ is a diagonal matrix. So, its characteristic polynomial is given by

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

which is a product of linear factors.

Remark: 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, then we will see a special property of T when we say that its characteristic polynomial has such a factorization. That is, we see is that d_i, the number of times which c_i is repeated as the root of characteristic polynomial f, is equal to the dimension of the space of characteristic vectors associated with the characteristic value c_i. Because the nullity of a diagonal matrix is equal to the number of zeros which it has on its main diagonal, and the matrix $\left.T - c_iI\right]_B$ 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 will provide us with a simpler way of determining whether a given operator is diagonalizable.

Lemma 10.3.5: Let$T$ be a linear operator on the finite-dimensional space V. Let $c_1, \ldots, c_k$ 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

$$W = W_1 + W_2 + \cdots + W_k,$$

then $dim\ W = dim\ W_1 + \dots + dim\ W_k$.

If B_i is an ordered basis for W_i, then $B = (B_1, B_2, \dots, B_k)$ is an ordered basis for W.

Proof: The space $W = W_1 + W_2 + \dots + W_k$ is the subspace spanned by all the characteristic vectors of T. Note that usually $dim\ W < dim\ W_1 + \dots + dim\ W_k$. This is because of linear relations which may exist between vectors in the various spaces.

To prove this lemma, it is sufficient to prove that the characteristic spaces associated with different characteristic values are independent of one another.

Suppose that (for each i) $a_i \in F$, $\alpha_i \in W_i$

$$a_1\alpha_1 + a_2\alpha_2 + \dots + a_k\alpha_k = 0 \ \dots (1)$$

Since $\alpha_i \in W_i$, α_i is a characteristic vector of T corresponding to the characteristic value c_i, then so is $a_i\alpha_i$. Let $\beta_i = a_i\alpha_i$

Then (1) is,

$$\beta_1 + \beta_2 + \dots + \beta_k = 0$$

where β_i is a characteristic vector of T corresponding to the characteristic value c_i.

We will show that $\beta_i = 0\ \forall\ i$

Since $T\beta_i = c_i\beta_i$

$$\begin{aligned} 0 &= f(T)0 \\ &= f(T)(\beta_1 + \beta_2 + \dots + \beta_k) \\ &= f(T)\beta_1 + f(T)\beta_2 + \dots + f(T)\beta_k \\ &= f(c_1)\beta_1 + f(c_2)\beta_2 + \dots + f(c_k)\beta_k \end{aligned}$$

Choose polynomials $f_1, f_2, \dots, f_k$ such that

$$f_i(c_j) = \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

Then

$$\begin{aligned} 0 &= f_i(T)0 \\ &= \sum_j \delta_{ij}\beta_j = \beta_i \end{aligned}$$

Now, let B_i be an ordered basis for W_i, and

let B be the sequence $B = (B_1, B_2, \dots, B_k)$.

Then B spans the subspace $W = W_1 + \dots + W_k$.

Also, B is a linearly independent sequence of vectors, for the following reason.

Any linear relation between the vectors in B will have the form $\beta_1 + \beta_2 + \dots + \beta_k = 0$ where β_i is some linear combination of the vectors in B_i. From what we just did, we know that $\beta_i = 0$ for each i. Since each B_i is linearly independent, we see that we have only the trivial linear relation between the vectors in B.

Theorem 10.3.6: Let T be a linear operator on a finite-dimensional space V. Let $c_1, \dots, c_k$ 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 $f = (x - c_1)^{d_1} \dots (x - c_k)^{d_k}$

and $dim\ W_i = d_i$, $i = 1, \dots, k$.

$(iii)\ \dim W_1 + \dim W_2 + \dots + \dim W_k = \dim V$

Proof: We have observed that (i) implies (ii).

Now we prove, (ii) implies (iii)

From (ii),

The characteristic polynomial for T is

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

and $\dim W_i = d_i$

Since $\dim V = n = \deg f$

Therefore,

$$d_1 + d_2 + \dots + d_k = n$$

That is,

$$\dim W_1 + \dim W_2 + \dots + \dim W_k = \dim V$$

Now we prove, (iii) implies (i)

From (iii),

$$\dim W_1 + \dim W_2 + \dots + \dim W_k = \dim V$$

From lemma,

$$\dim W_1 + \dim W_2 + \dots + \dim W_k = \dim W$$

W is a subspace of V and $\dim V = \dim W$

Then $V = W$

That is,

$$V = W_1 + W_2 + \dots + W_k$$

So, characteristic vectors of T span V. That is, T is diagonalizable.

This theorem gives an important characterization of diagonalizable operators given by a linear operator is diagonalizable if and only if its characteristic polynomial is a product of linear factors.

Remark 10.3.7: The matrix analogue of this theorem may be formulated as follows.

Let A be an $n \times n$ matrix with entries in a field F, and let $c_1, \dots, c_k$ 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

$(A - c_i I)X = 0$ and let B_i be an ordered basis for W_i.

The bases $B_1, B_2, \dots, B_k$ collectively string together to form the sequence of columns of a matrix P:

$$P = [P_1, P_2, \dots] = (B_1, \dots, B_k).$$

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.

Theorem 10.3.8: Let T be a diagonalizable linear operator on an n –dimensional vector space V over a field F and let $c_1, c_2, \dots, c_k$ be the distinct characteristic values of T. Then the minimal polynomial for T is the polynomial

$$p = (x - c_1) \dots (x - c_k)$$

Proof: If α is a characteristic vector, then one of the operators $T - c_1 I, \dots, T - c_k I$ sends α into 0. Therefore

$$(T - c_1 I) \dots (T - c_k I)\alpha = 0 \dots (1)$$

for every characteristic vector α.

Also, T is diagonalizable implies there is a basis $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ for the underlying space V which consists of characteristic vectors of T;

Hence, each α_i is a characteristic vector of T.

Let $x \in V$. Then there exist unique $x_1, x_2, \ldots, x_n \in F$ such that

$$x = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$$

Consider

$$\begin{aligned} p(T)x &= (T - c_1I)(T - c_2I)\ldots(T - c_kI)x \\ &= (T - c_1I)(T - c_2I)\ldots(T - c_kI)\left(\sum_{i=1}^{n} x_i\alpha_i\right) \\ &= \sum_{i=1}^{n} x_i(T - c_1I)(T - c_2I)\ldots(T - c_kI)\alpha_i \\ &= 0 \text{ (From (1))} \end{aligned}$$

So, $p(T)x = 0\ \forall\ x \in V$

This implies, $p(T) = 0$

Note:

From the above results, it is clear that

- The minimal polynomial of a diagonalizable linear operator on a finite-dimensional vector space is a product of distinct linear factors.
- However, we will see soon that it is the characterizing condition for a linear operator to be diagonalizable.

Result 10.3.9: Minimal polynomial of a linear operator T is of degree 1 if and only if it is a scalar multiple of identity operator.

Proof: Let minimal polynomial of T is $x + a; a \in F$.

$\Leftrightarrow T + aI = 0$

$\Leftrightarrow T = -aI$

$\Leftrightarrow T$ is a scalar multiple of identity operator.

Result 10.3.10: Minimal polynomial of a non-zero linear operator T is never a non-zero constant polynomial

Proof: Let minimal polynomial of T is

$$f(x) = c; c \neq 0,\ c \in F$$

$$f(T) = 0 \Leftrightarrow cI = 0 \Leftrightarrow c = 0$$

But $c \neq 0$, so, we arrive at a contradiction. Therefore, $f(x) \neq 0$.

Example 10.3.11:

Let T be a 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 since T has no characteristic value and hence, no characteristic vector. Therefore, T is not diagonalizable.

Example 10.3.12:

Let T be a linear operator on C^2 which is represented in the standard ordered basis by the matrix

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

We will discuss whether it is diagonalizable or not. If yes, then we try to find the matrix P for which $P^{-1}AP$ is a diagonal matrix.

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

Characteristic values of A are i and $-i$. Moreover, corresponding to i, characteristic vector is $\begin{bmatrix} i \\ 1 \end{bmatrix}$ and corresponding to $-i$, characteristic vector is $\begin{bmatrix} -i \\ 1 \end{bmatrix}$.

$$P = \begin{bmatrix} i & -i \\ 1 & 1 \end{bmatrix}$$

Then det $P = 2i \neq 0$

$$P^{-1} = \frac{1}{2i}\begin{bmatrix} 1 & i \\ -1 & i \end{bmatrix}$$

Thus

$$P^{-1}AP = \frac{1}{2i}\begin{bmatrix} 1 & i \\ -1 & i \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} i & -i \\ 1 & 1 \end{bmatrix}$$

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

Example 10.3.13:

Let T be a linear operator on R^3 which is represented in the standard ordered basis by the matrix

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

We will discuss whether it is diagonalizable or not. If yes, then we try to find the matrix P for which $P^{-1}AP$ is a diagonal matrix.

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

A has three characteristic values 1, 2, 2

Corresponding to $\lambda = 1$, the characteristic vector is $\begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix}$

Corresponding to $\lambda = 2$, the characteristic vector is $\begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix}$

Corresponding to three characteristic values, the number of linearly independent characteristic vectors is 2.

$$\dim R^3 = 3$$

Therefore, we can't find a basis of R^3 having characteristic vectors of T.

Hence, T is not diagonalizable.

Example 10.3.14:

Let T be a linear operator on R^3 which is represented in the standard ordered basis by the matrix

$$A = \begin{bmatrix} 5 & -6 & -6 \\ -1 & 4 & 2 \\ 3 & -6 & -4 \end{bmatrix}$$

If possible, find a basis of R^3, corresponding to which the matrix of T is a diagonal matrix.

Sol: Given

$$A = \begin{bmatrix} 5 & -6 & -6 \\ -1 & 4 & 2 \\ 3 & -6 & -4 \end{bmatrix}$$

The characteristic equation of A is

$$|A - \lambda I| = 0$$

$$\Rightarrow \begin{vmatrix} 5-\lambda & -6 & -6 \\ -1 & 4-\lambda & 2 \\ 3 & -6 & -4-\lambda \end{vmatrix} = 0$$

Solving we get, $\lambda = 1,\ 2,\ 2.$

Corresponding to $\lambda = 1$, let $X = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$ be a characteristic vector. Then

$$(A - I)X = 0$$

$$\Rightarrow \begin{bmatrix} 4 & -6 & -6 \\ -1 & 3 & 2 \\ 3 & -6 & -5 \end{bmatrix}\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Interchanging R_2 with R_1,

$$\Rightarrow \begin{bmatrix} -1 & 3 & 2 \\ 4 & -6 & -6 \\ 3 & -6 & -5 \end{bmatrix}\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Applying $R_2 \to R_2 + 4R_1,\ R_3 \to R_3 + 3R_1$

$$\Rightarrow \begin{bmatrix} -1 & 3 & 2 \\ 0 & 6 & 2 \\ 0 & 3 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Applying $R_3 \to R_3 - 2R_2$

$$\Rightarrow \begin{bmatrix} -1 & 3 & 2 \\ 0 & 6 & 2 \\ 0 & 0 & 0 \end{bmatrix}\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$-x + 3y + 2z = 0,\ 6y + 2z = 0$$

That is, $z = -3y = x$

So, $\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} -3y \\ y \\ -3y \end{bmatrix} = y\begin{bmatrix} -3 \\ 1 \\ -3 \end{bmatrix}$

The characteristic vector is $\begin{bmatrix} -3 \\ 1 \\ -3 \end{bmatrix}$.

W_1 has basis $B_1 = \{(-3,\ 1,\ -3)\}$

Corresponding to $\lambda = 2$, let $X = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$ be a characteristic vector. Then

$$(A - 2I)X = 0$$

$$\Rightarrow \begin{bmatrix} 3 & -6 & -6 \\ -1 & 2 & 2 \\ 3 & -6 & -6 \end{bmatrix}\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Interchanging R_2 with R_1,

$$\Rightarrow \begin{bmatrix} -1 & 2 & 2 \\ 3 & -6 & -6 \\ 3 & -6 & -6 \end{bmatrix}\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Applying $R_2 \to R_2 + 3R_1,\ R_3 \to R_3 + 3R_1$

$$\Rightarrow \begin{bmatrix} -1 & 3 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\Rightarrow\ -x + 2y + 2z = 0$$

So, $\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 2y + 2z \\ y \\ z \end{bmatrix} = y\begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} + z\begin{bmatrix} 2 \\ 0 \\ 1 \end{bmatrix}$

The characteristic vectors are $\begin{bmatrix}2\\1\\0\end{bmatrix}$ and $\begin{bmatrix}2\\0\\1\end{bmatrix}$.

W_2 has basis $B_2 = \{(2, 1, 0), (2, 0, 1)\}$

Consider $B = (B_1, B_2) = \{(-3, 1, -3), (2, 1, 0), (2, 0, 1)\}$.

Summary

- Characteristic value and characteristic vector of a linear operator on a finite-dimensional vector space V over F are defined.
- Annihilating polynomial of a linear operator T on a finite-dimensional vector space V over a field F is defined.
- Proved that the set of annihilating polynomials is an ideal of $F[x]$.
- The existence and uniqueness of minimal polynomial are proved.
- Cayley Hamilton Theorem is stated and proved.
- Examples are given to understand how to find minimal and annihilating polynomials of a linear operator
- The diagonalizable operator on a finite-dimensional vector space is defined.

Keywords

- Characteristic Values
- Characteristic Vectors
- Annihilating Polynomials
- Minimal Polynomial
- Cayley Hamilton theorem
- Diagonalization
- Diagonalizable linear operator

Self Assessment

1. Let eigenvalues of a matrix A of order 3 are 1, 2, and x. If determinant A is 6. Then the value of x is

A. 1
B. 2
C. 3
D. 6

2. Largest eigenvalue of the matrix $\begin{bmatrix}2 & 1 & 3\\0 & 3 & 1\\0 & 0 & 2\end{bmatrix}$ is

A. 2
B. 3
C. 4
D. 1

3. Let A= $\begin{bmatrix}3 & -2\\4 & -2\end{bmatrix}$ satisfies the matrix equation $A^2 - kA + 2I = 0$, then the value of k is

A. 0
B. 1
C. 2
D. 3

4. The characteristic polynomial of the matrix $\begin{bmatrix} 4 & 1 & 0 \\ 0 & 4 & 1 \\ 0 & 0 & 4 \end{bmatrix}$ is

A. $(x-4)^3$
B. $(x-4)^2(x-1)$
C. $(x-1)^2(x-4)$
D. $(x-1)^3$

5. Minimal polynomial of a matrix A of order 3 × 3 is of degree 1. Then A is a
A. scalar matrix
B. Zero matrix
C. Either scalar or zero matrix
D. Identity matrix

6. Similar matrices have the same
A. Characteristic polynomial
B. Characteristic values
C. Trace
D. All options are correct

7. Which of the following is an incorrect statement?
A. Minimal polynomial of a square matrix always divides its characteristic polynomial
B. Minimal polynomial of a square matrix divides each of its annihilating polynomials
C. The monic annihilating polynomial of a matrix is always unique
D. Roots of the minimal polynomial are the characteristic values of the matrix

8. Let T be a linear operator on R^4 such that the minimal polynomial of T is $x^2(x-1)$ then the number of distinct characteristic values of T is
A. 1
B. 2
C. 3
D. 4

9. Annihilating polynomial of matrix $A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ is

A. $x-1$
B. $(x-1)^2$
C. $(x-1)^3$
D. $(x-1)^4$

10. Let A be a square matrix of order 3 with entries from real numbers. Let A satisfies $A^3 = A$. Then A
A. is diagonalizable
B. is not diagonalizable
C. is invertible
D. has repeated eigenvalues

11. The matrix A= $\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$

A. is diagonalizable
B. is not invertible
C. has distinct eigenvalues
D. is not diagonalizable

12. Let A= $\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ then choose the correct statement

A. A is not diagonalizable
B. A is invertible
C. A has distinct eigenvalues
D. A has only one independent eigenvector

13. The invertible matrix P, such that $P^{-1}AP$ is a diagonal matrix where A= $\begin{bmatrix} 2 & 0 & 0 \\ 1 & 2 & 1 \\ -1 & 0 & 1 \end{bmatrix}$

A: $\begin{bmatrix} -1 & -1 & 0 \\ 1 & 0 & -1 \\ -1 & 1 & 1 \end{bmatrix}$
B: $\begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{bmatrix}$
C: $\begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & -1 \\ -1 & 0 & 1 \end{bmatrix}$
D: $\begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & -1 \\ -1 & 0 & 1 \end{bmatrix}$

14. Let P= $\begin{bmatrix} 2 & -1 \\ 5 & 1 \end{bmatrix}$ and D= $\begin{bmatrix} 6 & 0 \\ 0 & -1 \end{bmatrix}$. If D= $P^{-1}AP$ then A^3=

A: $\begin{bmatrix} 61 & 62 \\ 156 & 154 \end{bmatrix}$
B: $\begin{bmatrix} 61 & 62 \\ 155 & 154 \end{bmatrix}$
C: $\begin{bmatrix} 61 & 60 \\ 155 & 154 \end{bmatrix}$
D: $\begin{bmatrix} 61 & 62 \\ 155 & 150 \end{bmatrix}$

15. The matrix $\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$ is diagonalizable over
A. $\mathbb{R}$ (The field of real numbers)
B. $\mathbb{Z}$ (The ring of integers)
C. $\mathbb{Q}$ (The field of rational numbers)
D. $\mathbb{C}$ (The field of complex numbers)

Answers for Self Assessment

1.	C	2.	B	3.	B	4.	B	5.	A
6.	D	7.	C	8.	B	9.	D	10.	A
11.	A	12.	C	13.	B	14.	B	15.	D

Review Questions

1. Let P be the operator on R^2 which projects each vector onto the x −axis, parallel to the y −axis: $P(x, y) = (x, 0)$. Show that P is linear. What is the minimal polynomial for P?
2. Let A be an $n \times n$ matrix with characteristic polynomial $f = (x - c_1)^{d_1} \ldots (x - c_k)^{d_k}$. Show that $c_1 d_1 + c_2 d_2 + \cdots + c_k d_k = trace\ A$.
3. Let V be the vector space of $n \times n$ matrices over the field F. Let A be a fixed $n \times n$ matrix. Let T be the linear operator on V defined by $T(B) = AB$. Show that the minimal polynomial for T is the minimal polynomial for A.
4. Let A be a 4×4 matrix over the field of real numbers

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

   Find the characteristic and minimal polynomials of A.

5. Check whether the matrix A given in exercise 4 is similar over the field of complex numbers to a diagonal matrix.

Further Regarding

- Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress
- Topics in algebra by I.N. Hartstein, Wiley
- Abstract algebra by David S Dummit and Richard M Foote, Wiley

Weblinks

- https://nptel.ac.in/courses/111/102/111102009/
- https://nptel.ac.in/courses/111/105/111105112/#

Unit 11: Invariant Subspaces and Triangular Form

CONTENTS

Objective

After studying this unit, you will be able to

- define invariant subspaces of a vector space under a linear operator,
- prove important results related to invariant subspaces,
- define $T-$conductor of an element α into an invariant subspace W of V,
- understand the concept of triangulable operators with the help of examples.

Introduction

In this unit, you will be introduced to a special class of subspaces that are invariant under a linear operator T. Important results related to these subspaces will be proved. Further $T-$conductor of an element α into an invariant subspace W of V will be defined and the triangulation process will be explained with the help of examples.

11.1 Invariant Subspaces

Definition 11.1.1: Let V be a vector space and T a linear operator on V. If W is a subspace of V, we say that W is invariant under T if for each vector $\alpha \in W$, $T(\alpha) \in W$ i.e., if $T(W)$ is contained in W.

For example, every subspace is invariant under the identity operator.

Example [illegible] be a finite-dimensional vector space over a field F. Then for any operator T on V, $Ker\ T$ is an invariant subspace of V.

Proof: $Ker\ T = \{x \in V | T(x) = 0\}$

We know that $Ker\ T$ is a subspace of V.

Consider $\alpha \in Ker\ T$

This implies, $T(\alpha) = 0$

Since T is linear operator, $T(0) = 0$

That is $0 \in Ker\ T$

This implies $T(\alpha) \in Ker\ T\ \forall \alpha \in Ker\ T$

Hence, $Ker\ T$ is invariant under T.

Example 11.1.3: Let V be a finite-dimensional vector space over a field F. Then for any operator T on V, Range T is an invariant subspace of V.

Proof: Range $T = \{T(x) | x \in V\}$

We know that Range T is a subspace of V.

Consider $\alpha \in$ Range T

This implies, there exists $\beta \in V$ such that $T(\beta) = \alpha$

Since T is a linear operator on $V, T(\beta) \in V$

Let $T(\beta) = \gamma \in V$

Then $T(\gamma) = T\left(T(\beta)\right) = T(\alpha)$

So, $T(\alpha) \in$ Range $T\ \forall\ \alpha \in$ Range T

Hence, Range T is invariant under T.

Theorem 11.1.4: 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.

Proof: Let $\alpha \in W =$ Range U

This implies, there exists $\beta \in V$ such that $U(\beta) = \alpha$

Consider $T(\alpha) = T\left(U(\beta)\right)$

$$= TU(\beta)$$

$= UT(\beta) \in$ Range $U = W$

This implies, $T(\alpha) \in W\ \forall \alpha \in W$

That is, W in invariant under T.

Again, let $\alpha \in N$.

This implies, $U(\alpha) = 0$

Consider $UT(\alpha) = T\left(U(\alpha)\right)$

$$= T(0)$$

$$= 0$$

This implies, $T(\alpha) \in N\ \forall \alpha \in N$

That is, N in invariant under T.

Remark 11.1.5: Since any polynomial in T commutes with T, so for any polynomial $U = f(T)$, range space and null space of U are invariant under T.

Taking $U = T - cI,\ c \in F$, we see that the null space of U is invariant under T.

But null space of U is the space of characteristic vectors of T associated with characteristic value c.

This implies the space of characteristic vectors of T associated with characteristic value c is invariant under T.

Example 11.1.6: Let $V = R^2$ be a vector space over the field of real numbers. Define $T: R^2 \to R^2$ as $T(x, y) = (-y, x)$. Then T is a linear operator.

Consider the subspace $W = \{(x, 0) | x \in R\}$ of V.

Then $(1, 0) \in W$

But $T(1, 0) = (0, 1) \notin W$

Hence, W is not invariant under T.

