M. Sc. MATHEMATICS

MAL-521

(ADVANCE ABSTRACT ALGEBRA)

Lesson No &Lesson Name	Writer	Vetter
1 Linear Transformations	**Dr. Pankaj Kumar**	**Dr. Nawneet Hooda**
2 Canonical Transformations	**Dr. Pankaj Kumar**	**Dr. Nawneet Hooda**
3 Modules I	**Dr. Pankaj Kumar**	**Dr. Nawneet Hooda**
4 Modules II	**Dr. Pankaj Kumar**	**Dr. Nawneet Hooda**

DIRECTORATE OF DISTANCE EDUCATIONS

GURU JAMBHESHWAR UNIVERSITY OF SCIENCE & TECHNOLOGY

HISAR 125001

MAL-521: M. Sc. Mathematics (Algebra)

Lesson No. 1 **Written by Dr. Pankaj Kumar**

Lesson: Linear Transformations **Vetted by Dr. Nawneet Hooda**

STRUCTURE

1.0 OBJECTIVE

Objective of this Chapter is to study Linear Transformation on the finite dimensional vector space V over the field F.

1.1 INTRODUCTION

Let U and V be two given finite dimensional vector spaces over the same field F. Our interest is to find a relation (generally called as linear transformation) between the elements of U and V which satisfies certain conditions and, how this relation from U to V becomes a vector space over the field F. The set of all transformation on U into itself is of much interest. On finite dimensional vector space V over F, for given basis of V, there always exist a matrix and for given basis and given matrix of order n there always exist a linear transformation.

In this Chapter, in Section 1.2, we study about linear transformations. In Section 1.3, Algebra of linear transformations is studied. In next two sections characteristic roots and characteristic vectors of linear transformations are studied. In Section 1.6, matrix of transformation is studied. In Section 1.7 canonical transformations are studied and in last section we come to know about canonical form (Triangular form).

1.2 LINEAR TRANSFORMATIONS

1.2.1 Definition. Vector Space. Let F be a field. A non empty set V with two binary operations, addition (+)and scalar multiplications($\cdot$), is called a vector space over F if V is an abelian group under + and for $v \in V$, $\alpha.v \in V$. The following conditions are also satisfied:

(1) $\alpha.(v+w) = \alpha v+ \alpha w$ for all $\alpha \in F$ and v, w in V,

(2) $(\alpha+\beta).v = \alpha v+\beta v$,

(3) $(\alpha\beta).v = \alpha.(\beta v)$

(4) $1.v = v$

For all α, $\beta \in$ F and v, w belonging to V. Here v and w are called vectors and α, β are called scalar.

1.2.2 Definition. Homomorphism. Let V and W are two vector space over the same field F then the mapping T from V into W is called homomorphism if

(i) $(v_1+v_2)T= v_1T+v_2 T$

(ii) $(\alpha v_1)T= \alpha(v_1T)$

for all v_1, v_2 belonging to V and α belonging to F.

Above two conditions are equivalent to $(\alpha v_1+\beta v_2)T=\alpha(v_1T)+ \beta(v_2T)$.

If T is one-one and onto mapping from V to W, then T is called an isomorphism and the two spaces are isomorphic. Set of all homomorphism from V to W is denoted by Hom(V, W) or $Hom_R(V, W)$

1.2.3 Definition. Let S and T$\in$ Hom(V, W), then S+T and λS is defined as:

(i) $v(S+T)= vS+vT$ and

(ii) $v(\lambda S)= \lambda(vS)$ for all $v\in V$ and $\lambda\in F$

1.2.4 Problem. S+T and λS are elements of Hom(V, W) i.e. S+T and λS are homomorphisms from V to W.

Proof. For (i) we have to show that

$$(\alpha u+\beta v)(S+T)= \alpha(u(S+T))+ \beta(v(S+T))$$

By Definition 1.2.3, $(\alpha u+\beta v)(S+T)=(\alpha u+\beta v)S+(\alpha u+\beta v)T$. Since S and T are linear transformations, therefore,

$$\begin{aligned}(\alpha u+\beta v)(S+T)&=\alpha(uS)+\beta(vS)+\alpha(uT)+\beta(vT)\\ &=\alpha((uS)+\alpha(uT))+\beta((vS)+(vT))\end{aligned}$$

Again by definition 1.2.3, we get that $(\alpha u+\beta v)(S+T)=\alpha(u(S+T))+\beta(v(S+T))$. It proves the result.