Example 11.1.7: 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.

Proof: Let W be a subspace of R^2 invariant under T.

Since W is a subspace of R^2 and $\dim R^2 = 2$.

Therefore, $\dim W = 0,\ 1$ or 2.

If $\dim W = 0$ then W is $\{0\}$ subspace.

If $\dim W = 2 = \dim R^2$ then $W = R^2$

If $\dim W = 1$

Let $B = \{\alpha\},\ \alpha \neq 0$ be the basis of W

Since W is invariant under T and $\alpha \in W$

So, $T(\alpha) \in W = <\alpha>$

That is, there exists $c \in R$ such that $T(\alpha) = c\alpha$

This implies c is a characteristic value of T.

Since T is represented by the matrix

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

which has no real characteristic value.

Hence, we arrive at a contradiction.

That is, $\dim W \neq 1$

So, $W = \{0\}$ or R^2

<u>**Remark 11.1.8:**</u>Let T be a linear operator on a finite-dimensional vector space V over a field F.

Let W be a subspace of V invariant under T.Then by definition, $T(W) \subset W$

In this case, we can have a linear operator T_W on W such that $T_W(\alpha) = T(\alpha)\ \forall\ \alpha \in W$

Note: ... have a linear ... $T_W \neq T$ as $W \neq V$.

Theorem 11.1.9: Let T be a linear operator on a finite-dimensional vector space V over a field F.

Let W be a subspace of V invariant under T.Let $B' = \{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ be a basis of W and

$B_1' = \{\alpha_1, \alpha_2, \ldots, \alpha_r, \ldots, \alpha_n\}$ is the basis of V extended from B'.Then $[T]_{B_1'} = \begin{bmatrix} B & C \\ 0 & D \end{bmatrix}$ where B, C and D are block matrices of appropriate sizes.

Proof:$B' = \{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ is a basis of W and $B_1' = \{\alpha_1, \alpha_2, \ldots, \alpha_r, \ldots, \alpha_n\}$ is the basis of V extended from B'.

Since $\alpha_j \in W\ \forall\ 1 \leq j \leq r$ and W is invariant under T

Therefore, $T(\alpha_j) \in W\ \forall\ 1 \leq j \leq r$

$$T(\alpha_j) = \sum_{i=1}^{r} A_{ij}\alpha_i,\ 1 \le j \le r$$

That is,

$$T(\alpha_1) = A_{11}\alpha_1 + A_{21}\alpha_2 + \cdots + A_{r1}\alpha_r + 0 + 0 + \cdots + 0$$
$$T(\alpha_2) = A_{12}\alpha_1 + A_{22}\alpha_2 + \cdots + A_{r2}\alpha_r + 0 + 0 + \cdots + 0$$
$$\vdots$$
$$T(\alpha_r) = A_{1r}\alpha_1 + A_{2r}\alpha_2 + \cdots + A_{rr}\alpha_r + 0 + 0 + \cdots + 0$$
$$T(\alpha_{r+1}) = A_{1,r+1}\alpha_1 + \cdots + A_{r,r+1}\alpha_r + \cdots + A_{n,r+1}\alpha_n$$
$$\vdots$$
$$T(\alpha_n) = A_{1n}\alpha_1 + \cdots + A_{rn}\alpha_r + \cdots + A_{nn}\alpha_n$$

That is,

$$A = \begin{bmatrix} B & C \\ O & D \end{bmatrix}$$

where B, C and D are matrices given by

$$B = \begin{bmatrix} A_{11} & \cdots & A_{1r} \\ \vdots & \ddots & \vdots \\ A_{r1} & \cdots & A_{rr} \end{bmatrix},\ C = \begin{bmatrix} A_{1,r+1} & \cdots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{r\,r+1} & \cdots & A_{rn} \end{bmatrix},$$

$D = \begin{bmatrix} A_{r+1,r+1} & \cdots & A_{r+1,n} \\ \vdots & \ddots & \vdots \\ A_{n\,r+1} & \cdots & A_{nn} \end{bmatrix}$ and O denotes the zero matrix of order $n - r \times r$

Lemma 11.1.10: Let W be an invariant subspace for T. The characteristic polynomial for the restriction operator T_W divides the characteristic polynomial for T. The minimal polynomial for T_W divides the minimal polynomial for T.

Proof: We have done that $B' = \{\alpha_1, \alpha_2, \dots, \alpha_r\}$ be a basis of W and

$B_1' = \{\alpha_1, \alpha_2, \dots, \alpha_r, \dots, \alpha_n\}$ is the basis of V extended from B'.

Then $A = [T]_{B_1'} = \begin{bmatrix} B & C \\ 0 & D \end{bmatrix}$ where B, C and D are block matrices of appropriate sizes.

Clearly, $[T_W]_{B'} = B$

Because of the block form of the matrix

$$det\ (xI - A) = det\ (xI - B)\ det\ (xI - D)$$

That proves the statement about characteristic polynomials.

Note: We used I to represent identity matrices of three different sizes.

For example, A is a matrix of size $n \times n$, so identity matrix used in $xI - A$ is of order $n \times n$, etc.

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.

Remark 11.1.11: We have proved the following results

1. Let T be a linear operator on a finite-dimensional space V. Let $c_1, \dots, c_k$ 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

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

and

$$dim\ W_i = d_i,\ i = 1, \dots, k.$$

$$(iii)\ \dim W_1 + \dim W_2 + \cdots + \dim W_k = \dim V$$

2. The characteristic space associated with characteristic value c_i of T is invariant under T.

Now let W be the subspace spanned by all the characteristic vectors of T.

Then, we know that

$$\dim W = \dim W_1 + \dim W_2 + \cdots + \dim W_k$$

Also, let $B_1, B_2, \dots, B_k$ be the bases of $W_1, W_2, \dots, W_k$ respectively then $\tilde{B} = (B_1, B_2, \dots, B_k)$ is a basis of W.

Let $B' = \{\alpha_1, \alpha_2, \dots \alpha_r\}$ so that the first few α's are from B_1, the next from B_2 and so on. Then

$$T\alpha_i = t_i\alpha_i,\ i = 1, 2, \dots, r$$

where $(t_1, \dots, t_r) = (c_1, c_1, \dots, c_1, c_2, \dots, c_2, \dots c_k, \dots, c_k)$

Each c_i is repeated $\dim W_i$ times.

Now W is invariant under T, since for each $\alpha \in W$, we have

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_r\alpha_r$$

Then

$$T(\alpha) = T(x_1\alpha_1 + x_2\alpha_2 + \cdots + x_r\alpha_r)$$

$$= t_1x_1\alpha_1 + t_2x_2\alpha_2 + \cdots + t_rx_r\alpha_r$$

Choose any other vectors $\alpha_{r+1}, \dots, \alpha_n \in V$ such that $\tilde{B'} = \{\alpha_1, \dots, \alpha_k\}$ is a basis for V.

The matrix of T relative to $\tilde{B'}$, has the block form given by

$$A = \begin{bmatrix} B & C \\ 0 & D \end{bmatrix}$$

and the matrix of the restriction operator T_W relative to the basis B' is

$$B = \begin{bmatrix} t_1 & 0 & \dots & 0 \\ 0 & t_2 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & t_r \end{bmatrix}$$

The characteristic polynomial of B (i.e., of T_W) is

$$g = (x - c_1)^{e_1}(x - c_2)^{e_2} \dots (x - c_k)^{e_k}$$

where $e_i = \dim W_i$.

Further, g divides f, the characteristic polynomial for T.

Therefore, the multiplicity of c_i as a root of f is at least $\dim W_i$.

Remark 11.1.12: From this discussion, it is obvious that T is diagonalizable if and only if $r = n$, that is, if and only if $e_1 + e_2 + \cdots e_k = n$

So, in other words, T is diagonalizable if and only if there are n linearly independent characteristic vectors of T.

Task: Let V be a vector space of dimension 2. Let T be a linear operator on V. Prove that the 1-dimensional T-invariant subspace of V is generated by a characteristic vector of T.

11.2 Reduction to Triangular Form

Definition 11.2.1: 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.

That is,

$$S_T(\alpha; W) = \{g \in F[x] | g(T)\alpha \in W\}$$

Remark 11.2.2: In case, $W = \{0\}$,

$$S_T(\alpha; 0) = \{g \in F[x] | g(T)\alpha = 0\}$$

is called the T −annihilator of α.

Since the operator T will be fixed throughout most discussions, we shall usually drop the subscript T and write $S\ (\alpha\ ;\ W)$

Lemma 11.2.3: 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 $S(\alpha;\ W)$ 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.

Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$

Then $f(T)\beta = (a_0I + a_1T + \cdots + a_nT^n)\beta$

$$= a_0\beta + a_1T\beta + \cdots a_nT^n\beta \in W$$

Thus $f(T)\beta$ is in W for every polynomial f.

Further, we prove that $S(\alpha; W)$ is an ideal of $F[x]$

Let $f,\ g \in S(\alpha; W)$

Then $f(T)\alpha,\ g(T)\alpha \in W$

Since W is a subspace of V.

$$f(T)\alpha - g(T)\alpha \in W$$

Or,

$$(f - g)T\alpha \in W$$

This implies $f - g \in S(\alpha; W)$

Let $h \in F[x]$

Then since W is invariant under T,

$$hf(T)\alpha = h(T)f(T)\alpha \in W$$

Similarly, $fh(T)\alpha \in\ W$.

So that

$$fh,\ hf \in S(\alpha; W)\ \forall\ f \in S(\alpha; W),\ h \in F[x]$$

This implies, $S(\alpha; W)$ is an ideal of $F[x]$.

Note: $\alpha; W)$ is $F[x]$ is principal ideal domain and hence all its ideals are generated by single elements.

Remark 11.2.4: The unique monic generator of the ideal $S(\alpha,\ W)$ 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 $S(\alpha;\ W)$ if and only if g divides f.

Note that the conductor $S(\alpha;\ W)$ always contains the minimal polynomial for T;

Because if h is minimal polynomial for T, then $h(T) = 0$ and hence $h(T)\alpha = 0 \in W$.

hence, every T −conductor of α into W divides the minimal polynomial for T.

Definition 11.2.5: Let V be a finite-dimensional vector space over a field F.Let T a linear operator on V. The linear operator T is called triangulable if there is an ordered basis in which T is represented by a triangular matrix.

Lemma 11.2.6: 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

$$p = (x - c_1)^{r_1} \dots (x - c_k)^{r_k},\ c_i \text{ in } F$$

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

$(a)\alpha$ is not in W;

$(b)(T - cI)\alpha$ is in W, for some characteristic value c of the operator T.

Proof: Since $V \neq W$ and W is a subspace of V.

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.

If g is constant polynomial, then $g(T)\beta \in W$ implies $\beta \in W$.

Since β is not in W, the polynomial g is not constant.

Therefore,

$$g = (x - c_1)^{e_1}(x - c_2)^{e_2} \dots (x - c_k)^{e_k}$$

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 $(T - c_jI)\alpha = (T - c_jI)h(T)\beta = g(T)\beta$ is in W.

Theorem 11.2.7: 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

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

Consider $W_1 = \{0\}$.

By the lemma, there exists $\alpha_1 \in V$ such that α_1 is not in W_1 but $(T - c_iI)\alpha_1$ is in W_1, for some characteristic value c_i of the operator T.

That is, $(T - c_iI)\alpha_1 = 0$

$$T(\alpha_1) = c_i\alpha_1 \dots (1)$$

Now choose W_2 the subspace spanned by α_1.

Then by lemma, there exists $\alpha_2 \in V$ such that α_2 is not in W_2 but $(T - c_jI)\alpha_2$ is in W_2, for some characteristic value c_j of the operator T.

That is, $(T - c_jI)\alpha_2 = a_{12}\alpha_1; a_{12} \in F$

or $T\alpha_2 = a_{12}\alpha_1 + c_j\alpha_2$

By repeated application of the lemma above and renaming the scalars, we shall arrive at an ordered basis $B = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ in which the matrix representing T is upper-triangular.

$$[T]_B = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & a_{22} & a_{23} & \cdots & a_{2n} \\ 0 & 0 & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & a_{nn} \end{bmatrix}$$

and $T\alpha_j$ is in the subspace spanned by $\alpha_1, \ \ldots, \ \alpha_j$.

Conversely, if T is triangulable then there exists a basis $B = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ of V such that $[T]_B$ is upper-triangular.

Let

$$[T]_B = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & a_{22} & a_{23} & \cdots & a_{2n} \\ 0 & 0 & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & a_{nn} \end{bmatrix}$$

Then characteristic polynomial of T is given by

$$(x - a_{11})(x - a_{22}) \ldots (x - a_{nn})$$

which is a product of linear factors. Since minimal polynomial divides characteristic polynomial, so, it is also a product of linear factors.

Corollary 11.2.8: Let F be an algebraically closed field. Then we know that every polynomial can be split into a product of linear factors over F. The minimal polynomial of $n \times n$ matrix over F is a product of linear factors. Hence, every square matrix is similar over F to a triangular matrix.

Example 11.2.9: Let T be a linear operator defined on R^3. Let matrix of T with respect to the standard ordered basis of R^3 is given by

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

Find a basis B such that $[T]_B$ is in the triangular form.

Or equivalently, find an invertible matrix P for which $P^{-1}AP$ is a triangular matrix.

Solution: First we find characteristic values by putting $|A - \lambda I| = 0$

That is,

$$\begin{vmatrix} -\lambda & 1 & 0 \\ 2 & -2-\lambda & 2 \\ 2 & -3 & 2-\lambda \end{vmatrix} = 0$$

$\Rightarrow \lambda(4 - \lambda^2) + 4 - 6\lambda - 2(2 - \lambda) = 0$

$\Rightarrow \lambda^3 = 0$

$\Rightarrow \lambda = 0, 0, 0$

Now we find characteristic vector corresponding to $\lambda = 0$

Let $0 \neq X = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$ be the characteristic vector of A corresponding to $\lambda = 0$.

Then $AX = 0X$ or $AX = 0$ implies,

$$\begin{bmatrix} 0 & 1 & 0 \\ 2 & -2 & 2 \\ 2 & -3 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Applying row operation $R_3 \to R_3 - R_2$, we get,

$$\begin{bmatrix} 0 & 1 & 0 \\ 2 & -2 & 2 \\ 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

This implies, $y = 0$ and $2x - 2y + 2z = 0$

That is, $y = 0, x = -z$

So that $X = \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} x \\ 0 \\ -x \end{bmatrix} = x\begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix}$

Then $\alpha_1 = \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix}$ is the required vector.

Now we wish to find $\{\alpha_2, \alpha_3\}$ so that the set $B = \{\alpha_1, \alpha_2, \alpha_3\}$ is a basis of R^3 such that the matrix $[T; B]$ is an upper triangular matrix.

Consider α_2, by theorem, it can be obtained by the relation

$$A\alpha_2 = c_2\alpha_2 + d_1\alpha_1;\ d_1 \in R$$

Let $\alpha_2 = \begin{bmatrix} x_2 \\ y_2 \\ z_2 \end{bmatrix}$ since $c_2 = 0$,

$$\Rightarrow \begin{bmatrix} 0 & 1 & 0 \\ 2 & -2 & 2 \\ 2 & -3 & 2 \end{bmatrix}\begin{bmatrix} x_2 \\ y_2 \\ z_2 \end{bmatrix} = d_1\begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix}$$

This implies, $y_2 = d_1$

$2x_2 - 2y_2 + 2z_2 = 0$

$\Rightarrow x_2 = y_2 - z_2 = d_1 - z_2$

So, $\begin{bmatrix} x_2 \\ y_2 \\ z_2 \end{bmatrix} = \begin{bmatrix} d_1 - z_2 \\ d_1 \\ z_2 \end{bmatrix} = d_1\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} - z_2\begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix}$

We take $\alpha_2 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$

Now, to find α_3, take $A\alpha_3 = c_3\alpha_3 + d_2\alpha_2 + d_3\alpha_1; d_2, d_3 \in R$

Putting $c_3 = 0$ and $\alpha_3 = \begin{bmatrix} x_3 \\ y_3 \\ z_3 \end{bmatrix}$,

$$A\alpha_3 = d_2\alpha_2 + d_3\alpha_1$$

$$\Rightarrow \begin{bmatrix} 0 & 1 & 0 \\ 2 & -2 & 2 \\ 2 & -3 & 2 \end{bmatrix}\begin{bmatrix} x_3 \\ y_3 \\ z_3 \end{bmatrix} = d_2\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + d_3\begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} y_3 \\ 2x_3 - 2y_3 + 2z_3 \\ 2x_3 - 3y_3 + 2z_3 \end{bmatrix} = \begin{bmatrix} d_2 + d_3 \\ d_2 \\ -d_3 \end{bmatrix}$$

$\Rightarrow y_3 = d_2 + d_3$ and $x_3 - d_2 - d_3 + z_3 = \frac{d_2}{2}$

$\Rightarrow x_3 = \frac{3}{2}d_2 + d_3 - z_3, y_3 = d_2 + d_3, z_3 = z_3$

$$\begin{bmatrix} x_3 \\ y_3 \\ z_3 \end{bmatrix} = \begin{bmatrix} \frac{3}{2} \\ 1 \\ 0 \end{bmatrix} d_2 + \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} d_3 + \begin{bmatrix} -1 \\ 0 \\ 1 \end{bmatrix} z_3$$

Take $\alpha_3 = \begin{bmatrix} \frac{3}{2} \\ 1 \\ 0 \end{bmatrix}$

Then $B = \{\alpha_1, \alpha_2, \alpha_3\}$ is the required basis. That is, $[T : B]$ is an upper triangular matrix $P^{-1}AP$ such that,

$P = \begin{bmatrix} 1 & 1 & \frac{3}{2} \\ 0 & 1 & 1 \\ -1 & 0 & 0 \end{bmatrix}$, $P^{-1} = \begin{bmatrix} 0 & 0 & -1 \\ -2 & 3 & -2 \\ 2 & -2 & 2 \end{bmatrix}$ and $P^{-1}AP = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$.

Example 11.2.10: Let T be a linear operator defined on R^3. Let matrix of T with respect to the standard ordered basis of R^3 is given by

$$A = \begin{bmatrix} 1 & -3 & 3 \\ 0 & -1 & 2 \\ 0 & -3 & 4 \end{bmatrix}$$

Find a basis B such that $[T]_B$ is in the triangular form.

Or equivalently, find an invertible matrix P for which $P^{-1}AP$ is a triangular matrix.

Solution:

$$A = \begin{bmatrix} 1 & -3 & 3 \\ 0 & -1 & 2 \\ 0 & -3 & 4 \end{bmatrix}$$

First, we find characteristic values by putting $|A - \lambda I| = 0$

That is,

$$\begin{vmatrix} 1-\lambda & -3 & 3 \\ 0 & -1-\lambda & 2 \\ 0 & -3 & 4-\lambda \end{vmatrix} = 0$$

$\Rightarrow (1-\lambda)[-(1+\lambda)(4-\lambda)+6] = 0$

$\Rightarrow (1-\lambda)(\lambda^2 - 3\lambda + 2) = 0$

$\Rightarrow \lambda = 1, 1, 2$

Now we find characteristic vector corresponding to $\lambda = 1$

Let $0 \neq X = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$ is the required characteristic vector.

Then $(A - I)X = 0$

$\Rightarrow \begin{bmatrix} 1 & -3 & 3 \\ 0 & -1 & 2 \\ 0 & -3 & 4 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$

Applying $R_2 \to R_2 - \frac{2}{3}R_1, R_3 \to R_3 - R_1$

$\Rightarrow \begin{bmatrix} 0 & -3 & 3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$

$\Rightarrow -3y + 3z = 0$ or $y = z$

So, $\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} x \\ y \\ y \end{bmatrix} = x \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + y \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$

Then $\alpha_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \alpha_2 = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$

To find $\alpha_3 = \begin{bmatrix} x_2 \\ y_2 \\ z_2 \end{bmatrix}$,

$A\alpha_3 = c_3\alpha_3 + d_1\alpha_1 + d_2\alpha_2; d_1, d_2 \in R$

$\Rightarrow (A - c_3 I)\alpha_3 = d_1\alpha_1 + d_2\alpha_2$

$\Rightarrow \begin{bmatrix} -1 & -3 & 3 \\ 0 & -3 & 2 \\ 0 & -3 & 2 \end{bmatrix} \begin{bmatrix} x_2 \\ y_2 \\ z_2 \end{bmatrix} = d_1 \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + d_2 \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$

$\Rightarrow -x_2 - 3y_2 + 3z_2 = d_1, -3y_2 + 2z_2 = d_2$

$\Rightarrow \ -x_2 + z_2 = d_1 - d_2$

$\Rightarrow x_2 = z_2 - d_1 + d_2$

$\Rightarrow y_2 = \dfrac{-d_2 + 2z_2}{3}$

Then $\begin{bmatrix} x_2 \\ y_2 \\ z_2 \end{bmatrix} = \begin{bmatrix} z_2 - d_1 + d_2 \\ \frac{-d_2 + 2z_2}{3} \\ z_2 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \\ 3 \end{bmatrix} \frac{z_2}{3} - \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} d_1 + \begin{bmatrix} 1 \\ -\frac{1}{3} \\ 0 \end{bmatrix} d_2$

Take $\alpha_3 = (3, 2, 3)$

Then $P = \begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 2 \\ 0 & 1 & 3 \end{bmatrix}$ and $P^{-1}AP = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}$.

Consider $B = \{(1,0,0), (0,1,1), (3,2,3)\}$ and $[T; B] = P^{-1}AP$.

Theorem 11.2.11: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

$$p = (x - c_1)(x - c_2) \dots (x - c_k)$$

where $c_1, c_2, \dots, c_k$ are distinct elements of F.

Proof: We have proved 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 the characteristic vectors of T, and suppose $W \neq V$.

By the lemma, there is a vector α not in W and a characteristic value c_j of T such that the vector

$$\beta = (T - c_j I)\alpha$$

lies in W.

Since β is in W, $\beta = \beta_1 + \beta_2 + \dots + \beta_k$ where $T\beta_i = c_i\beta_i$, $1 \le i \le k$ 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

$$q(T)\alpha - q(c_j)\alpha = h(T)(T - c_j I)\alpha = h(T)\beta$$

But $h(T)\beta$ is in W and, since

$$0 = p(T)\alpha = (T - c_j I)q(T)\alpha,$$

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.

Note: There are two ways to check whether an operator T on an $n-$dimensional vector space V over a field F is diagonalizable or not

- The number of linearly independent characteristic vectors of T is n if and only if T is diagonalizable.
- T is diagonalizable if and only if its minimal polynomial is a product of distinct linear factors.
- T is triangulable if and only if its minimal polynomial is a product of linear factors.
- Every diagonal matrix is a triangular matrix as well so, every diagonalizable operator (matrix) is triangulable as well.

Every triangulable matrix may not be diagonalizable as seen in the example $A = \begin{bmatrix} 0 & 1 & 0 \\ 2 & -2 & 2 \\ 2 & -3 & 2 \end{bmatrix}$ is triangulable but not diagonalizable.

Summary

- invariant subspaces of a vector space under a linear operator are defined.
- important results related to invariant subspaces are proved.
- T −conductor of an element α into an invariant subspace W of V is defined.
- the concept of triangulable operators is explained with the help of examples.

Keywords

- invariant subspaces
- linear operator
- T −conductor of an element
- Triangulable operator
- Triangulation of a linear operator

Self Assessment

1. Let T be a linear operator on a finite-dimensional vector space V over a field F. Then one-dimensional invariant subspace of V is generated by

A. Any non-zero element of V
B. A characteristic value of T
C. A characteristic vector of T
D. Unity of field F

2. The set $W = \{(x, 0) | x \in \mathbb{R}\}$ be a subspace of $V = \mathbb{R}^2$. Consider the operator T on V as $T(x, y) = (2x, 0)$. Then

A. W is an invariant subspace of V under linear operator T
B. W is a subspace of V but not invariant under T
C. W is not a subspace of V
D. T is not a linear operator

3. The set $W = \{(x, 0) | x \in \mathbb{R}\}$ be a subspace of $V = \mathbb{R}^2$. Consider the operator T on V as $T(x, y) = (2x + 1, 0)$. Then

A. W is an invariant subspace of V under linear operator T
B. W is a subspace of V but not invariant under T
C. W is not a subspace of V
D. T is not a linear operator

4. Let T be a linear operator on a finite-dimensional vector space V over a field F. Consider $U = f(T)$; where $f(T)$ is a polynomial in T. Then

A. $Ker\ U$ is invariant under T and U both
B. $Ker\ U$ is invariant under T but not under U
C. $Ker\ U$ is invariant under U but not under T
D. $Ker\ U$ is invariant neither under T nor under U

5. True/False The space of characteristic vectors associated with some characteristic value of a linear operator T on a finite-dimensional space V is always invariant under T.

A. True
B. False

6. Let $T: \mathbb{R}^2 \to \mathbb{R}^2$ as $T(x,y) = (-y,x)$. Let W be a non-zero subspace of $\mathbb{R}^2$ and it is invariant under T. Then $dim W$ is
A. $= 0$
B. $= 1$
C. $= 2$
D. ≤ 2

7. Let T be a linear operator defined on a finite-dimensional vector space V over a field F. Let W be a subspace of V invariant under T.
A. The restriction map T_W is defined and $T_W = T$
B. The restriction map T_W is defined and $T_W(x) = T(x)\ \forall x \in V$
C. The restriction map T_W is not defined
D. The restriction map T_W is defined and $T_W(x) = T(x)\ \forall x \in W$

8. Let T be a linear operator defined on a finite-dimensional vector space V over a field F. Let W be a subspace of V invariant under T. Which of the following is not true?
A. Characteristic polynomial of T is divisible by characteristic polynomial of T_W
B. Characteristic polynomial of T is divisible by minimal polynomial of T_W
C. Minimal polynomial of T is divisible by characteristic polynomial of T_W
D. Minimal polynomial of T is divisible by minimal polynomial of T_W

9. Let T be a linear operator defined on a finite-dimensional vector space V over a field F. Let W be a subspace of V invariant under T. Let B' is a basis of W and B is a basis of V by extending B' such that $[T]_B = A$ and $[T_W]_{B'} = A'$ then
A. A' is a diagonal matrix with the same diagonal entries as A
B. A' is a minor of A
C. A' is a square submatrix of A
D. $A' = A$

10. Let $T: P_3 \to P_3$ be defined as differentiation operator. Consider the subspace $W = P_2$ of P_3 then for standard bases B and B' of P_3 and P_2 respectively, $[T]_B$ and $[T_W]_{B'}$ are

A: $[T]_B = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ and $[T_W]_{B'} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$

B: $[T]_B = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ and $[T_W]_{B'} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

C: $[T]_B = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}$ and $[T_W]_{B'} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

D: $[T]_B = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ and $[T_W]_{B'} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

11. Choose the correct statement
A. Characteristic values of every diagonalizable operator are always distinct
B. Characteristic values of every triangulable operator are always distinct
C. Every diagonalizable operator is always triangulable
D. Every triangulable operator is always diagonalizable

12. Let T be a linear operator on a finite-dimensional vector space over a field F. Let W be an invariant subspace of V. Then if $\beta \in V$ such that $\beta \notin W$ and $g(T)\beta \in W$ for some non-zero polynomial $g \in F[x]$. Then

A. deg $g = 0$
B. deg $g \geq 0$
C. deg $g > 0$
D. None of the options is correct

13. Which of the following is not a sufficient condition for an operator T over R^3 to be triangulable?
A. All the characteristic values of T are distinct
B. The characteristic polynomial of T is a product of linear factors
C. The minimal polynomial of T is a product of linear factors
D. The degree of the minimal polynomial of T is 2.

14. A square matrix A of order n is triangulable but not diagonalizable. Then choose the correct statement.
A. Characteristic polynomial of A is a product of distinct linear factors
B. Minimal polynomial of A is a product of distinct linear factors
C. Number of linearly independent characteristic vectors of T is equal to n
D. Roots of the minimal polynomial of T are not all distinct

15. Let minimal polynomial of an operator T on C^4 is $x(x^2 - 1)$. Then
A. T is diagonalizable
B. T is triangulable but not diagonalizable
C. T is neither diagonalizable nor triangulable
D. The given information is not sufficient to decide if the operator is diagonalizable or not

Answers for Self Assessment

1.	C	2.	A	3.	D	4.	A	5.	A
6.	C	7.	D	8.	C	9.	C	10.	A
11.	C	12.	C	13.	D	14.	D	15.	A

Review Questions

1. Let T be the linear operator on R^2, the matrix of which in the standard ordered basis is given by $A = \begin{bmatrix} 1 & -1 \\ 2 & 2 \end{bmatrix}$. Prove that the only subspaces of R^2 invariant under T are R^2 and the zero subspace.
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.
3. Show that for the matrix $A = \begin{bmatrix} 2 & -2 & -4 \\ -1 & 3 & 4 \\ 1 & -2 & -3 \end{bmatrix}$, $A^2 = A$.
4. Find the characteristic polynomial of the matrix A given in Problem 3. Also, check whether A is triangulable or not? If yes, find the corresponding triangular form.
5. Show that every matrix A such that $A^2 = A$ is similar to a diagonal matrix.

Further Readings

- Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge

universitypress

- Topics in algebra by I.N. Hartstein, Wiley
- Abstract algebra by David S Dummit and Richard M Foote, Wiley

Weblinks

- https://nptel.ac.in/courses/111/102/111102009/
- https://nptel.ac.in/courses/111/105/111105112/#

Dr. Isha Garg, Lovely Professional University

Unit 12: Nilpotent Operators and Invariants of Nilpotent Operators

CONTENTS

Objective

After this lecture, you will be able to

- define nilpotent operators and observe that all its characteristic values are 0,
- understand the canonical form associated with the nilpotent matrices,
- study the invariant factors of a nilpotent transformation,
- understand how to find the canonical form and invariance factors of a nilpotent operator on a finite-dimensional vector space.

Introduction

In this unit, you will be introduced to a special class of operators called nilpotent operators. The structure of characteristic values of nilpotent operators will be discussed. Further, we will discuss invariant factors of nilpotent operators and the method to find them. All the concepts will be elaborated with the help of examples.

12.1 Nilpotent Operators and Index of Nilpotency

Definition 12.1.1: Let V be an n −dimensional vector space over a field F. Let T be a linear operator on V, then T is called nilpotent operator if and only if $T^m = 0$ for some positive integer m.

Note An operator T on the vector space of dimension 1 is nilpotent if and only if $T = 0$)

Remark 12.1.2 Set of nilpotent operators is not a vector space.

Proof: Let $V = R^2$

Let T_1 and T_2 be two operators on R^2 given by $T_1(x, y) = (0, x)$ and $T_2(x, y) = (y, 0)$

$T_1(x, y) = (0, x)$

$T_1^2(x, y) = T_1(0, x) = (0, 0)$

This implies, $T_1^2 = 0$

Again, $T_2^2(x, y) = T_2(y, 0) = (0, 0)$

Thus, $T_2^2 = 0$

But

$$(T_1 + T_2)(x, y) = T_1(x, y) + T_2(x, y)$$
$$= (0, x) + (y, 0) = (y, x)$$

Consider

$$(T_1 + T_2)^2 = (T_1 + T_2)((T_1 + T_2)(x, y))$$
$$= (T_1 + T_2)(y, x)$$
$$= T_1(y, x) + T_2(y, x)$$
$$= (0, y) + (x, 0) = (x, y)$$

This implies, $(T_1 + T_2)^k \neq 0 \ \forall \ k$

So, the set of nilpotent operators is not closed under addition and hence it is not a vector space.

Remark 12.1.3: Power of a nilpotent operator is again a nilpotent operator.

Proof: Let $T: V \to V$ be a nilpotent operator. Then there exists natural number k such that $T^k = 0$

For any positive integer m, consider T^m;

Then $(T^m)^k = T^{km} = (T^k)^m = 0$

Hence, T^m is nilpotent operator.

Remark 12.1.4: For a nilpotent operator T and any polynomial $f(x) = a_0x + a_1x^2 + \cdots + a_nx^n$, $f(T)$ is also nilpotent.

Proof: Let $T: V \to V$ be a nilpotent operator. Then there exists natural number k such that $T^k = 0$

Consider $f(x) = a_1x + a_2x^2 + \cdots + a_nx^n$

Then

$$f(T) = a_1T + a_2T^2 + \cdots + a_nT^n$$
$$= T(a_1I + a_2T + \cdots + a_nT^{n-1})$$

Consider $\left(f(T)\right)^k = T^k(a_1I + a_2T + \cdots + a_nT^{n-1})^k = 0$

Theorem 12.1.5: Characteristic values of a nilpotent operator are all zero.

Proof: Let T be a nilpotent operator on V.

Then $T^m = 0$ for some positive integer m.

Consider $f(x) = x^m$ then $f(x)$ is the annihilating polynomial of T.

Since minimal polynomial of T is a divisor of $f(x)$.

Let minimal polynomial of T is $p(x)$.

Then $p(x) = x^k; k \leq m$

If $k = 0$

Then $p(x) = 1$ this implies $p(T) = I$, which is not possible as $p(T) = 0$.

So, $k \geq 1$

Therefore, the minimal polynomial has only one root 0.

So, T has only one characteristic value 0.

Theorem 12.1.6: Nilpotent operator is always triangulable.

Proof: As seen in Theorem 12.1.5, minimal polynomial $p(x)$ of T is given by $p(x) = x^k; k \geq 1$

That is, the minimal polynomial of T is a product of linear factors.

Hence, T is a triangulable operator.

Remark 12.1.7:A nilpotent operator T is diagonalizable if and only if it is a zero operator.

Proof: Let T is a nilpotent operator on an $n-$dimensional vector space V over a field F.

Then minimal polynomial $p(x)$ of T is

$$p(x) = x^k,\ 1 \le k \le n$$

We know that T is diagonalizable if and only if its minimal polynomial is a product of distinct linear factors.

That is, $p(x) = x$

This implies, $p(T) = T$

Also, $p(x)$ is minimal polynomial of T implies,

$$p(T) = T = 0$$

So, T is diagonalizable if and only if T = 0.

Note:A non-zero nilpotent operator is triangulable but never diagonalizable.

Lemma 12.1.8: If$V = V_1 \oplus V_2 \oplus \dots \oplus V_k$, where each subspace V_i is of dimension n_i and is invariant under T, where T is a linear operator on V, then a basis of V can be found so that the matrix of T in this basis is of the form

$$\begin{bmatrix} A_1 & 0 & \dots & 0 \\ 0 & A_2 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & A_k \end{bmatrix}$$

where each A_i is an $n_i \times n_i$ matrix and is the matrix of the linear transformation induced by T on V_i.

Proof: Let us choose a basis of V as follows:

Let $B_1 = \left\{v_1^{(1)}, \dots, v_{n_1}^{(1)}\right\}$ is a basis of V_1,

$B_2 = \left\{v_1^{(2)}, \dots, v_{n_2}^{(2)}\right\}$ is a basis of V_2, and so on.

Then basis B of V is $\left\{v_1^{(1)}, \dots, v_{n_1}^{(1)}, v_1^{(2)}, \dots, v_{n_2}^{(2)}, \dots, v_1^{(k)}, \dots, v_{n_k}^{(k)}\right\}$

Consider $v_i^{(1)}; 1 \le i \le n_1$

Then since $v_i^{(1)} \in V_1$ and V_1 is invariant under T.

So, the restriction map T_{V_1} is defined and $T\left(v_i^{(1)}\right) \in V_1$ and B_1 is a basis of V_1.

So,

$$T\left(v_i^{(1)}\right) = \sum_{j=1}^{n_1} \alpha_{ji}^{(1)} v_j^{(1)}$$

Similarly,

Consider $v_i^{(2)}; 1 \le i \le n_2$

Then since $v_i^{(2)} \in V_2$ and V_2 isinvariant under T.

So, the restriction map T_{V_2} is defined and $T\left(v_i^{(2)}\right) \in V_2$ and B_2 is a basis of V_2.

So,

$$T\left(v_i^{(2)}\right) = \sum_{j=1}^{n_2} \alpha_{ji}^{(2)} v_j^{(2)}$$

and so on…

Then we get

$$[T]_B = \begin{bmatrix} \alpha_{11}^{(1)} & \cdots & \alpha_{1n_1}^{(1)} & & & & & & & \\ \vdots & \ddots & \vdots & & & & & & & \\ \alpha_{n_1 1}^{(1)} & \cdots & \alpha_{n_1 n_1}^{(1)} & & & & & & & \\ & & & \alpha_{11}^{(2)} & \cdots & \alpha_{1n_2}^{(2)} & & & & \\ & & & \vdots & \ddots & \vdots & & & & \\ & & & \alpha_{n_2 1}^{(2)} & \cdots & \alpha_{n_2 n_2}^{(2)} & & & & \\ & & & & & & \ddots & \alpha_{11}^{(k)} & \cdots & \alpha_{1n_k}^{(k)} \\ & & & & & & & \vdots & \ddots & \vdots \\ & & & & & & & \alpha_{n_k 1}^{(k)} & \cdots & \alpha_{n_k n_k}^{(k)} \end{bmatrix}$$

That is,

$$[T]_B = \begin{bmatrix} A_1 & 0 & \dots & 0 \\ 0 & A_2 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & A_k \end{bmatrix}$$

where,

$$A_i = \begin{bmatrix} \alpha_{11}^{(i)} & \cdots & \alpha_{1n_i}^{(i)} \\ \vdots & \ddots & \vdots \\ \alpha_{n_i 1}^{(i)} & \cdots & \alpha_{n_i n_i}^{(i)} \end{bmatrix}$$

is the $n_i \times n_i$ matrix that is,

$$A_i = [T_{V_i}]_{B_i}$$

Lemma 12.1.9: If T is a linear operator on an $n-$ dimensional vector space V over F such that T is nilpotent, then

$$\alpha_0 + \alpha_1 T + \cdots + \alpha_n T^m,$$

where the $\alpha_i \in F$, is invertible if $\alpha_0 \neq 0$.

Proof: Let S be a linear operator on an $n-$dimensional vector space V.

First, we prove that if S is nilpotent and $\alpha_0 \neq 0$, $\alpha_0 \in F$, then $S + \alpha_0$ is invertible.

Since S is nilpotent, there exists some positive integer r such that $S^r = 0$

Consider

$$(\alpha_0 + S)\left(\frac{1}{\alpha_0} - \frac{S}{\alpha_0^2} + \frac{S^2}{\alpha_0^3} + \cdots + (-1)^{r-1}\frac{S^{r-1}}{\alpha_0^{r}}\right) = I + \left(\frac{S}{\alpha_0} - \frac{S}{\alpha_0}\right) + \left(\frac{S^2}{\alpha_0^2} - \frac{S^2}{\alpha_0^2}\right) + \cdots + (-1)^{r-1}\frac{S^r}{\alpha_0^r}$$

$$= I + \left(\frac{S}{\alpha_0}\right.$$

$$= I$$

This implies,

$\alpha_0 + S$ is invertible.

Let $S = \alpha_1 T + \cdots + \alpha_n T^m$

Since T is nilpotent then S is also nilpotent

Thus, for any

$$\alpha_0 \neq 0,\ \alpha_0 \in F,$$

$\alpha_0 + S$ is invertible.

Notation:M_t denote the $t \times t$ matrix all of whose entries are 0 except on the super-diagonal, where they are all 1's.

$$\begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & & & & & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 0 & \dots & 0 & 0 \end{bmatrix}$$

Definition 12.1.10: If T is a linear operator on an n −dimensional vector space V over F.

If T is nilpotent, then the smallest positive integer k for which $T^k = 0$, is called the index of nilpotency.

That is, if k is the index of nilpotency of T then $T^k = 0$, but $T^m \neq 0$ for all $m < k$.

Example 12.1.11: Let T be a linear operator on R^3 given by

$$T(x, y, z) = (0, x, y)$$

then T is nilpotent.

Solution: Given that

$$T(x, y, z) = (0, x, y)$$

Then

$$T^2(x, y, z) = T(T(x, y, z))$$

$$= T(0, x, y)$$

$$= (0, 0, x)$$

$$\neq (0, 0, 0)$$

Further,

$$T^3(x, y, z) = T(T^2(x, y, z))$$

$$= T(0, 0, x)$$

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

Hence, $T^3 = 0$

This implies, T is a nilpotent operator with index of nilpotency 3.

Task:

1. Let $A = \begin{bmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & 0 \end{bmatrix}$. Check whether A is nilpotent or not. If yes, find its index of nilpotency.
2. Find a nilpotent operator on R^3 with an index of nilpotency 2.

12.2 Invariant of Nilpotent Transformation

Theorem 12.2.1: If T is a linear operator on an n −dimensional vector space V over the field F such that T is a nilpotent operator with the index of nilpotency n_1, then a basis of V can be found such that the matrix of T in this basis has the form

$$\begin{bmatrix} M_{n_1} & & & \\ & M_{n_2} & & \\ & & \ddots & \\ & & & M_{n_r} \end{bmatrix}$$

where $n_1 \geq n_2 \geq \ldots \geq n_r$ and where $n_1 + n_2 + \cdots + n_r = \dim V$.

Index of nilpotency of T is n_1.

This implies, $T^{n_1} = 0$ but $T^{n_1 - 1} \neq 0$

So, there exists $v \in V$ such that $T^{n_1 - 1}v \neq 0$ ... (1)

T is a linear transformation and it is nilpotent.

Claim 1: The vectors $\{v, Tv, T^2v, \ldots, T^{n_1-1}v\}$ are linearly independent over F.

Suppose

$$\alpha_1 I(v) + \alpha_2 Tv + \alpha_3 T^2 v + \cdots + \alpha_{n_1-1} T^{n_1-1} v = 0 \ldots (2)$$

If α_i are not all zero, then there exists some $\alpha_s \neq 0$ and s is the least positive integer for which $\alpha_s \neq 0$

(1) becomes,

$$\alpha_s T^{s-1} v + \alpha_{s+1} T^s v + \cdots + \alpha_{n_1-1} T^{n_1-1} v = 0$$

That is,

$$T^{s-1}\left(\alpha_s + \alpha_{s+1} T + \cdots + \alpha_{n_1-1} T^{n_1-s}\right) v = 0 \ldots (3)$$

T is nilpotent and $\alpha_s \neq 0$

By lemma

$\alpha_s + \alpha_{s+1} T + \cdots + \alpha_{n_1-1} T^{n_1-s}$ is invertible.

This implies, $T^{s-1} v = 0$

For $s < n_1$

$$T^{n_1-1} v = T^{n_1-s+s-1} v$$

$$= T^{n_1-s}\left(T^{s-1} v\right) = 0$$

$T^{n_1-1} v = 0$ which is a contradiction to (1)

So, our supposition was wrong.

Therefore, $\alpha_i = 0 \ \forall \ i$

Hence, $\{v, Tv, T^2 v, \ldots, T^{n_1-1} v\}$ is linearly independent.

So, Claim 1 is established.

Let V_1 be the subspace of V spanned by B where $B = \{T^{n_1-1} v, T^{n_1-2} v, \ldots, Tv, v\}$.

We have proved in claim 1 that B is linearly independent and B spans V_1. Let $L(B)$ denotes the linear span of B. Then $V_1 = L(B)$

Hence, B is a basis of V_1.

Claim 2: V_1 is invariant under T.

$$\forall \ \alpha \in V_1 = L(B)$$

This implies,

$$\alpha = \sum_{i=0}^{n_1-1} \beta_i T^i(v); \ \beta_i \in F$$

So that

$$T(\alpha) = T\left(\sum_{i=0}^{n_1-1} \beta_i T^i(v)\right) = \sum_{i=0}^{n_1-1} \beta_i T^{i+1}(v)$$

Since $T^{n_1} = 0$

$$= \sum_{i=0}^{n_1-2} \beta_i T^{i+1}(v) \ \in L(B) = V_1$$

So, $T(\alpha) \in V_1 \ \forall \ \alpha \in V_1$

Therefore, V_1 is invariant under T

Claim 3: $\left.T_{V_1}\right]_B = M_{n_1}$

Consider T_{V_1} that is, the restriction of T on V_1.

By the definition of restriction map,

$T_{V_1}(x) = T(x) \ \forall \ x \in V_1$

$T_{V_1}\left(T^{n_1-1}(v)\right) = T\left(T^{n_1-1}(v)\right) = T^{n_1}(v) = 0$

$T_{V_1}(T^{n_1-2}(v)) = T(T^{n_1-2}(v)) = T^{n_1-1}(v)$

⋮

$T_{V_1}(T(v)) = T(T(v)) = T^2(v)$

$T_{V_1}(v) = T(v)$

Consider $B = \{T^{n_1-1}v, T^{n_1-2}v, \ldots, Tv, v\}$.