(ii) Similarly we can show that $(\alpha u+\beta v)(\lambda S)=\alpha(u(\lambda S))+\beta(v(\lambda S))$ i.e. λS is also linear transformation.

1.2.5 Theorem. Prove that Hom(V, W) becomes a vector space under the two operation operations $v(S+T)= vS + vT$ and $v(\lambda S)= \lambda(vS)$ for all $v\in V$, $\lambda\in F$ and S, T $\in$Hom(V, W).

Proof. As it is clear that both operations are binary operations on Hom(V, W). We will show that under +, Hom(V,W) becomes an abelian group. As $0\in$Hom(V,W) such that $v0=0$ $\forall$ $v\in V$(it is call zero transformation), therefore, $v(S+0)= vS+v0 = vS = 0+vS= v0+vS= v(0+S)$ $\forall$ $v\in V$ i.e. identity element exists in Hom(V, W). Further for $S\in$Hom(V, W), there exist $-S\in$Hom(V, W) such that $v(S+(-S))= vS+v(-S)= vS-vS=0= v0$ $\forall$ $v\in V$ i.e. $S+(-S)=0$. Hence inverse of every element exist in Hom(V, W). It is easy to see that $T_1+(T_2+T_3)= (T_1+T_2)+T_3$ and $T_1+T_2= T_2+T_1$ $\forall$ $T_1, T_2, T_3\in$Hom(V, W). Hence Hom(V, W) is an abelian group under +.

Further it is easy to see that for all S, T $\in$Hom(V, W) and $\alpha, \beta\in F$, we have $\alpha(S+T)= \alpha S+\alpha T$, $(\alpha+\beta)S= \alpha S+\beta S$, $(\alpha\beta)S= \alpha(\beta S)$ and $1.S=S$. It proves that Hom(V, W) is a vector space over F.

1.2.6 Theorem. If V and W are vector spaces over F of dimensions m and n respectively, then Hom(V, W) is of dimension mn over F.

Proof. Since V and W are vector spaces over F of dimensions m and n respectively, let $v_1, v_2,\ldots, v_m$ be basis of V over F and $w_1, w_2,\ldots, w_n$ be basis of W over F. Since $v=\delta_1 v_1+\delta_2 v_2+...+\delta_m v_m$ where $\delta_i \in F$ are uniquely determined for $v\in V$. Let us define T_{ij} from V to W by

$v_iT_{ij}=\delta_i w_j$ i.e. $v_iT_{kj}=\begin{cases} w_j & \text{if } i=k \\ 0 & \text{if } i\neq k \end{cases}$. It is easy to see that T_{ij} $\in$Hom(V,W). Now we will show that mn elements T_{ij} $1\le i\le m$ and $1\le j\le n$ form the basis for Hom(V, W). Take

$$\beta_{11}T_{11}+\beta_{12}T_{12}+...+\beta_{1n}T_{1n}+...+\beta_{i1}T_{i1}+\beta_{i2}T_{i2}+...+\beta_{in}T_{in}+$$
$$\ldots+\beta_{m1}T_{m1}+\beta_{m2}T_{m2}+...+\beta_{mn}T_{mn}=0$$

(Since a linear transformation on V can be determined completely if image of every basis element of it is determined)

$$\Rightarrow v_i(\beta_{11}T_{11}+\beta_{12}T_{12}+...+\beta_{1n}T_{1n}+...+\beta_{i1}T_{i1}+\beta_{i2}T_{i2}+...+\beta_{in}T_{in}+$$
$$\ldots+\beta_{m1}T_{m1}+\beta_{m2}T_{m2}+...+\beta_{mn}T_{mn})=v_i0=0$$

$$\Rightarrow \beta_{i1}w_1+\beta_{i2}w_2+...+\beta_{in}w_n=0 \ (\because v_iT_{kj}=\begin{cases} w_j & \text{if } i=k \\ 0 & \text{if } i\neq k \end{cases})$$