$T_{V_1}(T^{n_1-1}(v)) = 0 = 0T^{n_1-1}v + 0T^{n_1-2}v + \cdots + 0Tv + 0v$

$T_{V_1}(T^{n_1-2}(v)) = T^{n_1-1}(v) = 1T^{n_1-1}v + 0T^{n_1-2}v + \cdots + 0Tv + 0v$

⋮

$T_{V_1}(T(v)) = T^2(v) = 0T^{n_1-1}v + 0T^{n_1-2}v + \cdots 1T^2v + 0Tv + 0v$

$T_{V_1}(v) = T(v) = 0T^{n_1-1}v + 0T^{n_1-2}v + \cdots + 1Tv + 0v$

So,

$$T_{V_1}\big]_B = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & & & & & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ 0 & 0 & 0 & \ldots & 0 & 0 \end{bmatrix} = M_{n_1}$$

Claim 4: If $u \in V_1$ is such that $T^{n_1-k}u = 0$ where $0 < k \le n_1$, then $u = T^k u_0$ for some $u_0 \in V_1$

Since $u \in V_1 = L(B)$

Therefore, there exist $\alpha_1, \alpha_2, \ldots, \alpha_{n_1} \in F$ such that

$$u = \sum_{i=1}^{n_1} \alpha_i T^{i-1}(v) \ldots (4)$$

Since $T^{n_1-k}u = 0$

$$T^{n_1-k}\left(\sum_{i=1}^{n_1} \alpha_i T^{i-1}(v)\right) = 0$$

This implies,

$$\sum_{i=1}^{n_1} \alpha_i T^{n_1-k+i-1}(v) = 0$$

Or,

$$\sum_{i=1}^{n_1} \alpha_i T^{n_1-1-k+i}(v) = 0$$

Since $T^{n_1} = 0$,

So, we get

$$\sum_{i=1}^{k} \alpha_i T^{n_1-1-k+i}(v) = 0$$

Consider $B_1 = \{T^{n_1-k}(v), T^{n_1-k+1}(v), \ldots, T^{n_1-2}(v), T^{n_1-1}v\}$

Then B_1 is contained in B.

Hence, B_1 is linearly independent.

So, $\alpha_i = 0 \;\forall\; 1 \le i \le k$

Then from (4),

$$u = \sum_{i=k+1}^{n_1} \alpha_i T^{i-1}(v)$$

$$= T^k\left(\sum_{i=1}^{n_1} \alpha_{k+i} T^{i-1}(v)\right)$$

$$= T^k u_0$$

where $u_0 = \sum_{i=1}^{n_1} \alpha_{k+i} T^{i-1}(v) \in L(B) = V_1$

Claim 5: There exists a subspace W of V, invariant under T such that $V = V_1 \oplus W$.

Let W be a subspace of V, of largest possible dimension such that

(i) $V_1 \cap W = \{0\}$

(ii) W is invariant under T.

We show that $V = V_1 + W$

If $V \neq V_1 + W$

V_1 and W both are subspaces of V.

So, $V_1 + W$ is a subspace of V and hence,

$$V_1 + W \subset V$$

There exists $z \in V$ such that $z \notin V_1 + W$

Since $T^{n_1} = 0$, there exists integer k, $0 < k \leq n_1$ such that

$$T^k z \in V_1 + W$$

and

$$T^i z \notin V_1 + W \text{ for } i < k$$

$T^k z \in V_1 + W$ for some $0 < k \leq n_1$

This implies,

$$T^k z = u + w;\ u \in V_1,\ w \in W$$

Consider

$$T^{n_1} z = T^k(T^{n_1-k} z)$$

$$= (T^{n_1-k})(T^k z)$$

$$= T^{n_1-k}(u + w)$$

$$= T^{n_1-k} u + T^{n_1-k} w$$

Since $T^{n_1} = 0$

So, we get,

$$T^{n_1-k} u + T^{n_1-k} w = 0$$

Since both V_1 and W are invariant under T

Therefore,

$$T^{n_1-k} u \in V_1$$

and

$$T^{n_1-k} w \in W$$

That is,

$$T^{n_1-k} u = -T^{n_1-k} w \in V_1 \cap W = \{0\}$$

By Claim (4)

$u = T^k u_0$ where $u_0 \in V_1$

Hence,

$$T^k z = u + w = T^k u_0 + w$$

Let $z_1 = z - u_0$

Then

$$T^k z_1 = T^k z - T^k u_0 = w \in W$$

Then

$$T^k z_1 = T^k z - T^k u_0 = w \in W$$

For $m \geq k$

$$T^m z_1 = T^{m-k}(T^k z_1) = T^{m-k}(w) \in W$$

For $i < k$

$$T^i z_1 = T^i(z - u_0) = T^i z - T^i(u_0)$$

Since k is the least positive integer for which $T^k z_1 \in V_1 + W$

and $i < k$

$$T^i z_1 \notin V_1 + W$$

So, $T^i z_1 - T^i u_0 \notin V_1 + W$

Let W_1 be the subspace of V spanned by W and $z_1, Tz_1, \ldots, T^{k-1}z_1$

Since $z_1 \notin W$ and $W \subset W_1$

Therefore, $\dim W < \dim W_1$

Since $T^k z_1 \in W$ ... (5) and W is invariant under T

This implies, W_1 is invariant under T.

Also, W is a maximal invariant subspace of V such that $V_1 \cap W = \{0\}$ and W is properly contained in W_1.

So, $V_1 \cap W_1 \neq \{0\}$

There exists some element

$$x = w_0 + \alpha_1 z_1 + \alpha_2 T z_1 \ldots + \alpha_k T^{k-1} z_1 \neq 0$$

If $\alpha_i = 0 \; \forall \; i$, then

$$x = w_0 \in W$$

So, $x \in V_1 \cap W = \{0\}$

This implies, $x = 0$

But $x \neq 0$

So, we arrive at a contradiction.

That is, $\alpha_i's$ are not all zero.

Let α_s be the first non-zero α_i. That is, $\alpha_i = 0 \; \forall \; i < s$ and $\alpha_s \neq 0$.

Then

$$x = w_0 + \alpha_1 z_1 + \alpha_2 T z_1 \ldots + \alpha_k T^{k-1} z_1$$

$$= w_0 + \alpha_s T^{s-1} z_1 + \alpha_{s+1} T^s z_1 \ldots + \alpha_k T^{k-1} z_1$$

$$= w_0 + T^{s-1}(\alpha_s + \alpha_{s+1} T + \cdots + \alpha_k T^{k-s}) z_1 \in V_1$$

Since $\alpha_s \neq 0$

By lemma, $\alpha_s + \alpha_{s+1} T + \cdots + \alpha_k T^{k-s}$ is invertible.

Let R be the inverse of $\alpha_s + \alpha_{s+1} T + \cdots + \alpha_k T^{k-s}$.

Then R is also a polynomial in T

W and V_1 are invariant under T implies, W and V_1 are invariant under R.

Consider

$$w_0 R + T^{s-1} z_1 \in V_1 R \subset V_1$$

Again,

$$T^{s-1} z_1 \in V_1 + wR \subset V_1 + W$$

Since $s - 1 < k$

We arrive at a contradiction to the choice of k.

So, our supposition was wrong.

$$V_1 + W = V$$

Also, since $V_1 \cap W = \{0\}$

Therefore,

$$V = V_1 \oplus W$$

Proof of theorem:

$V = V_1 \oplus W$ where W is invariant under T.

Using basis $B = \{T^{n_1-1}v,\ T^{n_1-2}v, \dots, Tv,\ v\}$ of V_1 as taken in Claim 1.

By Claim 3, we get, $[T_{V_1}; B] = M_{n_1}$

This implies,

$$[T; B] = \begin{bmatrix} [T_{V_1}; B] & 0 \\ 0 & A_2 \end{bmatrix}$$

$$= \begin{bmatrix} M_{n_1} & 0 \\ 0 & A_2 \end{bmatrix}$$

where A_2 is matrix of T_2 that is a linear transformation of T induced on W.

Since $T^{n_1} = 0$

Also, $T_2(x) = T(x)\ \forall x \in W$

This implies, $T_2^{n_2} = 0$ for some $n_2 \leq n_1$

Repeating the same process on T_2 and W, we get the matrix,

$$\begin{bmatrix} M_{n_1} & & & \\ & M_{n_2} & & \\ & & \ddots & \\ & & & M_{n_r} \end{bmatrix}$$

where $n_1 \geq n_2 \geq \dots \geq n_r$ and $n_1 + n_2 + \cdots + n_r = \dim V$

Remark:

- The integers $n_1, n_2, \dots, n_r$ are called invariant factors of T.
- Taking $B = \{T^{n_1-1}v, T^{n_1-2}v, \dots, Tv, v\}$,

we get the matrix $[T_{V_1}; B] = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & & & & & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 0 & \dots & 0 & 0 \end{bmatrix}$

But some authors take

$$B = \{v, Tv, \dots, T^{n_1-2}v, T^{n_1-1}v\}$$

and then the matrix obtained is

$$[T_{V_1}; B] = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Any approach can be used.

Example 12.2.2: Let $T: R^3 \to R^3$ be such that the matrix of linear operator T with respect to the standard basis B is given by

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

Find the corresponding form as

$$\begin{bmatrix} M_{n_1} & & & \\ & M_{n_2} & & \\ & & \ddots & \\ & & & M_{n_r} \end{bmatrix}$$

where $n_1 \geq n_2 \geq \ldots \geq n_r$ and $n_1 + n_2 + \cdots + n_r = \dim V$. Also, find the basis corresponding to which $\left.T_{V_1}\right]_B = M_{n_1}$.

Proof:

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

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

Since $A^2 = 0$, index of nilpotency of $A = n_1 = 2$

Now, $n_1 \geq n_2 \geq \cdots$ such that $n_1 + n_2 + \cdots = 3$

Since $n_1 = 2, n_2 = 1$

Then the corresponding form is $\begin{bmatrix} M_2 & \\ & M_1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$

We choose v such that $Tv \neq 0$

Take $v = (0, 1, 0)$, $Tv = (1, 0, 0)$

Then $B = \{(1, 0, 0), (0, 1, 0)\}$ is the required basis and $\left.T_{V_1}\right]_B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

Summary

- nilpotent operators are defined.
- characteristic values of nilpotent operators are obtained.
- The canonical form associated with the nilpotent matrices is explained.
- The invariant factors of a nilpotent transformation are defined.
- Examples are given tounderstand how to find the canonical form and invariance factors of a nilpotent operator on a finite-dimensional vector space.

Keywords

- Nilpotent operators
- Characteristic values of a nilpotent operator
- The canonical form of a nilpotent operator
- Invariant factors of a nilpotent operator

Self Assessment

1. An operator T on the field of real numbers is nilpotent. Then the index of nilpotency of T is

A. $= 1$
B. > 1
C. $= 0$
D. Not defined

2. Let T be a non-zero nilpotent linear operator on R^2. Then its index of nilpotency is

A. < 2

B. = 2
C. = 1
D. = 0

3. Let T and U are two nilpotent operators on a finite-dimensional vector space V over a field F. Then choose the correct statement
A. $T+U$ is always nilpotent where $(T+U)x = Tx + Ux\ \forall\ x \in V$
B. $T-U$ is always nilpotent where $(T-U)x = Tx - Ux\ \forall\ x \in V$
C. TU is always nilpotent where $(TU)x = (Tx)(Ux)\ \forall\ x \in V$
D. None of the above options is correct

4. Let T be a nilpotent operator. Then which of the following is not nilpotent operator
A. T^2
B. $2T$
C. $2T+T^2$
D. $2T+T^2-1$

5. Let T be a linear operator on R^3 defined as $T(x,y,z) = (0,x,y)$. Then T is
A. Not nilpotent
B. Nilpotent of order 1
C. Nilpotent of order 2
D. Nilpotent of order 3

6. : Let V be the vector space of all polynomials of degree less than or equal to 3. Let D be the differentiation operator defined on V. Then D is the nilpotent operator with index of nilpotency
A. 1
B. 2
C. 3
D. 4

7. Which of the following operator is nilpotent on R^3
A. $T(x,y,z) = (2x,y,z)$
B. $T(x,y,z) = (2x,2y,z)$
C. $T(x,y,z) = (0,0,x)$
D. $T(x,y,z) = (0,0,z)$

8. Let T be a nilpotent transformation. Then all the eigenvalues of T are
A. Distinct
B. Equal but non-zero
C. Equal and all zero
D. Purely imaginary

9. A non-zero nilpotent operator is
A. Always diagonalizable
B. Always triangulable but never diagonalizable
C. Never triangulable
D. May or may not be diagonalizable

10. Which of the following is not a nilpotent operator on R^4?
A. $T(x,y,z,w) = (2w,2z,0,0)$
B. $T(x,y,z,w) = (0,0,2x,2y)$
C. $T(x,y,z,w) = (2z,2w,2x,0)$
D. $T(x,y,z,w) = (0,2z,0,0)$

11. Let $n_1, n_2, \ldots, n_r$ are all the invariant factors of a linear operator T on an n −dimensional vector space V over a field F. Then

A. $n_1 + n_2 + \cdots + n_r = n$
B. $n_1 n_2 \ldots n_r = n$
C. $n_1 = n$
D. $n_1 < n_2 < \cdots < n_r$

12. M_2 is equal to

A: $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

B: $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$

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

D: $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

13. Let T be a nilpotent linear operator on an n −dimensional vector space V over a field F with index of nilpotency k. Consider a vector v such that $T^{k-1}v \neq 0$. Consider the sets $A = \{v, Tv, T^2v, \ldots, T^{k-1}v\}$ and $B = \{v, Tv, T^2v, \ldots, T^kv\}$. Then

A. A is linearly independent and B is linearly dependent
B. A and B both are linearly independent
C. A and B both are linearly dependent
D. A is linearly dependent and B is linearly independent

14. Let T be a linear operator on a vector space V over a field F. Let W be a maximal invariant subspace of V under T. Let W_1 is any subspace of V containing W. Then

A. W_1 is always invariant under T
B. W_1 is never invariant under T
C. W_1 is invariant under T if and only if $W_1 = W$
D. W_1 is invariant under T if and only if $W_1 = \{0\}$

15. Let T be a linear operator on R^3 given by $T(x, y, z) = (0, x, 0)$. Then invariant factors of T are

A. 3, 2
B. 3, 1
C. 2, 1
D. 1, 1,1

Answers for Self Assessment

1.	A	2.	A	3.	C	4.	D	5.	C
6.	D	7.	C	8.	C	9.	B	10.	C
11.	A	12.	C	13.	A	14.	B	15.	C

Review Questions

1. Let $A = \begin{bmatrix} 6 & -3 & -2 \\ 4 & -1 & -2 \\ 10 & -5 & -3 \end{bmatrix}$. Check whether A is nilpotent or not. If yes, find its index of nilpotency.
2. Prove that the only nilpotent operator defined on a 1- dimensional vector space is the zero operator.

3. Let T be a linear operator on R^4 defined as $T(x, y, z, t) = (0, z, 0, 0)$. Checkwhether T is nilpotent or not. If yes, find its index of nilpotency.
4. Let $T: R^3 \to R^3$ be such that the matrix of linear operator T with respect to the standard basis B is given by

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

Find the corresponding form as

$$\begin{bmatrix} M_{n_1} & & & \\ & M_{n_2} & & \\ & & \ddots & \\ & & & M_{n_r} \end{bmatrix}$$

where $n_1 \geq n_2 \geq \ldots \geq n_r$ and $n_1 + n_2 + \cdots + n_r = \dim V$. Also, find the basis corresponding to which $[T_{V_1}]_B = M_{n_1}$.

5. Let $A = \begin{bmatrix} 1 & 4 & 2 \\ 6 & 1 & 2 \\ 1 & 5 & 3 \end{bmatrix}$. Check whether A is nilpotent or not. If yes, find its index of nilpotency.

Further Reading

- Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress
- Topics in algebra by I.N. Hartstein, Wiley
- Abstract algebra by David S Dummit and Richard M Foote, Wiley

Weblinks

- https://nptel.ac.in/courses/111/102/111102009/
- https://nptel.ac.in/courses/111/105/111105112/#

Unit 13: The Primary Decomposition Theorem

CONTENTS

Objective

After studying this unit, you will be able to

- state and prove the Primary Decomposition Theorem,
- understand the theorem with the help of an example.

Introduction

In this unit, you will be introduced to projections on a finite-dimensional vector space V over a field F. Important results about the range set and null space of a projection map are explained. Further, an important theorem Primary Decomposition Theorem is proved. This theorem establishes that for a linear operator T on a finite-dimensional vector space V over a field F, we can find subspaces $W_1, W_2, \ldots, W_k$ from the minimal polynomial of T such that V is a direct sum of $W_1, W_2, \ldots, W_k$.

13.1 Primary Decomposition Theorem

Definition 13.1.1: Let V be an n −dimensional vector space over a field F.

- A projection on V is a linear operator E such that $E^2 = E$
- Let E be a projection on V, then the range of E is denoted as R and the null space of E is denoted as N.

Theorem 13.1.2: Let V be an n −dimensional vector space over a field F. Then

(i) $\beta \in R$ if and only if $E\beta = \beta$

(ii) $V = R \oplus N$

Proof: Let $\beta \in R$.

There exists some $\alpha \in V$ such that $\beta = E(\alpha)$ ... (1)

This implies,

$$E\beta = E(E\alpha) = E^2\alpha = E\alpha = \beta$$

This implies, $E\beta = \beta \ \forall \ \beta \in R$

Conversely, let $E\beta = \beta$

$\beta = E\beta \in R$

For proof of part (ii)

Let $v \in V$

$v = Ev + (v - Ev)$

From part $(i) Ev \in R$

Consider

$E(v - Ev) = Ev - E^2 v = Ev - Ev = 0$

This implies, $v - Ev \in N$

So, $v = Ev + (v - Ev) \in R + N$

Hence, $V = R + N$

Let $x \in R \cap N$

Then by part (i), $x \in R$, $Ex = x$

Again, $x \in N$, $Ex = 0$

Therefore,

$x = Ex = 0$

So, $R \cap N = \{0\}$ and hence, $V = R \oplus N$

Theorem 13.1.3: Any projection E on an $n-$dimensional vector space V over a field F is always diagonalizable.

Proof:

Let E be a projection on V.

Then $E^2 = E$

This implies, $f(x) = x^2 - x$ is annihilating polynomial of E over F.

Let $p(x)$ be minimal polynomial of E over F.

Then $p(x)$ divides $f(x)$

So, $p(x) = x$, $x - 1$ or $x(x - 1)$

In any case, $p(x)$ is a product of distinct linear factors over F.

Hence, E is diagonalizable.

Task:

1. If E_1 and E_2 are projections onto independent subspaces, then $E_1 + E_2$ is a projection. True or false?
2. If E is a projection and f is a polynomial, then $f(E) = aI + bE$. What are a and b in terms of coefficients of f?

Theorem 13.1.4: Let $V = W_1 \oplus W_2 \oplus \ldots \oplus W_k$, then there exist k linear operators $E_1, E_2, \ldots, E_k$ on V such that

(i) Each E_i is a projection.

(ii) For $i \neq j$, $E_i E_j = 0$

(iii) $I = E_1 + E_2 + \cdots + E_k$

(iv) $R(E_i) = W_i$ where $R(E_i)$ is range of E_i.

Conversely, if $E_1, E_2, \ldots, E_k$ are k linear operators on V which satisfy (i), (ii) and (iii), and if we let W_i is the range of E_i then

$V = W_1 \oplus W_2 \oplus \ldots \oplus W_k$.

Proof:

$$V = W_1 \oplus W_2 \oplus \ldots \oplus W_k$$

$\forall \alpha \in V$, there exist unique $\alpha_1, \alpha_2, \ldots, \alpha_k \in W_i$ such that

$$\alpha = \alpha_1 + \alpha_2 + \cdots + \alpha_k \ldots (1)$$

Define the map $E_j: V \to W_j$ as $E_j(\alpha) = \alpha_j$

Since the representation (1) is unique, the map E_j is well defined.

Proof of (i)

Consider $\alpha \in V$

$$\alpha = \alpha_1 + \alpha_2 + \cdots + \alpha_k; \alpha_i \in W_i$$

$$E_j(\alpha) = \alpha_j \in W_j \subset V$$

By the uniqueness, we can write

$$\alpha_j = 0 + 0 + \cdots + 0 + \alpha_j + 0 + \cdots + 0$$

So that

$$E_j(\alpha_j) = \alpha_j$$

That is

$$E_j\left(E_j(\alpha)\right) = E_j(\alpha) \; \forall \; \alpha \in V$$

This implies,

$E_j^2 = E_j$ which proves part (i) that each E_j is a projection.

Proof of part (ii)

Let $\alpha = \alpha_1 + \alpha_2 + \cdots + \alpha_k \in V$

Then

$$E_j(\alpha) = \alpha_j$$

$$= \sum_{p=1}^{K} \beta_p$$

where $\beta_j = \alpha_j$ and $\beta_p = 0 \; \forall \; p \neq j$

For some $i \neq j$,

$$E_i\left(E_j(\alpha)\right) = E_i(\alpha_j)$$

$$= E_i\left(\sum_{p=1}^{K} \beta_p\right) = \beta_i$$

But since, $i \neq j$, $\beta_i = 0$

This implies,

$$E_i\left(E_j(\alpha)\right) = 0 \; \forall \; \alpha \in V$$

That is, $E_i E_j = 0 \; \forall \; i \neq j$

Proof of part (iii)

Consider $\alpha = \alpha_1 + \alpha_2 + \cdots + \alpha_k \in V$

Then

$E_j(\alpha) = \alpha_j$

$$\sum_{j=1}^{k} E_j(\alpha) = \sum_{j=1}^{k} \alpha_j = \alpha$$

So,

$$\sum_{j=1}^{k} E_j(\alpha) = I(\alpha)\ \forall\ \alpha \in V$$

This proves that

$$\sum_{j=1}^{k} E_j = I$$

Proof of part (iv)

Since $E_i : V \to W_i$, therefore, $R(E_i)$ is contained in W_i.

Now let $x \in W_i$

Then $x = 0 + 0 + \cdots + 0 + x + 0 + \cdots 0$

So that, $E_i(x) = x$, which implies $x \in R(E_i)$

This proves part (iv) that $R(E_i) = W_i$.

Conversely,

Suppose $E_1, E_2, \ldots, E_k$ are linear operators on V which satisfy the first three conditions,

and let W_i be the range of E_i.

Then for $\alpha \in V$

From (iii), $I(\alpha) = (E_1 + E_2 + \cdots + E_k)\alpha$

That is,

$$\alpha = E_1(\alpha) + E_2(\alpha) + \cdots + E_k(\alpha)$$
$$= \alpha_1 + \alpha_2 + \cdots + \alpha_k \ldots (2)$$

where $\alpha_i = E_i(\alpha) \in R(E_i) = W_i$

Therefore,

$$V = W_1 + W_2 + \cdots + W_k$$

Now, if possible, let

$$\alpha = \beta_1 + \beta_2 + \cdots + \beta_k \ldots (3)$$

Then since $\beta_i \in W_i = R(E_i)$

$$E_i(\beta_i) = \beta_i\ \forall\ i$$

Consider

$$E_j(\alpha) = \sum_{i=1}^{k} E_j(\beta_i)$$
$$= \sum_{i=1}^{k} E_j(E_i(\beta_i))$$
$$= E_j^2(\beta_j)\ \text{(Using (ii))}$$
$$= E_j(\beta_j)\ \text{Using (i)}$$

From (2), $E_j(\alpha) = \alpha_j$

This implies,

$$\alpha_j = \beta_j \; \forall \; j$$

Hence the sum is given by

$$V = W_1 + W_2 + \cdots + W_k$$

is a direct sum.

That is,

$$V = W_1 \oplus W_2 \oplus \ldots \oplus W_k$$

Definition 13.1.5: Consider the direct-sum decompositions $V = W_1 \oplus W_2 \oplus \ldots \oplus W_k$, where each of the subspaces W_i is invariant under some given linear operator T. Given such a decomposition of V, T induces a linear operator T_i on each W_i by restriction. The action of T is then this.

If

$$\alpha = \alpha_1 + \alpha_2 + \cdots + \alpha_k \in V,$$

then $\alpha_i \in W_i$ is uniquely determined.

We can observe that $T\alpha = T_1\alpha_1 + T_2\alpha_2 + \cdots + T_k\alpha_k$.

We shall describe this situation by saying that T is the direct sum of the operators $T_1, \ldots, T_k$.

It must be remembered in using this terminology that the T_i are not linear operators on the space V but the various subspaces W_i. The fact that $V = W_1 \oplus W_2 \oplus \ldots \oplus W_k$ enables us to associate with each $\alpha \in V$, a unique k −tuple $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ of vectors $\alpha_i \in W_i$ (by $\alpha = \alpha_1 + \alpha_2 + \cdots + \alpha_k$) 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.

Note: Our purpose is to study T by finding invariant direct-sum decompositions in which the T_i are operators of an elementary nature.

Theorem 13.1.6: Let T be a linear operator on the space V and let $W_1, W_2, \ldots, W_k$ and $E_1, E_2, \ldots, E_k$ be as defined earlier. Then a necessary and sufficient condition that each subspace W_i be invariant under T is that T commute with each of the projections E_i, i.e., $TE_i = E_iT$, $i = 1, 2, \ldots, k$.

Proof:

Suppose $TE_i = E_iT$, $i = 1, 2, \ldots, k$.

Let $\alpha \in W_j = R(E_j)$

Then $E_j\alpha = \alpha$ and

$$T\alpha = T(E_j\alpha)$$
$$= E_j(T\alpha)$$

which shows that $T\alpha \in W_j$ so W_j is invariant under T.

Conversely, assume that each W_j is invariant under T.

We shall show that $TE_j = E_jT \; \forall \; j$.

Let $\alpha \in V$,

Then

$$\alpha = E_1\alpha + E_2\alpha + \cdots + E_k\alpha$$

so that,

$$T\alpha = TE_1\alpha + TE_2\alpha + \cdots + TE_k\alpha$$

Since $E_i\alpha \in W_i$, which is invariant under T, so,

$T(E_i\alpha) = E_i\beta_i$ for some vector β_i.

Then

$$E_jTE_i\alpha = E_jE_i\beta_i$$
$$= \begin{cases} 0, & if\ i \neq j \\ E_j\beta_j & if\ i = j \end{cases}$$

Thus

$$E_jT\alpha = E_jTE_1\alpha + \cdots + E_jTE_k\alpha$$
$$= E_j\beta_j = TE_j\alpha$$

This holds for each $\alpha \in V$, so $E_jT = TE_j$.

Theorem 13.1.7: Let T be a linear operator on a finite-dimensional space V.

If T is diagonalizable and if $c_1, c_2, \ldots, c_k$ are the distinct characteristic values of T, then there exist, linear operators, $E_1, E_2, \ldots, E_k$ on V such that

$$(i)\ T = c_1E_1 + c_2E_2 + \cdots + c_kE_k$$
$$(ii)\ I = E_1 + E_2 + \cdots + E_k$$
$$(iii)\ E_iE_j = 0\ \forall\ i \neq j$$
$$(iv)\ E_i^2 = E_i$$

(v) the range of E_i is the characteristic space for T associated with c_i.

Conversely, if there exist k distinct scalars $c_1, c_2, \ldots, c_k$ and k non-zero linear operators $E_1, \ldots, E_k$ which satisfy conditions (i), (ii), and (iii),

then T is diagonalizable, $c_1, c_2, \ldots, c_k$ 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 $c_1, c_2, \ldots, c_k$.

Let W_i be the space of characteristic vectors associated with the characteristic value c_i.

As we have seen,

$$V = W_1 \oplus W_2 \oplus \ldots \oplus W_k$$

Let $E_1, E_2, \ldots, E_k$ be the projections associated with this decomposition.

Then we have proved that (ii), (iii), (iv), and (v) are satisfied.

To verify (i),

For each $\alpha \in V$,

$$\alpha = E_1\alpha + \cdots + E_k\alpha$$

and so,

$$T\alpha = TE_1\alpha + TE_2\alpha + \cdots + TEk\alpha$$
$$= c_1E_1\alpha + c_2E_2\alpha + \cdots + c_kE_k\alpha$$

In other words, $T = c_1E_1 + c_2E_2 + \cdots + c_kE_k$

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

$$I = E_1 + E_2 + \cdots + E_k$$

by E_i

and obtain immediately $E_i^2 = E_i$.

Multiplying

$$T = c_1E_1 + c_2E_2 + \cdots + c_kE_k$$

by E_i,

we then have

$$TE_i = c_iE_i,$$
$$(T - c_iI)E_i = 0$$

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 the characteristic values of T; for, if c is any scalar,

then

$$T - cI = (c_1 - c)E_1 + (c_2 - c)E_2 + \cdots + (c_k - c)E_k$$

So, if $(T - cI)\alpha = 0$,

Then

$$((c_1 - c)E_1 + (c_2 - c)E_2 + \cdots + (c_k - c)E_k)\alpha = 0$$

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 $c_i - c = 0$.

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 $I = E_1 + \ldots + E_k$shows that these characteristic vectors span V, therefore, T is diagonalizable.

Now we show that the null space of $(T - c_iI)$ is exactly the range of E_i.

Let α is in null space of $(T - c_iI)$.

That is, $T\alpha = c_i\alpha$, then using $(T - c_iI)\alpha = 0$and

$$(T - c_iI)\alpha = ((c_1 - c_i)E_1 + \cdots + (c_k - c_i)E_k)\alpha$$
$$\sum_{j=1}^{k}(c_j - c_i)E_j\alpha = 0$$

hence $(c_j - c_i)E_j\alpha = 0$ for each j

and then $E_j\alpha = 0$, $j \neq i$.

Since $\alpha = E_1\alpha + \cdots + E_k\alpha$ 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.

Theorem 13.1.8: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, $p = p_1^{r_1}p_2^{r_2}\ldots p_k^{r_k}$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 $p_i(T)^{r_i}$; $i = 1, 2, \ldots, k$.

Then

(*i*) $V = W_1 \oplus W_2 \oplus \ldots \oplus W_k$

(*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 $p_i^{r_i}$.

Proof:

For each i, let

$$f_i = \frac{p}{p_i^{r_i}} = p_1^{r_1} p_2^{r_2} \cdots p_{i-1}^{r_{i-1}} p_{i+1}^{r_{i+1}} \cdots p_k^{r_k}$$

Note that p_i does not divide f_i and p_j divides $f_i\ \forall\, j \neq i$.

Since $p_1, p_2, \ldots, p_k$ are distinct prime polynomials, the polynomials $f_1, f_2, \ldots, f_k$ are relatively prime.

Thus, there are polynomials $g_1, g_2, \ldots, g_k$ such that

$$\sum_{i=1}^{k} f_i g_i = 1$$

Note also that if $i \neq j$, then

$$f_i f_j = \frac{p^2}{p_i^{r_i} p_j^{r_j}}$$

$$= \frac{p_i^{r_i} p_j^{r_j}}{} \, p p_1^{r_1} p_2^{r_2} \cdots p_{i-1}^{r_{i-1}} p_{i+1}^{r_{i+1}} \cdots p_{j-1}^{r_{j-1}} p_{j+1}^{r_{j+1}} \cdots p_k^{r_k}$$

is divisible by the polynomial p, because $f_i f_j$ contains each $p_m^{r_m}$ as a factor.

Consider the polynomials $h_i = f_i g_i$.

Let $E_i = h_i(T) = f_i(T) g_i(T)$.

Since $\sum_{i=1}^{k} f_i g_i = 1$ and p divides $f_i f_j\ \forall\, i \neq j$,

we have,

$$E_1 + E_2 + \cdots + E_k = h_1(T) + h_2(T) + \cdots + h_k(T)$$

$$= f_1(T) g_1(T) + f_2(T) g_2(T) + \cdots + f_k(T) g_k(T)$$

$$= \sum_i f_i(T) g_i(T)$$

So, $E_1 + E_2 + \cdots + E_k = I \ldots (1)$

Again, p divides $f_i f_j\ \forall\, j \neq i$

$$f_i f_j = pq\,;\ q \in F[x]$$

Since p is minimal polynomial for T, $p(T) = 0$ implies,

$$f_i(T) f_j(T) = p(T) q(T) = 0\ \forall\, i \neq j$$

For $i \neq j$, consider

$$E_i E_j = f_i(T) g_i(T) f_j(T) g_j(T)$$

$$= f_i(T) f_j(T) g_i(T) g_j(T)$$

$$= 0\ \forall\, i \neq j$$

$E_i E_j = 0\ \forall\, i \neq j \ldots (2)$

From (1), $E_1 + E_2 + \cdots + E_k = I$

Pre-multiplying both sides by E_i and using (2), we get,

$$E_i^2 = E_i\ \forall i \ldots (3)$$

Thus, the E_i are projections that correspond to some direct-sum decomposition of the space V.

Now we wish to show that the range of E_i is exactly the subspace W_i.

Conversely,

Let $\alpha \in W_i$ = Null space of $p_i^{r_i}(T)$

If $j \neq i$, then $f_j g_j$ is divisible by $p_i^{r_i}$ and so $f_j(T)g_j(T)\alpha = 0$ that is $E_j\alpha = 0$ for $j \neq i$.

Also, $I = E_1 + E_2 + \cdots + E_k$

$$I(\alpha) = E_1(\alpha) + E_2(\alpha) + \cdots + E_k(\alpha)$$

That is,

$$\alpha = E_i\alpha$$

which implies,$\alpha \in$ Range of E_i

This proves that the range of E_i is exactly the subspace W_i.

W_i, being null space of $p_i^{r_i}(T)$ that is, the null space of a polynomial in T is invariant under T.

If T_i is the operator induced on W_i by T, then evidently $p_i^{r_i}(T_i) = 0$

because by definition, $p_i^{r_i}(T) = 0$ 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 $p_i^{r_i}$.

Example 13.1.9: Let$T$ be a linear operator on R^3 which is represented in the standard ordered basis by the matrix

$$\begin{bmatrix} 6 & -3 & -2 \\ 4 & -1 & -2 \\ 10 & -5 & -3 \end{bmatrix}$$

Express the minimal polynomial p for T in the form $p = p_1p_2$, where p_1 and p_2 are monic and irreducible over the field of real numbers.

Let W_i be the null space of $p_i(T)$. Find bases B_i for the spaces $W_i; i = 1, 2$. If T_i is the operator induced on W_i by T, find the matrix of T_i in the basis B_i.

Sol:

$$A = \begin{bmatrix} 6 & -3 & -2 \\ 4 & -1 & -2 \\ 10 & -5 & -3 \end{bmatrix}$$

The characteristic polynomial of A is $|xI - A|$

$$\Rightarrow \begin{vmatrix} x-6 & 3 & 2 \\ -4 & x+1 & 2 \\ -10 & 5 & x+3 \end{vmatrix} = 0$$

$\Rightarrow x^3 - 2x^2 + x - 2 = 0$

$\Rightarrow (x-2)(x^2+1) = 0$

The characteristic polynomial of A is $(x-2)(x^2+1)$.

Also, the characteristic polynomial is the same as the minimal polynomial.

That is, the minimal polynomial is

$$p(x) = (x-2)(x^2+1) = p_1p_2$$

Here $p_1 = x - 2$, $p_2 = x^2 + 1$

$p_1(T) = T - 2I$

$W_1 = \{X \in R^3 \mid p_1(T)X = 0\}$

$X = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$

$p_1(T)X = 0$

$\Rightarrow (T - 2I)X = 0$ or $(A - 2I)X = 0$

$\Rightarrow \begin{bmatrix} 4 & -3 & -2 \\ 4 & -3 & -2 \\ 10 & -5 & -5 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$

Applying $R_2 \to R_2 - R_1$

$\Rightarrow \begin{bmatrix} 4 & -3 & -2 \\ 0 & 0 & 0 \\ 10 & -5 & -5 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$

Applying $R_3 \to \frac{R_3}{5}$

$\Rightarrow \begin{bmatrix} 4 & -3 & -2 \\ 0 & 0 & 0 \\ 2 & -1 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$

$R_1 \to R_1 - 2R_3$

$\Rightarrow \begin{bmatrix} 0 & -1 & 0 \\ 0 & 0 & 0 \\ 2 & -1 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$

$y = 0,\ 2x = z$

$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} x \\ 0 \\ 2x \end{bmatrix} = x \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix}$

$B_1 = \{(1,\ 0,\ 2)\}$

W_2 =null space of $p_2(T) = \{X \in R^3 | p_2(T)X = 0\}$

$X = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$

$(T^2 + I)X = 0$

$\Rightarrow \begin{bmatrix} 5 & -5 & 0 \\ 0 & 0 & 0 \\ 10 & -10 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$

$5x - 5y = 0,\ x = y$

$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} x \\ x \\ z \end{bmatrix} = x \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + z \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$

$B_2 = \{(1,1,0),\ (0,0,\ 1)\}$

$T(1,\ 0,\ 0) = (6,\ 4,\ 10)$

$T(0,\ 1,\ 0) = (-3,\ -1,\ -5)$

$T(0,\ 0,\ 1) = (-2,\ -2,\ -3)$

For $(x,\ y,\ z) \in R^3$

$T(x,\ y,\ z) = (6x - 3y - 2z,\ 4x - y - 2z,\ 10x - 5y - 3z)$

$T(1,\ 0,\ 2) = (2,\ 0,\ 4) = 2(1,\ 0,\ 2)$

$[T_1]_{B_1} = [2]$

$T_2(1,1,0) = T(1,\ 1,\ 0) = (3,3,5)$

$T_2(0,\ 0,\ 1) = T(0,\ 0,\ 1) = (-2,\ -2,\ -3)$

$T_2(1,1,0) = (3,3,5) = 3(1,\ 1,\ 0) + 5(0,\ 0,\ 1)$

$T_2(0,\ 0,\ 1) = (-2,\ -2,\ -3) = -2\ (1,\ 1,\ 0) - 3(0,\ 0,\ 1)$

$[T_2]_{B_2} = \begin{bmatrix} 3 & -2 \\ 5 & -3 \end{bmatrix}$

Summary

- A projection map is defined for a finite-dimensional vector space
- Important results about the null space and range space of a projection map are explained.
- The Primary Decomposition Theorem is proved.

Keywords

- Projection map
- Range of a projection map
- Null space of a projection map
- The Primary Decomposition Theorem

Self Assessment

1. Let E be a projection defined on a vector space V over a field F. Then

A. $E^2 = E$

B. $E^3 = E$

C. $E^k = E$ for every natural number k

D. All options are correct

2. Let E be a projection on an n dimensional vector space V over a field F and R denotes the range of E. Then

A. $\beta \in R$ if and only if $E\beta = \beta$

B. $\beta \in R$ if and only if $E\beta \neq \beta$

C. $\beta \in R$ if and only if $E\beta = 0$

D. $\beta \in R$ if and only if $E\beta = 1$

3. Let E be a projection on an n dimensional vector space V over a field F. Let R and N denote the range space and null space of E respectively. Then $R \cap N =$

A. ϕ (Empty set)

B. $\{0\}$

C. V

D. F

4. Let E be a projection on a 5- dimensional vector space V over F. Then which of the following cannot be the minimal polynomials of E.

A. x

B. $x - 1$

C. $x(x-1)$

D. $x^4(x-1)$

5. The set of characteristic values of a non-zero, non-identity projection map is given by

A. $\{0\}$

B. $\{1\}$

C. $\{0, 1\}$

D. $\{0, 1, -1\}$

6. Let $V = W_1 \oplus W_2 \oplus W_3$, such that there exist 3 linear operators E_1, E_2, E_3 on V such that each E_i is a projection. Then

A. $E_1E_3 = 0$ and $E_1^2 = 0$ (0 denotes the zero map)

B. $E_1E_3 = I$ and $E_1^2 = 0$(I denotes the identity map)

C. $E_1E_3 = 0$ and $E_1^2 = E_1$

D. $E_1E_3 = I$ and $E_1^2 = I$

7. Let E be a projection map and I is an identity map on vector space V. Then $E^k(E-I)^k =$

A. $E(E-I)$

B. $E(I-E)$

C. $E(E-I)$ or $E(I-E)$

D. $E^{k+1} - E^k$

8. Let E be a projection map on R^5 then $x^5 - x$ is

A. An annihilating but not characteristic polynomial of E

B. A characteristic polynomial of E

C. A minimal polynomial of E

D. All options are correct

9. Let $V = R^5$, R denotes the field of real numbers. Define $T: R^5 \to R^5$ as $T(x_1, x_2, x_3, x_4, x_5) = (x_1, x_2, 0, 0, 0)$. Then

A. T is a linear map but not a projection

B. T is a projection on R^5 with characteristic polynomial $x^5 - x$

C. T is a projection on R^5 with characteristic polynomial $x^2(x-1)^3$

D. T is a projection on R^5 with characteristic polynomial $x^3(x-1)^2$

10. True/False: Differentiation map defined on P_3, the vector space of polynomials of degree less than or equal to 3 over the field of real numbers, is a projection on P_3

A. True

B. False

11. Let R denote the field of real numbers. Let $T: R^2 \to R^2$ be defined as $T(x, y) = (y, -x)$. Then $R^2 = W_1 \oplus W_2 \oplus \ldots \oplus W_k$ where each W_i is T $-$invariant.

A. R^2 has a primary decomposition with $k = 2$.

B. R^2 has a primary decomposition with $k = 3$.

C. R^2 has a primary decomposition with $k = 4$.

D. R^2 has no such primary decomposition

12. Let V be an n −dimensional vector space over a field F. Let T be a linear operator with distinct characteristic values $c_1, c_2, \ldots, c_k$. Then there exist linear maps $E_1, E_2, \ldots, E_k$ such that $T = c_1E_1 + c_2E_2 + \cdots + c_kE_k$ if and only if

A. T is any linear operator

B. T is diagonalizable

C. T is a linear operator with distinct characteristic values

D. T is triangulable

13. Let V be an n −dimensional vector space over a field F. Let T be a diagonalizable linear operator with distinct characteristic values $c_1, c_2, \ldots, c_k$. Consider linear maps $E_1, E_2, \ldots, E_k$ such that $T = c_1E_1 + c_2E_2 + \cdots + c_kE_k$. Then $T^2 =$

A. $c_1^2E_1 + c_2^2E_2 + \cdots + c_k^2E_k$

B. $c_1E_1^2 + c_2E_2^2 + \cdots + c_kE_k^2$

C. $2c_1E_1 + 2c_2E_2 + \cdots + 2c_kE_k$

D. $E_1E_2 + E_2E_3 + \cdots + E_{k-1}E_k$

14. Consider a linear operator T on R^2 given by $T(x, y) = (y, x)$. Then

A. T can be expressed as a sum of two projections on R^2

B. T can be expressed as a difference of two projections on R^2

C. T can be expressed as a product of two projections on R^2

D. T can be expressed as a sum of three projections on R^2

15. Consider a linear operator T on R^2 given by $T(x, y) = (y, x)$. Then $T = c_1E_1 + c_2E_2$, such that

A. $E_1(x, y) = \left(\frac{x+y}{2}, \frac{x+y}{2}\right), E_2(x, y) = \left(\frac{x-y}{2}, \frac{y-x}{2}\right)$

B. $E_1(x, y) = \left(\frac{x-y}{2}, \frac{x+y}{2}\right), E_2(x, y) = \left(\frac{x+y}{2}, \frac{y-x}{2}\right)$

C. $E_1(x, y) = \left(\frac{x+y}{2}, \frac{x+y}{2}\right), E_2(x, y) = \left(\frac{x-y}{2}, \frac{x-y}{2}\right)$

D. $E_1(x, y) = \left(\frac{x+y}{4}, \frac{x+y}{4}\right), E_2(x, y) = \left(\frac{x-y}{4}, \frac{y-x}{4}\right)$

Answers for Self Assessment

1.	D	2.	A	3.	B	4.	D	5.	C
6.	C	7.	C	8.	A	9.	D	10.	B
11.	D	12.	B	13.	A	14.	B	15.	A

Review Questions

1. Let T be the diagonalizable linear operator on R^3 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 $A = E_1 + 2E_2$, $E_1 + E_2 = I, E_1E_2 = 0$.