But $w_1, w_2, \ldots, w_n$ are linearly independent over F, therefore, $\beta_{i1}=\beta_{i2}=...=\beta_{in}=0$. Ranging i in $1\le i\le m$, we get each $\beta_{ij}=0$. Hence T_{ij} are linearly independent over F. Now we claim that every element of Hom(V,W) is linear combination of T_{ij} over F. Let S $\in$Hom(V,W) such that

$$v_1S=\alpha_{11}w_1+\alpha_{12}w_2+...+\alpha_{1n}w_n,$$
$$v_iS=\alpha_{i1}w_1+\alpha_{i2}w_2+...+\alpha_{in}w_n$$
$$v_mS=\alpha_{m1}w_1+\alpha_{m2}w_2+...+\alpha_{mn}w_n.$$

Take $S_0=\alpha_{11}T_{11}+\alpha_{12}T_{12}+...+\alpha_{1n}T_{1n}+...+\alpha_{i1}T_{i1}+\alpha_{i2}T_{i2}+...+\alpha_{in}T_{in}+$ $\alpha_{m1}T_{m1}+\alpha_{m2}T_{m2}+...+\alpha_{mn}T_{mn}$ .Then

$$v_iS_0=v_i(\alpha_{11}T_{11}+\alpha_{12}T_{12}+...+\alpha_{1n}T_{1n}+...+\alpha_{i1}T_{i1}+\alpha_{i2}T_{i2}+...+\alpha_{in}T_{in}$$
$$+\alpha_{m1}T_{m1}+\alpha_{m2}T_{m2}+...+\alpha_{mn}T_{mn})$$
$$=\alpha_{i1}w_1+\alpha_{i2}w_2+...+\alpha_{in}w_n=v_iS.$$

Similarly we can see that $v_iS_0=v_iS$ for every i, $1\le i\le m$.

Therefore, $vS_0=vS\ \forall\ v\in V$. Hence S_0=S. It shows that every element of Hom(V,W) is a linear combination of T_{ij} over F. It proves the result.

1.2.7 Corollary. If dimension of V over F is n, then dimension of Hom(V,V) over F $=n^2$ and dimension of Hom(V,F) is n over F.

1.2.8 Note. Hom(V, F) is called dual space and its elements are called linear functional on V into F. Let $v_1, v_2,\ldots, v_n$ be basis of V over F then $\hat{v}_1, \hat{v}_2, \ldots, \hat{v}_n$ defined by $\hat{v}_i(v_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$ are linear functionals on V which acts as basis elements for V. If v is non zero element of V then choose $v_1=v$, $v_2,\ldots, v_n$ as the basis for V. Then there exist $\hat{v}_1(v_1) = \hat{v}_1(v) = 1 \neq 0$. In other words we have shown that for given non zero vector v in V we have a linear transformation f(say) such that $f(v)\neq 0$.

1.3 ALGEBRA OF LINEAR TRANSFORMATIONS

1.3.1 Definition. Algebra. An associative ring A which is a vector space over F such that $\alpha(ab)= (\alpha a)b= a(\alpha b)$ for all $a, b\in A$ and $\alpha\in F$ is called an algebra over F.

1.3.2 Note. It is easy to see that set of all Hom(V, V) becomes an algebra under the multiplication of S and T $\in$Hom(V, V) defined as:

$$v(ST)= (vS)T \text{ for all } v\in V.$$

we will denote Hom(V, V)=A(V). If dimension of V over F i.e. $\dim_F V=n$, then $\dim_F A(V)=n^2$ over F.

1.3.3 Theorem. Let A be an algebra with unit element and $\dim_F A=n$, then every element of A satisfies some polynomial of degree at most n. In particular if $\dim_F V=n$, then every element of A(V) satisfies some polynomial of degree at most n^2.

Proof. Let e be the unit element of A. As $\dim_F A=n$, therefore, for $a\in A$, the n+1 elements e, a, $a^2,\ldots,a^n$ are all in A and are linearly dependent over F, i.e. there exist $\beta_0, \beta_1,\ldots, \beta_n$ in F , not all zero, such that $\beta_0 e+\beta_1 a+\ldots+ \beta_n a^n=0$. But then a satisfies a polynomial $\beta_0+\beta_1 x+\ldots+ \beta_n x^n$ over F. It proves the result. Since the $\dim_F A(V)=n^2$, therefore, every element of A(V) satisfies some polynomial of degree at most n^2.

1.3.4 Definition. An element $T \in A(V)$ is called right invertible if there exist $S \in A(V)$ such that TS=I. Similarly ST=I (Here I is identity mapping) implies that T is left invertible. An element T is called invertible or regular if it both right as well as left invertible. If T is not regular then it is called singular transformation. It may be that an element of A(V) is right invertible but not left. For example, Let F be the field of real numbers and V be the space of all polynomial in x over F. Define T on V by $f(x)T = \frac{df(x)}{dx}$ and S by $f(x)S = \int_1^x f(x)dx$. Both S and T are linear transformations. Since $f(x)(ST) \neq f(x)$ i.e. $ST \neq I$ and $f(x)(TS) = f(x)$ i.e. TS =I. Here T is right invertible while it is not left invertible.

1.3.5 Note. Since $T \in A(V)$ satisfies some polynomial over F, the polynomial of minimum degree satisfied by T is called the minimal polynomial of T over F

1.3.6 Theorem. If V is finite dimensional over F, then $T \in A(V)$ is invertible if and only if the constant term of the minimal polynomial for T is non zero.

Proof. Let $p(x) = \beta_0 + \beta_1 x + \ldots + \beta_n x^n$, $\beta_n \neq 0$, be the minimal polynomial for T over F. First suppose that $\beta_0 \neq 0$, then $0 = p(T) = \beta_0 + \beta_1 T + \ldots + \beta_n T^n$ implies that $-\beta_0 I = T(\beta_1 T + \ldots + \beta_n T^{n-1})$ or

$$I = T\left(-\frac{\beta_1}{\beta_0} - \frac{\beta_1}{\beta_0}T - \ldots - -\frac{\beta_1}{\beta_0}T^{n-1}\right) = \left(-\frac{\beta_1}{\beta_0} - \frac{\beta_1}{\beta_0}T - \ldots - -\frac{\beta_1}{\beta_0}T^{n-1}\right)T.$$

Therefore, $S = \left(-\frac{\beta_1}{\beta_0} - \frac{\beta_1}{\beta_0}T - \ldots - -\frac{\beta_1}{\beta_0}T^{n-1}\right)$ is the inverse of T.

Conversely suppose that T is invertible, yet $\beta_0 = 0$. Then $\beta_1 T + \ldots + \beta_n T^n = 0 \Rightarrow (\beta_1 T + \ldots + \beta_n T^{n-1})T = 0$. As T is invertible, on operating T^{-1} on both sides of above equations we get $(\beta_1 T + \ldots + \beta_n T^{n-1}) = 0$ i.e. T satisfies a polynomial of degree less then the degree of minimal polynomial of T, contradicting to our assumption that $\beta_0 = 0$. Hence $\beta_0 \neq 0$. It proves the result.

1.3.7 Corollary. If V is finite dimensional over F and if T $\in$A(V) is singular, then there exist non zero element S of A(V) such that ST=TS=*0*.

Proof. Let p(x)= $\beta_0+\beta_1 x+\ldots+\beta_n x^n$, $\beta_n \neq 0$ be the minimal polynomial for T over F. Since T is singular, therefore, constant term of p(x) is zero. Hence $(\beta_1 T+\ldots+\beta_n T^{n-1})T=T(\beta_1 T+\ldots+\beta_n T^{n-1})=0$. Choose $S=(\beta_1 T+\ldots+\beta_n T^{n-1})$, then S$\neq$0(if S=0, then T satisfies the polynomial of degree less than the degree of minimal polynomial of it) fulfill the requirement of the result.