2. Let A be the 4×4 matrix given by

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

Find matrices E_1, E_2, E_3 such that $A = c_1E_1 + c_2E_2 + c_3E_3, E_1 + E_2 + E_3 = I, E_iE_j = 0\ \forall\ i \neq j$

3. Let V be a real vector space and E an idempotent linear operator on V, that is, a projection. Prove that $I + E$ is invertible. Find $(I + E)^{-1}$.
4. Find a projection E that projects R^2 onto the subspace spanned by $(1, -1)$ along the subspace spanned by $(1, 2)$.
5. Let E be a projection of V and let T be a linear operator on V. Prove that the range of E is invariant under T if and only if $ETE = TE$. Prove that both the range and null space of E are invariant under T if and only if $ET = TE$.

Further Readings

- Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress
- Topics in algebra by I.N. Hartstein, Wiley
- Abstract algebra by David S Dummit and Richard M Foote, Wiley

Weblinks

- https://nptel.ac.in/courses/111/102/111102009/
- https://nptel.ac.in/courses/111/105/111105112/#

Unit 14: Rational and Jordan Canonical Form

CONTENTS

Objective

After studying this unit, you will be able to

- define T −cyclic subspace corresponding to a linear operator T defined on a vector space V over a field F and understand results about the same,
- define T −annihilator of some element α corresponding to a linear operator T defined on a vector space V over a field F and understand results about the same,
- define T −admissible subspaces of a vector space V and a linear operator T on V,
- state and prove the Cyclic Decomposition Theorem,
- understand rational canonical form and find rational canonical form corresponding to a given operator (on a finite dimensional vector space) or a square matrix,
- understand Jordan Canonical form of a given matrix A or a linear operator T on a finite dimensional vector space V.

Introduction

In this unit, we are taking linear operators on a finite- dimensional vector space over a field F. T −cyclic subspace corresponding to a linear operator T will be defined and understand results about the same. T −annihilator of some element α corresponding to a linear operator T is defined. T −admissible subspaces of a vector space V will be defined. Cyclic Decomposition Theorem will be proved. Rational canonical form is explained and rational canonical form corresponding to a given operator (on a finite dimensional vector space) or a square matrix is elaborated with the help of examples. Jordan Canonical form of a given matrix A or a linear operator T on a finite dimensional vector space V is explained.

14.1 Cyclic Subspaces and Annihilators

Theorem 14.1.1: Let V is a finite-dimensional vector space over the field F and T is a fixed (but arbitrary) linear operator on V. If α is any vector in V and W is an invariant subspace of V containing α then $g(T)\alpha \in W$ for every polynomial $g \in F[x]$.

Proof: Let 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

$$T(T\alpha) = T^2\alpha,$$

$$T(T^2\alpha) = T^3\alpha$$

$$\vdots$$

$$T(T^{k-1}\alpha) = T^k\alpha \ \forall\ k$$

Consider

$$g(x) = a_0 + a_1x + \cdots + a_nx^n$$

Then

$$\begin{aligned} g(T)\alpha &= (a_0I + a_1T + \cdots + a_nT^n)\alpha \\ &= a_0\alpha + a_1T\alpha + \cdots + a_nT^n\alpha \in W \end{aligned}$$

In other words, W must contain $g(T)\alpha$ for every polynomial g over F.

Note: 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 contain α. In particular, the set of all vectors of the form $g(T)\alpha$ with g in $F[x]$, is the smallest $T-$invariant subspace which contains α.

Definition 14.1.2: 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, $Z(\alpha;T)$ 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 14.1.3:

(i) For any T, the $T-$ cyclic subspace generated by the zero vector is the zero subspace.

(ii) The space $Z(\alpha;T)$ is one dimensional if and only if α is a characteristic vector for T.

(iii) For the identity operator, every non-zero vector generates a one-dimensional cyclic subspace; thus, if dimension of $V > 1$, the identity operator has no cyclic vector.

Proof: Recall that

$$Z(\alpha;T) = \{g(T)\alpha \mid g \in F[x]\}$$

For $\alpha = 0$

$$\begin{aligned} Z(0;T) &= \{g(T)0 \mid g \in F[x]\} \\ &= \{0\} \end{aligned}$$

That proves part (i).

For part (ii)

The space $Z(\alpha;T)$ is one dimensional

Claim: $B = \{\alpha\}$ is a basis of $Z(\alpha;T)$

Let $\{\beta\}$ be the basis of $Z(\alpha;T)$

Since $g(T)\alpha \in Z(\alpha;T)$ for all $g \in F[x]$

Taking $g(x) = 1$, we get, $\alpha \in Z(\alpha;T)$

Therefore, $\alpha = c\beta; c \in F$

Clearly, $c \neq 0$ so that $\beta = c^{-1}\alpha$

So, $\beta = \ <\alpha>$ this implies, $Z(\alpha;T) = \ <\alpha>$.

Again, since $g(T)\alpha \in Z(\alpha;T)\ \forall\ g \in F[x]$

This implies, $g(T)\alpha = \ < \alpha >$

Also, taking $g(x) = x$, we have, $g(T)\alpha = c'\alpha$

That is, $T\alpha = c'\alpha$

So that, α is characteristic vector of T.

Conversely, let α is characteristic vector of T.

Then there exist some $c \in F$ such that $T\alpha = c\alpha$

In that case, $g(T)\alpha = g(c)\alpha$

This implies, $g(T)\alpha = \ < \alpha >$ for all $g \in F[x]$

That is, $Z(\alpha; T) =< \alpha >$

Proof of part (iii)

For $T = I$,

$Z(\alpha; I) = \{g(I)\alpha; g \in F[x]\}$

Let $g(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$

Then

$$g(I) = a_0I + a_1I^2 + \cdots + a_nI^n$$
$$= (a_0 + a_1 + \cdots + a_n)I = cI$$

So that,

$$Z(\alpha; I) = \{cI\alpha; c \in F\}$$
$$= \{c\alpha; c \in F\}$$
$$=< \alpha >$$

Since $\alpha \neq 0$,

$\{\alpha\}$ is linearly independent.

So, $Z(\alpha; T)$ has basis $\{\alpha\}$

That is, $Z(\alpha; T)$ is $1-$dimensional.

Further, if dimension $V > 1$, $T = I$

then $Z(\alpha; T)$ is one dimensional

but since dimension $V > 1$.

That is, $Z(\alpha; T)$ is a proper subspace of V.

So, $V \neq Z(\alpha; T)$ for any α,

hence, identity operator has no cyclic vector if dim $V > 1$

Example 14.1.4: An operator which has a cyclic vector.

Let T be an operator on F^2 which is represented in the standard ordered basis by matrix

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

Proof: Let $\alpha = (1, 0)$

Claim: $Z(\alpha; T) = F^2$

$Z(\alpha; T) = \{g(T)\alpha | g \in F[x]\}$ is a subspace of F^2.

Therefore, $Z(\alpha; T) \subseteq F^2$ ... (1)

Let $(a, b) \in F^2$

Let $g(x) = a + bx$

$$g(T)\alpha = (aI + bT)\alpha$$

$$= (aI + bT)\alpha \quad a\alpha + bT(\alpha)$$

$$= a\alpha + \quad a(1, 0) + \quad b\,T(1, 0)$$

$$= +\,b\,T \quad a(1, 0) + \quad b(0, 1) = (a, b)$$

So,

$$(a, b) = g(T)\alpha \in Z(\alpha; T)$$

That is,

$$F^2 \subseteq Z(\alpha; T) \ldots (2)$$

From (1) and (2), we get,

$$F^2 = Z(\alpha; T)$$

This proves that α is a cyclic vector.

Definition 14.1.5: Let $\alpha \in V$, then T −annihilator of α is the set $M(\alpha; T)$ of $F[x]$ given by

$$M(\alpha; T) = \{g \in F[x] | g(T)\alpha = 0\}$$

If $\alpha = 0$, then $g(T)\alpha = 0 \; \forall \; g \in F[x]$

So, if $\alpha = 0$ then $M(\alpha; T) = F[x]$

Theorem 14.1.6: $M(\alpha; T)$ is an ideal of $F[x]$

Proof:

$$M(\alpha; T) = \{g \in F[x] | g(T)\alpha = 0\}$$

Let $g(x) = 0 \; \forall \; x$

$$g(T) = 0$$
$$g(T)\alpha = 0$$

So, $g(x) = 0, \; g \in M(\alpha; T)$

$$M(\alpha; T) \neq \phi$$

Let $g, \; h \in M(\alpha; T)$

$$g(T)\alpha = 0, \; h(T)\alpha = 0$$

Then

$$g(T)\alpha - h(T)\alpha = 0$$

implies

$$(g - h)(T)\alpha = 0$$

That is,

$$g - h \in M(\alpha; T)$$

Let $f \in F[x], \; g \in M(\alpha; T)$

This implies, $g(T)\alpha = 0$

$$(fg)(T)\alpha = f(T)g(T)\alpha = 0$$

That is,

$$fg \in M(\alpha; T)$$

Similarly,

$$gf \in M(\alpha; T)$$

This implies, $M(\alpha;T)$ is an ideal of $F[x]$.

Notes:

- $F[x]$ is a principal ideal domain therefore, $M(\alpha;T)$ is generated by a single element.

We denote it as p_α.

- p_α is also called the T −annihilator of α.
- p_α divides the minimal polynomial of T.

Let p is the minimal polynomial for T.

Then $p(T) = 0$. Hence $p(T)\alpha = 0$

So, $p \in M(\alpha;T) = \ < p_\alpha >$ this implies, $p_\alpha | p$

- $\deg p_\alpha > 0$ unless $\alpha = 0$

Let $\alpha \neq 0$ and $\deg p_\alpha = 0$;

Then $p_\alpha = c; c \in F$

Since $p_\alpha(T)\alpha = 0$, $cI\alpha = 0, c\alpha = 0$

Again, $\alpha \neq 0$ implies $c = 0$

Then $M(\alpha;T) =< p_\alpha > \ = \{0\}$

But the minimal polynomial p of T belongs to $M(\alpha;T)$.

That is, $p = 0$ and hence $T = 0$

Consider $g(x) = x$

Then $g(T)\alpha = T\alpha = 0$

So, $g \in M(\alpha;T) = \{0\}$

That is not true.

So, we get a contradiction to our supposition.

That means, $\deg p_\alpha > 0$ unless $\alpha = 0$

Theorem 14.1.7: 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 $\alpha, T\alpha, T^2\alpha, \ldots, T^{k-1}\alpha$ 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.

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 $p_\alpha(T)\alpha = 0$

and hence

$$p_\alpha q(T)\alpha = p_\alpha(T)q(T)\alpha = q(T)p_\alpha(T)\alpha = 0$$

This implies,

$$g(T)\alpha = r(T)\alpha.$$

Since $r = 0$ or $deg\ (r) < k$,

Let

$$r(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n; n \leq k; a_i \in F$$

Then

$$r(T)\alpha = a_0\alpha + a_1T\alpha + a_2T^2\alpha + \cdots + a_nT^n\alpha; n \leq k$$

the vector $r(T)\alpha$ is a linear combination of the vectors $\alpha, T\alpha, \ldots, T^{k-1}\alpha$ and

since $g(T)\alpha$ is any vector in $Z(\alpha; T)$, this shows that these k vectors span $Z(\alpha; T)$.

These vectors are certainly linearly independent, because if not, then there exist scalars $a_0, a_1, \ldots, a_{k-1}$ (not all zero) such that$a_0\alpha + a_1T\alpha + a_2T^2\alpha + \cdots + a_{k-1}T^{k-1}\alpha = 0$

Then consider $g(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}$, then $g(T)\alpha = 0$but $deg\ (g) < deg\ (p_\alpha)$, which is absurd.

This proves (ii).

Let U be the linear operator on $Z(\alpha; T)$ obtained by restricting T.

If g is any polynomial over F, then

$$p_\alpha(U)g(T)\alpha = p_\alpha(T)g(T)\alpha = g(T)p_\alpha(T)\alpha = g(T)0 = 0$$

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.

Remark 14.1.8: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.

Example 14.1.9: Let W be a space of dimension k. Let U be a linear operator on W such that U has a cyclic vector α. Find matrix of U with respect to the basis $\{\alpha, U\alpha, \ldots, U^{k-1}\alpha\}$.

Given basis is $\{\alpha, U\alpha, \ldots, U^{k-1}\alpha\}$

Let

$$\alpha_1 = \alpha$$
$$\alpha_2 = U\alpha$$
$$\vdots$$
$$\alpha_k = U^{k-1}\alpha$$
$$U\alpha_1 = U\alpha = \alpha_2 = 0\alpha_1 + 1\alpha_2 + 0\alpha_3 + \cdots + 0\alpha_k$$
$$U\alpha_2 = U^2\alpha = \alpha_3 = 0\alpha_1 + 0\alpha_2 + 1\alpha_3 + \cdots + 0\alpha_k$$
$$\vdots$$
$$U\alpha_{k-1} = U^{k-1}\alpha = \alpha_k = 0\alpha_1 + 0\alpha_2 + \cdots + 1\alpha_k$$
$$U\alpha_k = U^k\alpha$$

Let $p_\alpha = c_0 + c_1x + \cdots + c_{k-1}x^{k-1} + x^k$ be $U -$ annihilator of α in W

and hence minimal polynomial of U.

We know that $p_\alpha(U) = 0$

$$c_0I + c_1U + \cdots + c_{k-1}U^{k-1} + U^k = 0$$
$$(c_0I + c_1U + \cdots + c_{k-1}U^{k-1} + U^k)\alpha = 0$$
$$c_0\alpha + c_1U\alpha + \cdots + c_{k-1}U^{k-1}\alpha + U^k\alpha = 0$$
$$c_0\alpha_1 + c_1\alpha_2 + \cdots + c_{k-1}\alpha_k + U\alpha_k = 0$$

$$U\alpha_k = -c_0\alpha_1 - c_1\alpha_2 - \cdots - c_{k-1}\alpha_k$$

That is,

$$U^k\alpha + c_{k-1}U^{k-1}\alpha + \cdots + c_1 U\alpha + c_0\alpha = 0$$

So,

$$[U]_B = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & -c_0 \\ 1 & 0 & 0 & \dots & 0 & -c_1 \\ 0 & 1 & 0 & \cdots & 0 & -c_2 \\ \vdots & & & & & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -c_{k-1} \end{bmatrix}$$

This matrix is known as companion matrix of the monic polynomial p_α.

Theorem 14.1.10: 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 $B = \{\alpha_1, \alpha_2, \dots, \alpha_k\}$ for W in which U is represented by the companion matrix of its minimal polynomial,

That is,

$$[U]_B = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & -c_0 \\ 1 & 0 & 0 & \dots & 0 & -c_1 \\ 0 & 1 & 0 & \cdots & 0 & -c_2 \\ \vdots & & & & & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -c_{k-1} \end{bmatrix}$$

Then

$$U\alpha_1 = 0\alpha_1 + 1\alpha_2 + 0\alpha_3 + \cdots + 0\alpha_k = \alpha_2$$

$$U\alpha_2 = 0\alpha_1 + 0\alpha_2 + 1\alpha_3 + \cdots + 0\alpha_k = \alpha_3$$

$$\vdots$$

$$U\alpha_{k-1} = 0\alpha_1 + 0\alpha_2 + \cdots + 1\alpha_k = \alpha_k$$

$$U\alpha_k = -c_0\alpha_1 - c_1\alpha_2 - \cdots - c_{k-1}\alpha_k$$

So that

$$B = \{\alpha_1, U\alpha_1, U\alpha_2, \dots, U\alpha_{k-1}\}$$

$$= \{\alpha_1, U\alpha_1, U^2\alpha_1, \dots, U^k\alpha_1\}$$

Clearly, α_1 is a cyclic vector for U.

Corollary 14.1.11: If A is the companion matrix of a monic polynomial p, then p is both the minimal and the characteristic polynomial of A.

Proof. Let U be the linear operator on F^k which is represented by A in the standard ordered basis.

Apply theorem together with the Cayley-Hamilton theorem, we get the desired result.

Example 14.1.12: Let T be the linear operator on R^3 which is represented in the standard ordered basis by the matrix

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

Prove that T has no cyclic vector. Find the T-cyclic subspace generated by the vector $(1, -1, 3)$

$$T(1, 0,0) = (2, 0, 0)$$

$$T(0,1,0) = (0, 2, 0)$$

$$T(0,0,1) = (0, 0, -1)$$

Hence for any $(x, y, z) \in R^3$

$$T(x, y, z) = (2x, 2y, -z)$$

$$T^2(x,\ y,\ z) = T(2x,\ 2y,\ -z)$$
$$= (4x,\ 4y,\ z)$$

If possible, let $(x,\ y,\ z)$ be the cyclic vector for T.

Then the set $B = \{(x,\ y,\ z),\ T(x,\ y,\ z),\ T^2(x,\ y,\ z)\}$ is a basis of R^3.

Then $B = \{(x,\ y,\ z),\ (2x,\ 2y,\ -z),\ (4x,\ 4y,\ z)\}$

Note that

$$2(x,\ y,\ z) + (2x,\ 2y,\ -z) - (4x,\ 4y,\ z) = 0$$

This implies that B is linearly dependent but B being basis is linearly independent.

So, we arrive at a contradiction

That is, T has no cyclic vector.

Consider the vector $\alpha = (1,\ -1,\ 3)$

Then $T(\alpha) = (2,\ -2,\ -3)$

So, the T −cyclic subspace W generated by $(1,\ -1,\ 3)$ is $\{a(1,\ -1,\ 3) + b(2,\ -2,\ -3) | a,\ b \in R\}$

That is, $\{(a + 2b,\ -(a + 2b),\ 3a - 3b) | a,\ b \in R\}$

So, $W = \{(x, -x,\ 3(x - 3y)) | x,\ y \in R\}$

Example 14.1.13: Let T be the linear operator on C^3 which is represented in the standard ordered basis by the matrix

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

Find the annihilator of the vector $(1,\ 0,\ 0)$. Find the T −annihilator of $(1,\ 0,\ i)$.

Sol:

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

To find the characteristic equation, we put,

$|xI - A| = 0$

$\Rightarrow \begin{vmatrix} x-1 & -i & 0 \\ 1 & x-2 & i \\ 0 & -1 & x-1 \end{vmatrix} = 0$

$\Rightarrow (x - 1)\ (x^2 - 3x + 2 + 2i) = 0$

So, the characteristic polynomial is $(x - 1)(x^2 - 3x + 2 + 2i)$.

Minimal polynomial is $(x - 1)(x^2 - 3x + 2 + 2i)$.

Consider $\alpha = (1,\ 0,\ 0)$

Let p be the T − annihilator of α then

$$p | (x - 1)(x^2 - 3x + 2 + 2i)$$

Clearly, $p \neq 0$

If $\deg p = 0$

$p = c,\ c \neq 0$

$p(T)\alpha = c\alpha \neq 0$

Therefore, $\deg p \neq 0$

If $\deg p = 1$

$p = x + a,\ a \in F$

$p(T)\alpha = 0$ implies $(T + aI)\alpha = 0$

$(A + aI)\alpha = 0$

$$\Rightarrow \left(\begin{bmatrix} 1 & i & 0 \\ -1 & 2 & -i \\ 0 & 1 & 1 \end{bmatrix} + \begin{bmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{bmatrix}\right)\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = 0$$

$$\Rightarrow \begin{bmatrix} 1+a & i & 0 \\ -1 & 2+a & -i \\ 0 & 1 & 1+a \end{bmatrix}\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = 0$$

$\Rightarrow \begin{bmatrix} 1+a \\ -1 \\ 0 \end{bmatrix} = 0$ which is not true.

Therefore, $\deg p \neq 1$.

If $\deg p = 2$

$p(x) = x^2 + ax + b$

$p(T)\alpha = 0$ implies $(T^2 + aT + bI)\alpha = 0$

That is, $(A^2 + aA + bI)\alpha = 0$

$$\Rightarrow \left(\begin{bmatrix} 1-i & 3i & 1 \\ -3 & 4-2i & -3i \\ -1 & 3 & 1-i \end{bmatrix} + \begin{bmatrix} a & ai & 0 \\ -a & 2a & -ia \\ 0 & a & a \end{bmatrix} + \begin{bmatrix} b & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & b \end{bmatrix}\right) = 0$$

$\Rightarrow \begin{bmatrix} (1-i)+a+b \\ -3-a \\ -1 \end{bmatrix} = 0$ which is not true.

$\deg p(x) \neq 2$

Hence $\deg p(x) = 3$

So, $p(x) = (x-1)(x^2 - 3x + 2 + 2i)$

Let $\beta = \begin{bmatrix} 1 \\ 0 \\ i \end{bmatrix}$

Consider $(A - I)\beta = \begin{bmatrix} 0 & i & 0 \\ -1 & 1 & -i \\ 0 & 1 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \\ i \end{bmatrix} = 0$

That is, $(A - I)\beta = 0$

So, $f(x) = x - 1$ is T −annihilator of β in V.

Task:

1. Prove that if T^2 has a cyclic vector, then T has a cyclic vector. Is the converse true?
2. Let V be an n −dimensional vector space over the field F, and let N be a nilpotent linear operator on V. Suppose $N^{n-1} \neq 0$, and let α be any vector in V such that $N^{n-1}\alpha \neq 0$. Prove that α is a cyclic vector for N. What exactly is the matrix of N in the ordered basis $\{\alpha, N\alpha, \ldots, N^{n-1}\alpha\}$.

14.2 Cyclic Decomposition and the Rational Form

Remark 14.2.1: Let $V = W \oplus W'$, W and W' both are invariant under T then for $\beta \in V$, $g(T)\beta \in W$ if $g(T)\beta = g(T)\gamma$ for some $\gamma \in W$

Proof: $\beta \in V = W \oplus W'$

There exist unique $\gamma \in W$, $\delta \in W'$ such that

$\beta = \gamma + \delta$

$g(T)\beta = g(T)\gamma + g(T)\delta$

Since W and W' are both invariant under T, therefore, for

$\gamma \in W$, $g(T)\gamma \in W$ and $\delta \in W'$, $g(T)\delta \in W'$ ... (1)

Again, $g(T)\beta = g(T)\gamma + g(T)\delta$

This implies, $g(T)\beta - g(T)\gamma = g(T)\delta$

$g(T)\beta \in W$ (given)

$g(T)\gamma \in W$ (from(1))

$\Rightarrow g(T)\beta - g(T)\gamma \in W$

$\Rightarrow g(T)\delta \in W$

Also, $g(T)\delta \in W'$

$\Rightarrow g(T)\delta \in W \cap W' = \{0\}$

$\Rightarrow g(T)\delta = 0$

Hence, $g(T)\beta = g(T)\gamma$

Definition 14.2.2: 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

(*i*)W is invariant under T;

(*ii*) if $f(T)\beta$ is in W, there exists a vector γ in W such that $f(T)\beta = f(T)\gamma$.