1.3.8 Corollary. If V is finite dimensional over F and if T belonging to A(V) is right invertible, then it is left invertible also. In other words if T is right invertible then it is invertible.

Proof. Let U$\in$A(V) be the right inverse of T i.e. TU=I. If possible suppose T is singular, then there exist non-zero transformation S such that ST=TS=*0*. As

$$S(TU)= (ST)U$$

$\Rightarrow$ SI=*0*U $\Rightarrow$ S=*0*, a contradiction that S is non zero. This contradiction proves that T is invertible.

1.3.9 Theorem. For a finite dimensional vector space over F, T$\in$A(V) is singular if and only if there exist a v$\neq$0 in V such that vT=0.

Proof. By Corollary 1.3.7, T is singular if and only if there exist non zero element S$\in$A(V) such that ST=TS=*0*. As S is non zero, therefore, there exist an element u$\in$V such that uS$\neq$0. More over 0=u*0*=u(ST)=(uS)T. Choose v=uS, then v$\neq$0 and vT=0. It prove the result.

1.4 CHARACTERISTIC ROOTS

In rest of the results, V is always finite dimensional vector space over F.

1.4.1 Definition. For T$\in$A(V), $\lambda\in$F is called Characteristic root of T if λI-T is singular where I is identity transformation in A(V).

If T is singular, then clearly 0 is characteristic root of T.

1.4.2 Theorem. The element $\lambda\in$F is called characteristic root of T if and only there exist an element v$\neq$0 in V such that vT=λv.

Proof. Since λ is characteristic root of T, therefore, by definition the mapping $\lambda I-T$ is singular. But then by Theorem 1.3.9, $\lambda I-T$ is singular if and only if $v(\lambda I-T)=0$ for some $v\neq 0$ in V. As $v(\lambda I-T)=0 \Rightarrow v\lambda-vT=0 \Rightarrow vT=\lambda v$. Hence $\lambda\in F$ is characteristic root of T if and only there exist an element $v\neq 0$ in V such that $vT=\lambda v$.

1.4.3 Theorem. If $\lambda\in F$ is a characteristic root of T, then for any polynomial q(x) over F[x], $q(\lambda)$ is a characteristic root of q[T].

Proof. By Theorem 1.4.2, if $\lambda\in F$ is characteristic root of T then there exist an element $v\neq 0$ in V such that $vT=\lambda v$. But then $vT^2=(vT)T=(\lambda v)T=\lambda\lambda v=\lambda^2 v$. i.e. $vT^2=\lambda^2 v$. Continuing in this way we get, $vT^k=\lambda^k v$. Let $q(x)=\beta_0+\beta_1 x+\ldots+\beta_n x^n$, then $q(T)=\beta_0+\beta_1 T+\ldots+\beta_n T^n$. Now by above discussion, $vq(T)=v(\beta_0+\beta_1 T+\ldots+\beta_n T^n)=\beta_0 v+\beta_1(vT)+\ldots+\beta_n(vT^n)=\beta_0 v+\beta_1\lambda^2 v+\ldots+\beta_n\lambda^n v=(\beta_0+\beta_1\lambda^2+\ldots+\beta_n\lambda^n)v=q(\lambda)v$. Hence $q(\lambda)$ is characteristic root of q(T).

1.4.4 Theorem. If λ is characteristic root of T, then λ is a root of minimal polynomial of T. In particular, T has a finite number of characteristic roots in F.

Proof. As we know that if λ is a characteristic root of T, then for any polynomial q(x) over F, there exist a non zero vector v such that $vq(T)=q(\lambda)v$. If we take q(x) as minimal polynomial of T then $q(T)=0$. But then $vq(T)=q(\lambda)v \Rightarrow q(\lambda)v=0$. As v is non zero, therefore, $q(\lambda)=0$ i.e. λ is root of minimal polynomial of T.