Theorem 14.2.3: LetW' be any proper T −invariant subspace of V.

Then there exists some non-zero α such that $W \cap Z(\alpha;T) = \{0\}$

Proof: Since $W \neq V$, W is a subspace of V.

There exist $0 \neq \beta$ such that $\beta \in V$, $\beta \notin W$

T − conductor of β in W is$S(\beta;W) = \{g|g(T)\beta \in W\}$

Let $f = s(\beta;W)$ be the monic generator of $S(\beta;W)$.

Then $f(T)\beta \in W$

Now, if W is T −admissible, there exists $\gamma \in W$ such that $f(T)\beta = f(T)\gamma$ ... (1)

Let $\alpha = \beta - \gamma$

Then $\gamma = \beta - \alpha$

$\gamma \in W$, so $\beta - \alpha$, $\alpha - \beta \in W$

That means, $g(T)\beta \in W$ if and only if $g(T)\alpha \in W$

That is, $s(\alpha;W) = s(\beta;W)$

So, f is also T −conductor of α in W but from (1)

$$f(T)(\beta - \gamma) = f(T)\beta - f(T)\gamma = 0$$

So, $f(T)\alpha = 0$

This implies, $g(T)\alpha \in W$ if and only if $g(T)\alpha = 0$

Therefore, $Z(\alpha;T) \cap W = \{0\}$

$Z(\alpha;T)$ and W are independent and f is T −annihilator of α.

Theorem 14.2.4: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 $\alpha_1, \alpha_2, \dots, \alpha_r$ in V with respective T −annihilators $p_1, p_2, \dots, p_r$ such that

$$(i) V = W_0 \oplus Z(\alpha_1;T) \oplus \dots \oplus Z(\alpha_r;T)$$

(*ii*) p_k divides p_{k-1}, $k = 2, 3, \dots, r$.

Furthermore, the integer r and the annihilators $p_1, p_2, \dots, p_r$ are uniquely determined by (i), (ii), and the fact that no α_k is 0.

Proof: We will do the proof in 4 steps. We shall abbreviate $f(T)\beta$ to $f\beta$.

Step 1:

There exist non-zero vectors $\beta_1, \beta_2, \dots, \beta_r \in V$ such that

$$(a) V = W_0 \oplus Z(\beta_1; T) \oplus \dots \oplus Z(\beta_r; T)$$

(b) If $1 \le k \le r$ and

$$W_k = W_0 \oplus Z(\beta_1; T) \oplus \dots \oplus Z(\beta_k; T)$$

then the conductor $p_k = s(\beta_k; W_{k-1})$ has maximum degree among all the $T-$ conductors into the subspace W_{k-1} that is, for all k,

$$deg\, p_k = \max_{\alpha \in V} deg\, s(\alpha, W_{k-1})$$

Proof of step 1:

If W is a proper $T-$invariant subspace, then

$$0 < \max_{\alpha} \deg s(\alpha; W) \le \dim V \dots (1)$$

$$\deg s(\beta; W) = \max_{\alpha \in V} \deg s(\alpha; W)$$

Now if $\beta \in W$ then $g(T)\beta \in W$ taking $g(T)$ as a constant polynomial. So, the constant polynomial is the least degree polynomial hence $\deg s(\beta; W) = 0$, which is a contradiction to (1). So, $\beta \notin W$.

Since W is invariant under T and $Z(\beta; T)$ consists of polynomials in T. Thus, the subspace $W + Z(\beta; T)$ is $T-$invariant. Since $\beta \notin W$, $W + Z(\beta; T)$ has dimension larger than $\dim W$.

Since W was arbitrary proper subspace of V. Similarly, for W_0 we can find β_1 such that $W_0 + Z(\beta_1; T)$ is a proper invariant subspace of V.

Let $W_1 = W_0 + Z(\beta_1; T)$

For W_1, $\exists$ some β_2 such that $\deg s(\beta_2; W_1) = \max_\alpha \deg s(\alpha; W_1)$ and proceeding like this we get,

$$W_0 + Z(\beta_1; T) + Z(\beta_2; T) + \cdots$$

so on.

This process will continue for a finite number of steps because $\beta_1, \beta_2, \dots, \beta_r$ can not be more than $\dim V$ (As $\dim W_k > \dim W_{k-1}\ \forall k$). Therefore, we must reach $W_r = V$ is not more than $n = \dim V$ steps.

$$V = W_0 + Z(\beta_1; T) + Z(\beta_2; T) + \cdots + Z(\beta_r; T)$$

Step 2: Let $\beta_1, \beta_2, \dots, \beta_r$ be non-zero vectors that satisfy conditions (a) and (b) of step 1.

Fix k, $1 \le k \le r$, let $\beta \in V$ and $f = s(\beta; W_{k-1})$

If

$$f(T)\beta = \beta_0 + \sum_{1 \le i < k} g_i \beta_i, \quad \beta_i \in W_i$$

then f divides each polynomial g_i and $\beta_0 = f(T)\gamma_0$ where $\gamma_0 \in W_0$.

Proof of Step 2: For $k = 1$, W_i is $T-$admissible.

Let us prove the result for $k > 1$

We need to prove that $f | g_i\ \forall i$

Divide f by g_i, we get h_i, r_i such that $g_i = f h_i + r_i$ where $r_i = 0$ or $\deg r_i < \deg f \dots (*)$

Let

$$\gamma = \beta - \sum_{i=1}^{k-1} h_i \beta_i \dots (2)$$

Now, $\beta_i \in W_i\ \forall i$ and $W_i \subset W_{i+1}\ \forall i$

So, $\beta_i \in W_{k-1}\ \forall\, 1 \le i \le k-1$ and W_{k-1} is a subspace of V

$$\sum_{i=1}^{k-1} h_i \beta_i \in W_{k-1}$$

implies $\gamma - \beta \in W_{k-1}$

This implies,

$$s(\gamma; W_{k-1}) = s(\beta; W_{k-1}) = f$$

Furthermore,

$$f(T)\gamma = f(T)\beta - \sum_{i=1}^{k-1} f(T) h_i \beta_i$$

$$\sum_{i=1}^{1} (g_i \beta_i - f(T) h_i \beta_i)$$

The second part is due to the given statement.

$$f(T)\gamma = \beta_0 + \sum_{i=1}^{k-1} (g_i - f(T)h_i)\beta_i$$

$$= \beta_0 + \sum_{i=1}^{k-1} r_i \beta_i \ldots (3)$$

where $r_i = g_i - f(T)h_i$

Suppose some $r_i \neq 0$

let j be the largest index, for which $r_i \neq 0$ that is, $\forall\, i > j,\ r_i = 0$.

From (3) applying g on both sides, we get

$$p\gamma = g\beta_0 + \sum_{i=1}^{j} g r_i \beta_i \ldots (4)$$

$$p\gamma = g f \gamma = g r_j \beta_j + g\beta_0 + \sum_{1 \le i < j} g r_i \beta_i \ldots (5)$$

Now,

$$\beta_0 + \sum_{1 \le i < j} r_i \beta_i \in W_{j-1}$$

$$g\left(\beta_0 + \sum_{1 \le i < j} r_i \beta_i\right) \in W_{j-1}$$

Also,

$$p\gamma = p(T)\gamma \in W_{j-1}$$

From (5),

$$g r_j \beta_j \in W_{j-1}$$

Now from condition (b) of step 2

$$\deg(g r_j) \ge \deg s(\beta_j; W_{j-1})$$

From the statement of step 1,

$$\deg s(\beta_j; W_{j-1}) = \deg p_j$$

Hence,

$$\deg_{(g r_j)} \ge \deg_{p_j}$$

$$\geq \deg s(\gamma; W_{j-1})$$

$$= \deg p = \deg fg$$

This implies,

$\deg r_j \geq \deg f$

which is a contradiction to (*).

Therefore, $r_i = 0$

therefore, f divides $g_i \ \forall i$

Also, from (2)

$\beta_0 = f(T)\gamma$

Since W_0 is T −admissible and $\beta_0 \in W_0$

This implies, $f(T)\gamma \in W_0$

Then from the definition of T −admissible subspace there exist γ_0 such that $f(T)\gamma = f(T)\gamma_0$

Step 3: There exist non-zero vectors $\alpha_1, \alpha_2, \ldots, \alpha_r \in V$ which satisfy (i) and (ii) of the statement of the theorem.

Proof of Step 3:

Start with $\beta_1, \beta_2, \ldots, \beta_r$ as in step 1. Fix k, $1 \leq k \leq r$, apply step 2, we find $\beta = \beta_k$ and $T-$conductor $f = p_k$, we observe,

$$\beta = \beta_k \in W_{k-1}$$

$$= W_0 + Z(\beta_1; T) + Z(\beta_2; T) + \cdots + Z(\beta_k; T)$$

$$\beta_k = \gamma_0 + \sum_{1 \leq i \leq k-1} h_i \beta_i$$

we get,

$$p_k\beta_k = p_k\gamma_0 + \sum_{1 \leq i \leq k-1} p_k h_i \beta_i$$

where $\gamma_0 \in W_0$ and $h_1, h_2, \ldots, h_{k-1}$ are polynomials.

Let

$$\alpha_k = \beta_k - \gamma_0 - \sum_{1 \leq i \leq k-1} h_i \beta_i$$

Since $\beta_k - \alpha_k \in W_{k-1}$

Therefore, $s(\alpha_k; W_{k-1}) = s(\beta_k; W_{k-1}) = p_k$

Since $p_k\alpha_k = 0$

let some vector $\beta \notin W_{k-1}$

Consider T −conductor of $\beta \in W_{k-1}$ is $s(\beta; W_{k-1}) = l$. This implies, $l(T)\beta \in W_{k-1}$.

Also, T −conductor of β_k in W_{k-1} is p_k.

So, $p_k(T)\beta_k \in W_{k-1}$

W_{k-1} is T −admissible, therefore, there exists γ_k such that $p_k\beta_k = p_k\gamma_k$, $\gamma_k \in W_{k-1}$.

Let $\alpha_k = \beta_k - \gamma_k$

Then $p_k\alpha_k = 0$

For any polynomial g, $g(T)\alpha_k \in W_{k-1}$ if and only if $g(T)\alpha_k = 0$

$\Rightarrow W_k \cap Z(\alpha_k; T) = \{0\}$

Therefore,

$$W_k = W_0 \oplus Z(\alpha_1;T) \oplus Z(\alpha_2;T) \oplus \ldots \oplus Z(\alpha_k;T)$$

Claim: $p_k | p_{k-1}$

Since, $p_i \alpha_i = 0 \; \forall \, i$

$p_k \alpha_k = 0 + p_1 \alpha_1 + \cdots + p_{k-1} \alpha_{k-1}$

$f(T)\beta = \beta_0 + \sum_{1 \le i < k} g_i \beta_i, \; \beta_i \in W_i$

implies $f | g_i \; \forall \, i$

Here, $f = p_k, \; \beta_0 = 0, \; g_i = p_i, \; \beta_i = \alpha_i$

That is,

$p_k | p_i \; \forall \, i < k$

In particular, $p_k | p_{k-1}$

Step 4: The number rand the polynomials $p_1, \; p_2, \ldots, \; p_r$ are uniquely determined.

Proof of step 4: Let in addition to $\alpha_1, \; \alpha_2, \ldots, \; \alpha_r$ in step 3, we have non-zero $\gamma_1, \gamma_2, \ldots, \gamma_s$ with respective T −annihilators $g_1, \; g_2, \ldots, \; g_s$ such that

$$V = W_0 \oplus Z(\gamma_1;T) \oplus \ldots \oplus Z(\gamma_s;T)$$

$g_k | g_{k-1} \; \forall \, k = 2, 3, \ldots, s$

Claim: $r = s$ and $p_i = g_i \; \forall \, i$

g_1 is T −conductor of V into W_0

Let $S(V;W_0) = \{ f(T) | f(T)\beta \in W_0 \; \forall \, \beta \in V \}$

In other words, range of $f(T)$ is contained in W_0.

Also, $S(V, W_0)$ is an ideal in $F[x]$ with a monic generator g_1.

As for any $\beta \in V = W_0 \oplus Z(\gamma_1;T) \oplus \ldots \oplus Z(\gamma_s;T)$

$$\beta = \beta_0 + \sum_{i=1}^{s} f_i \gamma_i$$

This implies,

$$g_1 \beta = g_1 \beta_0 + \sum_{i=1}^{s} g_1 f_i \gamma_i$$

$\Rightarrow g_i | g_{i-1} \; \forall \, i$

$\Rightarrow g_i | g_1 \; \forall \, i$

$\Rightarrow g_1 = g_i h_i ; \; h_i \in F[x]$

and $g_i \gamma_i = 0$

Consider $g_1 \gamma_i = g_i h_i \gamma_i = h_i g_i \gamma_i = 0$

$g_1 \beta = g_1 \beta_0 \in W_0 \; \forall \beta$

Therefore, $g_1 \in S(V;W_0)$

Also, g_1 is a monic polynomial of least degree in $S(V;W_0)$

Similarly, p_1 is the generator of $S(V;W_0)$

Therefore, $p_1 = g_1$

If $r \ge 2$,

$$V = W_0 \oplus Z(\alpha_1;T) \oplus \ldots \oplus Z(\alpha_r;T)$$

That is,

$$\dim V = \dim W_0 + \dim Z(\alpha_1;T) + \cdots + \dim Z(\alpha_r;T) > \dim W_0 + \dim Z(\alpha_1;T)$$

Now $p_1 = g_1$

that is, generator of $Z(\alpha_1;T)$ and $Z(\gamma_1;T)$ are same.

This implies, $\dim Z(\alpha_1;T) = \dim Z(\gamma_1;T)$

$$\dim V > \dim W_0 + \dim Z(\gamma_1;T)$$

This implies, $s \geq 2$

Therefore, g_2 exists.

From two decompositions of V, we have,

$$p_2V = p_2W_0 \oplus Z(p_2\alpha_1;T)$$

and

$$p_2V = p_2W_0 \oplus Z(p_2\gamma_1;T) \oplus \dots \oplus Z(p_2\gamma_s;T) \dots(6)$$

Now $p_1 = g_1$

This implies,

$\dim Z(p_2\alpha_1;T) = \dim Z(p_2\gamma_1;T)$

$\Rightarrow \dim Z(p_2\gamma_i;T) = 0 \; \forall \; i \geq 2$

$\Rightarrow p_2\gamma_2 = 0$ that is, $g_2|p_2$

Similarly, we can show that $p_2|g_2$

Hence, the decomposition is unique.

Corollary 14.2.5: 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 T −admissible subspace of V.

If $W_0 = V$,

The complement we seek is {0}.

If W_0 is proper, applying the theorem, and letting,

$$W_0' = Z(\alpha_1;T) \oplus \dots \oplus Z(\alpha_r;T)$$

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 $V = W_0 \oplus Z(\alpha_1;T) \oplus \dots \oplus Z(\alpha_r;T)$

where the T −annihilators $p_1, p_2, \dots, p_r$ are such that p_{k+1} divides p_k, $1 \leq k \leq r-1$.

As we noted in the proof of Theorem, it easily follows that p_1 is the minimal polynomial for T, i.e., the T −conductor of V into {0}. We have proved (a).

We have already seen 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 $V = Z(\alpha;T)$.

Rational Canonical Form

Let T be a linear operator and the direct-sum decomposition given in Cyclic Decomposition Theorem. Let B_i be the 'cyclic ordered basis $\{\alpha_i, T\alpha_i, \dots, T^{k_i-1}\alpha_i\}$ for $Z(\alpha_i;T)$.

Here 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 B_i is the companion matrix of the polynomial p_i.

Thus, if we let B be the ordered basis for V which is the union of the B_i arranged in the order $B_1, B_2, \ldots, B_r$, then the matrix of T in the ordered basis B will be

$$A = \begin{bmatrix} A_1 & 0 & \ldots & 0 \\ 0 & A_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \ldots & A_r \end{bmatrix}$$

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 of companion matrices of non-scalar monic polynomials $p_1, p_2, \ldots, p_r$ such that p_{i+1} divides p_i for $i = 1, \ldots, r-1$, will be said to be in rational form.

Theorem 14.2.6: Let F be a field and let B be an $n \times n$ matrix over F. Then B is similar over the field F to one and only one matrix which is in rational form.

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 $g_1, g_2, \ldots, g_s$ such that g_{i+1} divides g_i for $i = 1, \ldots, s-1$, then it is apparent that we shall have non-zero vectors $\beta_1, \beta_2, \ldots, \beta_s$ in V with T-annihilators $g_1, g_2, \ldots, g_s$ such that

$$V = Z(\beta_1; T) \oplus Z(\beta_2; T) \oplus \ldots \oplus Z(\beta_s; T)$$

But then by the uniqueness statement in the cyclic decomposition theorem, the polynomials g_i are identical with the polynomials p_i which defines the matrix A. Thus $C = A$.

Example 14.2.7: Suppose T is a linear operator on a vector space V over a field F of dimension 2. Then T is similar over F to a matrix of one of the two types

$$\begin{bmatrix} 0 & -c_1 \\ 1 & -c_2 \end{bmatrix} \text{ or } \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix}.$$

Proof: Since $\dim V = 2$

Therefore, the characteristic polynomial of T is of degree 2.

Let minimal polynomial of T is p.

Two cases arise

Case 1: $\deg p = 2$

Let $p(x) = x^2 + ax + b; a, b \in F$

Then T is represented by the companion matrix of its minimal polynomial.

Then is, it is of the type

$$\begin{bmatrix} 0 & -c_0 \\ 1 & -c_1 \end{bmatrix}$$

where $c_0 = b,\ c_1 = a$

Case 2: $\deg p = 1$

Let $p(x) = x + a; a \in F$

Then characteristic polynomial of T is $(x+a)^2$

Then for any two linearly independent vectors α_1 and α_2 in V, we have

$$V = Z(\alpha_1; T) \oplus Z(\alpha_2; T)$$

$$p_1 = p_2 = x - c; c = a$$

So, T over F is similar to the matrix $\begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix}$

Example 14.2.8: Let T be the linear operator on R^3 which is represented by the matrix

$$A = \begin{bmatrix} 5 & -6 & -6 \\ -1 & 4 & 2 \\ 3 & -6 & -4 \end{bmatrix}$$

Find the corresponding rational matrix A' and a basis B such that $[T; B] = A'$.

Characteristic polynomial $f = (x-1)(x-2)^2$

Minimal polynomial

$$p = (x-1)(x-2) = x^2 - 3x + 2$$

We know that in the cyclic decomposition for T, the vector α_1 will have p as its $T-$ annihilator.

Corresponding companion matrix is $\begin{bmatrix} 0 & -2 \\ 1 & 3 \end{bmatrix}$

Since dim $R^3 = 3$, therefore, there will be only one other vector α_2.

It must be the characteristic vector of T. Its T −annihilator p_2 must be such that $pp_2 = f$

That is, $p_2 = x - 2$

Corresponding companion matrix is [2]

So, $A \sim A'$where

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

That is, T is represented by A' in some ordered basis.

Now we need to find basis $B = (B_1, B_2)$ where B_1 is the ordered basis for $Z(\alpha_1; T)$ and B_2 for $Z(\alpha_2; T)$

$$\dim Z(\alpha_1; T) = degree\ p = 2$$

$$\dim Z(\alpha_2; T) = degree\ p_2 = 1$$

Consider $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$.

Let $\alpha_1 = (1, 0, 0)$

$T(1, 0, 0) = (5, -1, 3) \neq c(1, 0, 0)$ for any $c \in F$

Take $\alpha_1 = (1, 0, 0)$

$$B_1 = \{\alpha_1, T\alpha_1\} = \{(1, 0, 0), (5, -1, 3)\}$$

Again, $Z(\alpha_2; T)$ is 1 −dimensional space. It is generated by a characteristic vector of T corresponding to $\lambda = 2$.

$(A - 2I)X = 0$

$$\Rightarrow \begin{bmatrix} 3 & -6 & -6 \\ -1 & 2 & 2 \\ 3 & -6 & -6 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Interchanging R_2 with R_1

$$\Rightarrow \begin{bmatrix} -1 & 2 & 2 \\ 3 & -6 & -6 \\ 3 & -6 & -6 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Applying $R_2 \to R_2 + 3R_1$and $R_3 \to R_3 + 3R_1$

$$\Rightarrow \begin{bmatrix} -1 & 2 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$\Rightarrow -x + 2y + 2z = 0$

$\Rightarrow x = 2y + 2z$

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 2y + 2z \\ y \\ z \end{bmatrix} = y \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} + z \begin{bmatrix} 2 \\ 0 \\ 1 \end{bmatrix}$$

$B_2 = \{\alpha_2\} = \{(2,\ 1,\ 0)\}$

$B = \{(1,\ 0,\ 0),\ (5,\ -1,\ 3),\ (2,\ 1,\ 0)\}$

Example 14.2.9: Let T be the linear operator on Q^3 which is represented by the matrix

$$A = \begin{bmatrix} 0 & 6 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{bmatrix}$$

Find the matrix P such that $P^{-1}AP$ is in the rational form

Sol: Characteristic polynomial is given by

$$|xI - A| = 0$$

$$\begin{vmatrix} x & -6 & -1 \\ -1 & x & 1 \\ 0 & -1 & x-1 \end{vmatrix} = 0$$

$\Rightarrow x^2(x-1) - 5(x-1) = 0$

$\Rightarrow (x^2-5)(x-1) = 0$

Characteristic polynomial $f = (x-1)(x^2-5)$

So, the corresponding rational form is

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 5 \\ 0 & 1 & 0 \end{bmatrix}$$

Now the required matrix will correspond to the matrix $P = [v_1 \quad v_2 \quad Tv_2]$ where v_1 is such that $x-1$ is T –annihilator of v_1 and x^2-5 is T –annihilator of v_2.

Let $v_1 = \begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix}$, $\alpha, \beta, \gamma \in Q$

Consider $(A-I)v_1 = 0$

$$\begin{bmatrix} -1 & 6 & 1 \\ 1 & -1 & -1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} -\alpha + 6\beta + \gamma \\ \alpha - \beta - \gamma \\ \beta \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$\Rightarrow \beta = 0,\ \ \alpha = \gamma$

Therefore, $v_1 = \begin{bmatrix} \alpha \\ 0 \\ \alpha \end{bmatrix} = \alpha \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$

Taking $\alpha = 1$, $v_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$

Let $v_2 = \begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix}$

$(A^2 - 5I)v_2 = 0$

$$\Rightarrow \left(\begin{bmatrix} 6 & 1 & -5 \\ 0 & 5 & 0 \\ 1 & 1 & 0 \end{bmatrix} - \begin{bmatrix} 5 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 5 \end{bmatrix} \right) v_2 = 0$$

$$\Rightarrow \begin{bmatrix} 1 & 1 & -5 \\ 0 & 0 & 0 \\ 1 & 1 & -5 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix} = 0$$

$\Rightarrow \alpha + \beta - 5\gamma = 0$

$\Rightarrow \alpha = 1,\ \beta = -1,\ \gamma = 0$

$$v_2 = \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}$$

$$Tv_2 = Av_2 = \begin{bmatrix} 0 & 6 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix} = \begin{bmatrix} -6 \\ 1 \\ -1 \end{bmatrix}$$

$$P = \begin{bmatrix} 1 & 1 & -6 \\ 0 & -1 & 1 \\ 1 & 0 & -1 \end{bmatrix}$$

14.3 Jordan Blocks, Jordan Forms, and Generalized Jordan Form over any Field.

Remark 14.3.1: Suppose that N is a nilpotent linear operator on the finite-dimensional space V.

Consider the cyclic decomposition of N, we have a positive integer r and r non-zero vectors $\alpha_1, \alpha_2, \ldots, \alpha_r$ in V with N −annihilators $p_1, p_2, \ldots, p_r$ such that

$$V = Z(\alpha_1; N) \oplus \ldots \oplus Z(\alpha_r; N)$$

and p_{i+1} divides p_i for $i = 1, \ldots, r-1$.

Since N is nilpotent, the minimal polynomial is x^k for some $k \le n$.

Thus, each p_i is of the form

$$p_i = x^{k_i},$$

and the divisibility condition simply says that

$$k_1 \ge k_2 \ge \cdots \ge k_r.$$

Also, $k_1 = k$ and $k_r \ge 1$.

The companion matrix of x^{k_i} is the square matrix of order k_i given by

$$A_i = \begin{bmatrix} 0 & 0 & \cdots & \cdots & 0 & 0 \\ 1 & 0 & \cdots & \cdots & 0 & 0 \\ 0 & 1 & & & 0 & 0 \\ \vdots & \vdots & \cdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & 0 & 0 \\ 0 & 0 & \cdots & \cdots & 1 & 0 \end{bmatrix}$$

Thus, by cyclic decomposition theorem there exists an ordered basis for V in which the matrix of N is the direct sum of the elementary nilpotent matrices, the sizes of which decrease as i increases.

The companion matrix of x^{k_i} is the square matrix of order k_i given by

$$A_i = \begin{bmatrix} 0 & 0 & \cdots & \cdots & 0 & 0 \\ 1 & 0 & \cdots & \cdots & 0 & 0 \\ 0 & 1 & & & 0 & 0 \\ \vdots & \vdots & \cdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & 0 & 0 \\ 0 & 0 & \cdots & \cdots & 1 & 0 \end{bmatrix}$$

Thus, by cyclic decomposition theorem there exists an ordered basis for V in which the matrix of N is the direct sum of the elementary nilpotent matrices, the sizes of which decrease as i increases.

One sees from this that associated with a nilpotent $n \times n$ matrix is a positive integer r and r positive integers $k_1, k_2, \ldots, k_r$ such that $k_1 + k_2 + \cdots + k_r = n$ and $k_i \ge k_{i+1}$, and these positive integers determine the rational form of the matrix, i.e., determine the matrix up to similarity.

The positive integer r is precisely the nullity of N; in fact, the null space has as a basis the r vectors $N^{k_i-1}\alpha_i$.

For, let α be in the null space of N. We write α in the form

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

where f_i is a polynomial, the degree of which we may assume is less than k_i.

Since $N\alpha = 0$ for each i we have

$$0 = N(f_i\alpha_i)$$
$$= N(f_i\alpha_i)$$
$$= N(f_i)N(\alpha_i))$$

$$= (xf_i)\alpha_i$$

Thus, xf_i is divisible by x^{k_i}, and since $\deg(f_i) > k$, this means that $f_i = c_i x^{k_i - 1}$ where c_i is some scalar.

But then

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

which shows us that the vectors $\{N^{k_i-1}\alpha_i\}$ form a basis for the null space of N.

This fact is also quite clear from the matrix point of view.

Now we wish to do is to combine our findings of nilpotent operators or matrices with the primary decomposition theorem.

The situation is this:

Suppose that T is a linear operator on V and that the characteristic polynomial for T factors over F as follows:

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

where $c_1, c_2, \ldots, c_k$ are distinct elements of F and $d_i \geq 1$.

Then the minimal polynomial for T will be

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

where $1 \leq r_i \leq d_i$.

If W_i is the null space of $(T - c_i I)^{r_i}$;

then the primary decomposition theorem tells us that

$$V = W_1 \oplus W_2 \oplus \ldots \oplus W_k$$

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 $N_i = T_i - c_i I$.

Then N_i is nilpotent and has minimal polynomial x^{r_i}.

On W_i, T acts like N_i plus the scalar c_i times the identity operator.

Suppose we choose a basis for the subspace W_i corresponding to the cyclic decomposition for the nilpotent operator N_i.

Then the matrix of T_i in this ordered basis will be the direct sum of matrices

$$\begin{bmatrix} c & 0 & 0 & \ldots & 0 & 0 \\ 1 & c & 0 & \ldots & 0 & 0 \\ \vdots & & & & & \vdots \\ 0 & 0 & 0 & \ldots & c & 0 \\ 0 & 0 & 0 & \ldots & 1 & c \end{bmatrix}$$

each with $c = c_i$.

Furthermore, the sizes of these matrices will decrease as one reads from left to right.

A matrix of this form 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

$$A = \begin{bmatrix} A_1 & 0 & \ldots & 0 \\ 0 & A_2 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & A_k \end{bmatrix}$$

of matrices $A_1, A_2, \ldots, A_k$.

Each A_i is of the form

$$A = \begin{bmatrix} J_1^{(i)} & 0 & \dots & 0 \\ 0 & J_2^{(i)} & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & J_{n_i}^{(i)} \end{bmatrix}$$

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 (for some distinct scalars $c_1, c_2, \dots, c_k$) 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.

In other words, if two matrices are in Jordan form and they are similar, then they can differ only in that the order of the scalars c_i is different.

The uniqueness we see is 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 T.

In other words, the characteristic polynomial for T is

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

Then shows that $c_1, c_2, \dots, c_k$ and $d_1, d_2, \dots, d_k$ 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

$$V = W_1 \oplus W_2 \oplus \dots \oplus W_k$$

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 $(T_i - c_iI)$.

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 $c_1, c_2, \dots, c_k$ 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 value 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 $(T - c_iI)$. 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_i 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 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.

Example 14.3.2: Suppose T is a linear operator on C^2. Then T is similar over C to a matrix of one of the two types $\begin{bmatrix} c_1 & 0 \\ 0 & c_2 \end{bmatrix}$ or $\begin{bmatrix} c & 0 \\ 1 & c \end{bmatrix}$.

Sol: The characteristic polynomial of T is of types

$I\ f = (x-c)^2$

$II\ f = (x-c_1)(x-c_2);\ c, c_1, c_2 \in F$

If $f = (x-c)^2$ Let p be the minimal polynomial. Then $p = x - c$ or $(x-c)^2$

If $p = x - c$ then Jordan block is $\begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix}$

If $p = (x-c)^2$ then Jordan block is $\begin{bmatrix} c & 0 \\ 1 & c \end{bmatrix}$

Case II $p = (x-c_1)(x-c_2)$

Then Jordan form is $\begin{bmatrix} c_1 & 0 \\ 0 & c_2 \end{bmatrix}$

Example 14.3.3: Let A be the complex 3×3 matrix

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

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

Sol: Characteristic polynomial of $A = (x-2)^2(x+1)$

The minimal polynomial can be $(x-2)^2\ (x+1)$ but in this case, it is not diagonalizable.

So, minimal polynomial $p = (x-2)(x+1)$

This implies, $(A - 2I)(A + I) = 0$

$$\Rightarrow \begin{bmatrix} 0 & 0 & 0 \\ a & 0 & 0 \\ b & c & -3 \end{bmatrix}\begin{bmatrix} 3 & 0 & 0 \\ a & 3 & 0 \\ b & c & 0 \end{bmatrix} = O$$

$$\Rightarrow \begin{bmatrix} 0 & 0 & 0 \\ 3a & 0 & 0 \\ 3b + ac - 3b & 0 & 0 \end{bmatrix} = O$$

$$\Rightarrow \begin{bmatrix} 0 & 0 & 0 \\ 3a & 0 & 0 \\ ac & 0 & 0 \end{bmatrix} = O$$

$\Rightarrow a = 0$

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

Example 14.3.4: Let A be the complex 4×4 matrix

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

Sol: Characteristic polynomial of A is $(x-2)^4$

The minimal polynomial of A is $x-2,\ (x-2)^2,\ (x-2)^3,\ (x-2)^4$

If minimal polynomial $p = x - 2$

$\Rightarrow A - 2I = 0$

$\Rightarrow A = 2I$

But $A \neq 2I$

Now consider $(x-2)^2$

$$(A-2I)^2 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha & 0 \end{bmatrix}$$

If minimal polynomial $p = x - 2$

$\Rightarrow A - 2I = 0$

$\Rightarrow A = 2I$

But $A \neq 2I$

Now consider $(x-2)^2$

$$(A-2I)^2 = O$$

$$p = (x-2)^2$$

If $\alpha = 0$, then the matrix is given by

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

If $\alpha = 1$, then the matrix is given by

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

Note that these two forms are not similar.

When $\alpha = 0$ then the Jordan form is

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

So that the characteristic space for 2 is of dimension 3.

When $\alpha = 1$, then the same space has dimension 2.

Definition 14.3.5: Let $\lambda \in F$ is a characteristic value of $A \in F^{n \times n}$, then a non-zero $X \in F^n$ is called a generalized characteristic vector of A corresponding to characteristic value λ if $(A - \lambda I)^m X = 0$ for some $m \in N$.

The smallest m is called the period of the generalized characteristic vector.

Note that a characteristic vector is a generalized characteristic vector with period 1.

Method: Here we see the method to find the invertible matrix P such that for a given square matrix A, $P^{-1}AP$ is in the Jordan form.

Step 1: Find the distinct characteristic values.

Step 2: Find the period s of a characteristic value λ

Step 3: Corresponding to the characteristic value λ, find the least positive integer m such that

$$rank\ (A-\lambda I)^m = rank\ (A-\lambda I)^{m+1}$$

Step 4: Find m number of linearly independent solutions to $(A-\lambda I)^s X = 0$ and $(A-\lambda I)^{s-1} X \neq 0$

It will give generalized characteristic vector X corresponding to the characteristic value λ.

Step 5: Find the vectors $X,\ (A-\lambda I)X,\ \ldots (A-\lambda I)^{s-1}X$ these are first s columns of P

Repeat this process with all characteristic values and find the matrix P.

Example 14.3.6: Let $A = \begin{bmatrix} 5 & 1 & -2 & 4 \\ 0 & 5 & 2 & 2 \\ 0 & 0 & 5 & 3 \\ 0 & 0 & 0 & 4 \end{bmatrix}$. Find an invertible matrix P such that $P^{-1}AP$ is in Jordan canonical form.

Or

Let T be a linear operator on R^4 such that matrix of T with respect to the standard ordered basis of R^4 is given by A. Find a basis B of R^4 such that $[T]_B$ is in Jordan form

Sol: Given

$$A = \begin{bmatrix} 5 & 1 & -2 & 4 \\ 0 & 5 & 2 & 2 \\ 0 & 0 & 5 & 3 \\ 0 & 0 & 0 & 4 \end{bmatrix}$$

Distinct characteristic values of A are 5 and 4.

$$A - 5I = \begin{bmatrix} 0 & 1 & -2 & 4 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

Apply $R_4 \to R_4 + \frac{1}{3}R_3$

$$\begin{bmatrix} 0 & 1 & -2 & 4 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Rank $(A-5I) = 3$

$$(A-5I)^2 = \begin{bmatrix} 0 & 0 & 2 & -8 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & -3 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Rank $(A-5I)^2 = 2$

$$(A-5I)^3 = \begin{bmatrix} 0 & 0 & 0 & 14 \\ 0 & 0 & 0 & -4 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

Rank $(A-5I)^3 = 1$

Rank $(A-5I)^4 = 1$

$q_1 = 4 - rank\,(A-5I) = 4 - 3 = 1$

$q_2 = rank\,(A-5I) - rank\,(A-5I)^2 = 1$

$q_3 = 1,\ q_4 = 0$

Jordan block corresponding to $\lambda = 5$ is of size 3.

$$\begin{bmatrix} 5 & 0 & 0 \\ 1 & 5 & 0 \\ 0 & 1 & 5 \end{bmatrix}$$

Again, $A - 4I = \begin{bmatrix} 1 & 1 & -2 & 4 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}$

Rank $(A-4I) = 3$

$$\text{Rank } (A-4I)^2 = \text{Rank} \begin{bmatrix} 1 & 2 & -2 & 0 \\ 0 & 1 & 4 & 8 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix} = 3$$

$q_1 = 4 - 3 = 1$

$q_2 = 0$

Corresponding Jordan block is [4]

$$P^{-1}AP = \begin{bmatrix} 5 & 0 & 0 & 0 \\ 1 & 5 & 0 & 0 \\ 0 & 1 & 5 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix}$$

To find P,

Period of $5 = 3$

Let $(A-5I)^3X = 0$, $(A-5I)^2X \neq 0$

$$\begin{bmatrix} 0 & 0 & 0 & 14 \\ 0 & 0 & 0 & -4 \\ 0 & 0 & 0 & -3 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \\ t \end{bmatrix} = 0$$

We get, $t = 0$

Consider $(A-5I)^2X \neq 0$

$$\begin{bmatrix} 0 & 0 & 2 & -8 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & -3 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \\ 0 \end{bmatrix} \neq 0$$

$$2z \neq 0,\ z \neq 0$$

Take $X = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$

$$X,\ (A-5I)X,\ (A-5I)^2X = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} -2 \\ 2 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

For $\lambda = 4$

Period of $4 = 1$

$$(A-4I)X = 0$$

$$\begin{bmatrix} 1 & 1 & -2 & 4 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \\ t \end{bmatrix} = 0$$

Applying $R_1 \to R_1 - R_2$

$$\begin{bmatrix} 1 & 0 & -4 & 2 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \\ t \end{bmatrix} = 0$$

$$x = -14t,\ y = 4t,\ z = -3t$$

$X = \begin{bmatrix} -14 \\ 4 \\ -3 \\ 1 \end{bmatrix}$

$P = \begin{bmatrix} 0 & -2 & -2 & -14 \\ 0 & 2 & 0 & 4 \\ 1 & 0 & 0 & -3 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

$$P^{-1}AP = \begin{bmatrix} 5 & 0 & 0 & 0 \\ 1 & 5 & 0 & 0 \\ 0 & 1 & 5 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix}$$

The corresponding basis is

$$B = \{(0,\ 0,\ 1,\ 0),\ (-2,\ 2,\ 0,\ 0),\ (2,\ 0,\ 0,\ 0),\ (-14,\ 4,\ -3,\ 1)\}$$

Summary

- T −cyclic subspace corresponding to a linear operator T are defined and related results are explained.
- T −annihilator of some element α corresponding to a linear operator T is defined.
- T −admissible subspaces of a vector space V is defined.
- The cyclic Decomposition Theorem is proved.
- The rational canonical form is explained and rational canonical form corresponding to a given operator (on a finite-dimensional vector space) or a square matrix is elaborated with the help of examples.
- Jordan Canonical form of a given matrix A or a linear operator T on a finite-dimensional vector space V is explained.

Keywords

- T −cyclic subspace
- T −annihilator of α
- T −admissible subspace
- Rational Canonical Form
- Jordan Canonical Form

Self Assessment

1. Let V be a finite-dimensional vector space over the field F. Let W be an invariant subspace of V. Then for any polynomial $g \in F[x]$,

A. $g(T)\beta \in W \ \forall \beta \in V$
B. $g(T)\beta \in W \ \forall \beta \in W$
C. $g(T)\beta \in W$ if and only if $\beta \in W$
D. No option is correct

2. Let V be a finite-dimensional vector space over the field F. The T −cyclic subspace generated by α is 1 −dimensional. Then

A. α is any non-zero element of V
B. $\alpha = 0$
C. α is any non-zero characteristic value of T
D. α is a characteristic vector of T

3. Choose the correct statement

A. $\deg p_\alpha \neq 0 \ \forall \alpha \in V$
B. $\deg p_\alpha = \dim V$
C. $\deg p_\alpha = \dim Z(\alpha;T)$
D. $Z(\alpha;T)$ is not T −invariant

4. Companion matrix of the polynomial $f(x) = x^3 + 2x^2 + 1$ is

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

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

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

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

5. The matrix $\begin{bmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \end{bmatrix}$ is companion matrix to the polynomial

A. $x^4 - 2x^3 - x^2 + 1$
B. $x^4 + 2x^3 + 3x - 1$
C. $x^4 - 2x^3 - 3x^2 + 1$
D. $x^4 - 2x^3 - 3x + 1$

6. If T is a linear operator on a finite-dimensional vector space, then every $T-$admissible subspace

A. has a complementary subspace which is also invariant under T
B. has a complementary subspace which is not invariant under T
C. may or may not have a complementary subspace
D. is a finite subspace

7. Let T is an operator on a finite-dimensional vector space V such that it has a cyclic vector. Then

A. Characteristic and minimal polynomial of T are always the same
B. Characteristic polynomial and minimal polynomial are always distinct
C. Characteristic polynomial and minimal polynomial may or may not be distinct
D. Degree of the minimal polynomial is less than dimension V

8. Let V be a finite-dimensional vector space over a field F. Let W be a $T-$invariant subspace of V. Let $\beta \in V, \beta \notin W$, then

A. $\dim W < \dim(W + Z(\beta;T))$
B. $\dim W \leq \dim(W + Z(\beta;T))$
C. $\dim W = \dim(W + Z(\beta;T))$
D. $\dim W > \dim(W + Z(\beta;T))$

9. True/False Every $T-$admissible subspace is $T-$invariant.

A. True
B. False

10. Rational canonical form of the matrix $\begin{bmatrix} -3 & 2 & 0 \\ 1 & 0 & 1 \\ 1 & -3 & -2 \end{bmatrix}$ is

A: $\begin{bmatrix} 0 & 0 & -3 \\ 1 & 0 & -7 \\ 0 & 1 & -5 \end{bmatrix}$

B: $\begin{bmatrix} 0 & 0 & -3 \\ 1 & 0 & 7 \\ 0 & 1 & -5 \end{bmatrix}$

C: $\begin{bmatrix} 0 & 0 & 3 \\ 1 & 0 & -7 \\ 0 & 1 & -5 \end{bmatrix}$

D: $\begin{bmatrix} 0 & 0 & -3 \\ 1 & 0 & -5 \\ 0 & 1 & 7 \end{bmatrix}$

11. True/False Rational form of a matrix is unique

A. True
B. False

12. True/ False Suppose T is a linear operator on a vector space V over a field F of dimension 2. If T has distinct characteristic values, then T is diagonalizable.

A. True
B. False

13. Let A be a matrix of order 3 such that eigenvalues of A are 1, 1, 2. Then the Jordan block corresponding to the eigenvalue 1 is

A: $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$

B: $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

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

D: $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$

14. Let a matrix A of order 3 has only one eigenvalue λ. Then Jordan canonical form of A is

A: $\begin{bmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{bmatrix}$

B: $\begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix}$

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

D: $\begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 1 & \lambda \end{bmatrix}$

15. Let characteristic equation of a matrix A of order 3 is $(x-1)^2(x-2)$ and minimal polynomial is $(x-1)(x-2)$. Then Jordan canonical form of A is

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

B: $\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}$

C: $\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{bmatrix}$

D: $\begin{bmatrix} 2 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$

Answers for Self Assessment

1. B	2. D	3. C	4. A	5. D

6. A	7. A	8. A	9. A	10. A
11. A	12. A	13. B	14. B	15. A

Review Questions

1. Let T be a linear operator on the finite-dimensional space V, and let R be the range of T. Prove that R has a complementary $T-$invariant subspace if and only if R is independent of the null space N of T.
2. Let T be a linear operator on the finite-dimensional space V, and let R be the range of T. If R and N are independent, prove that N is the unique $T-$invariant subspace complementary to R.
3. Let T be the linear operator on F^4 which is represented in the standard ordered basis by the matrix
$$\begin{bmatrix} c & 0 & 0 & 0 \\ 1 & c & 0 & 0 \\ 0 & 1 & c & 0 \\ 0 & 0 & 1 & c \end{bmatrix}$$
Let W be the null space of $T-cI$. Prove that W is the subspace spanned by ϵ_4.
4. Find the minimal and the rational form of the matrix $\begin{bmatrix} 0 & -1 & -1 \\ 1 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix}$.
5. The differentiation operator on the space of polynomials of degree less than or equal to 3 is represented in the natural ordered basis 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 this matrix?

Further Readings

- Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress
- Topics in algebra by I.N. Hartstein, Wiley
- Abstract algebra by David S Dummit and Richard M Foote, Wiley

Weblinks

- https://nptel.ac.in/courses/111/102/111102009/
- https://nptel.ac.in/courses/111/105/111105112/#

LOVELY PROFESSIONAL UNIVERSITY
Jalandhar-Delhi G.T. Road (NH-1)
Phagwara, Punjab (India)-144411
For Enquiry: +91-1824-521360
Fax.: +91-1824-506111
Email: odl@lpu.co.in