1.5 CHARACTERISTIC VECTORS

1.5.1 Definition. The non zero vector $v\in V$ is called characteristic vector belonging to characteristic root $\lambda\in F$ if $vT=\lambda v$.

1.5.2 Theorem. If $v_1, v_2,\ldots,v_n$ are different characteristic vectors belonging to distinct characteristic roots $\lambda_1, \lambda_2,\ldots, \lambda_n$ respectively , then $v_1, v_2,\ldots,v_k$ are linearly independent over F.

Proof. Let if possible $v_1, v_2,\ldots,v_n$ are linearly dependent over F, then there exist a relation $\beta_1v_1+\ldots+\beta_nv_n=0$, where $\beta_1,+\ldots+\beta_n$ are all in F and not all of them are zero. In all such relation, there is one relation having as few non zero coefficient as possible. By suitably renumbering the vectors, let us assume that this shortest relation be

$$\beta_1v_1+\ldots+\beta_kv_k=0, \text{ where } \beta_1\neq0,\ldots,\beta_k\neq0. \qquad \text{(i)}$$

Applying T on both sides and using $v_iT=\lambda_iv_i$ in (i) we get

$$\lambda_1\beta_1v_1+\ldots+\lambda_k\beta_kv_k=0 \qquad \text{(ii)}$$

Multiplying (i) by λ_1 and subtracting from (ii), we obtain

$$(\lambda_2-\lambda_1)\beta_2v_2+\ldots+(\lambda_k-\lambda_1)\beta_kv_k=0$$

Now $(\lambda_i-\lambda_1)\neq0$ for $i>1$ and $\beta_2\neq0$, therefore, $(\lambda_i-\lambda_1)\beta_i\neq0$. But then we obtain a shorter relation than that in (i) between $v_1, v_2,\ldots,v_n$. This contradiction proves the theorem.

1.5.3 Corollary. If $\dim_FV=n$, then $T\in A(V)$ can have at most n distinct characteristic roots in F.

Proof. Let if possible T has more than n distinct characteristic roots in F, then there will be more than n distinct characteristic vectors belonging to these distinct characteristic roots. By Theorem 1.5.2, these vectors will be linearly independent over F. Since $\dim_FV=n$, these n+1 element will be linearly dependent, a contradiction. This contradiction proves T can have at most n distinct characteristic roots in F.

1.5.4 Corollary. If $\dim_FV=n$ and $T\in A(V)$ has n distinct characteristic roots in F. Then there is a basis of V over F which consists of characteristic vectors of T.

Proof. As T has n distinct characteristic roots in F, therefore, n characteristic vectors belonging to these characteristic roots will be linearly independent over F. As we know that if $\dim_FV=n$ then every set of n linearly independent vectors acts as basis of V(prove it). Hence set of characteristic vectors will act as basis of V over F. It proves the result.

Example. If $T\in A(V)$ and if $q(x)\in F[x]$ is such that $q(T)=0$, is it true that every root of q(x) in F is a characteristic root of T? Either prove that this is true or give an example to show that it is false.

Solution. It is not true always. For it take V, a vector space over F with $\dim_F V=2$ with v_1 and v_2 as basis element. It is clear that for $v\in V$, we have unique α, β in F such that $v=\alpha v_1+\beta v_2$. Define a transformation $T\in A(V)$ by $v_1T=v_2$ and $v_2T=0$. let λ be characteristic root of T in F, then $\lambda I-T$ is singular. It mean there exist a vector $v(\neq 0)$ in V such that

$vT=\lambda v \Rightarrow (\alpha v_1+\beta v_2)T=\lambda\alpha v_1+\lambda\beta v_2 \Rightarrow \alpha(v_1T)+\beta(v_2T)=\lambda\alpha v_1+\lambda\beta v_2 \Rightarrow \alpha v_2+\beta.0=\lambda\alpha v_1+\lambda\beta v_2$. As v is nonzero vector, therefore, at least one of α or β is nonzero. But then $\alpha v_2+\beta.0=\lambda\alpha v_1+\lambda\beta v_2$ implies that $\lambda=0$. Hence zero is the only characteristic root of T in F. If We take a polynomial $q(x)=x^2(x-1)$, then $q(T)=T^2(T-I)$. Now $v_1q(T)=((v_1T)T)(T-I)=(v_2T)(T-I)=0(T-I)=0$, $v_2q(T)=((v_2T)T)(T-I)=(0T)(T-I)=0$, therefore, $vq(T)=0 \ \forall \ v\in V$. Hence $q(T)=0$. As every root of q(x) lies in F yet every root of T is not a characteristic root of T.

Example. If $T\in A(V)$ and if $p(x)\in F[x]$ is the minimal polynomial for T over F, suppose that p(x) has all its roots in F. Prove that every root of p(x) is a characteristic root of T.

Solution. Let $p(x)= x^n + \beta_1 x^{n-1} +\ldots+\beta_0$be the minimal polynomial for T and λ be its root. Then $p(x)= (x-\lambda)(x^{n-1} + \gamma_1x^{n-2} +\ldots+\gamma_0)$. Since $p(T)=0$, therefore, $(T-\lambda)(T^{n-1} + \gamma_1 T^{n-2} +\ldots+\gamma_0)=0$. If $(T-\lambda)$ is regular then $(T^{n-1} +\gamma_1 T^{n-2} +\ldots+\gamma_0)=0$, contradicting the fact that the minimal polynomial of T is of degree n over F. Hence $(T-\lambda)$ is not regular i.e. $(T-\lambda)$ is singular and hence there exist a non zero vector v in V such that $v(T-\lambda)=0$ i.e. $vT=\lambda v$. Consequently λ is characteristic root of T.

1.6 MATRIX OF TRANSFORMATIONS

1.6.1 Notation. The matrix of T under given basis of V is denoted by m(T).

We know that for determining a transformation $T\in A(V)$ it is sufficient to find out the image of every basis element of V. Let $v_1, v_2,\ldots,v_n$ be the basis of V over F and let

$$v_1T=\alpha_{11}v_1+\alpha_{12}v_2+\ldots+\alpha_{1n}v_n$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$$

$$v_iT=\alpha_{i1}v_1+\alpha_{i2}v_2+\ldots+\alpha_{in}v_n$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$$

$$v_n T = \alpha_{n1} v_1 + \alpha_{n2} v_2 + \ldots + \alpha_{nn} v_n$$

Then matrix of T under this basis is

$$m(T)=\begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \cdots & \cdots & \cdots & \cdots\cdot \\ \alpha_{i1} & \alpha_{i2} & \cdots & \alpha_{in} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} \end{bmatrix}_{n\times n}$$

Example. Let F be the field and V be the set of all polynomials in x of degree n-1 or less. It is clear that V is a vector space over F. The dimension of this vector space is n. Let $\{1, x, x^2,\ldots, x^{n-1}\}$ be its basis. For $\beta_0+\beta_1 x+\ldots+ \beta_{n-1}x^{n-1} \in V$, Define $(\beta_0+\beta_1 x+\ldots+ \beta_{n-1}x^{n-1})D=\beta_1+2\beta_2 x^2+\ldots+n\text{-}1\beta_{n-1}x^{n-2}$. Then D is a linear transformation on V. Now we calculate the matrix of D under the basis $v_1(=1)$, $v_2(=x)$, $v_3(=x^2)$,.., $v_n(=x^{n-1})$ as:

$$v_1D=1D=0=0.v_1 + 0.v_2 + \ldots + 0.v_n$$

$$v_2D=xD=1=1.v_1 + 0.v_2 + \ldots + 0.v_n$$

$$v_3D=x^2D=2x=0.v_1 + 2.v_2 + \ldots + 0.v_n$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots$$

$$v_iD= x^{i-1}D=ix^{i-1}= 0.v_1 + 0.v_2 + \ldots iv_i + \ldots + 0.v_n$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$$

$$v_nD= x^{n-1}D=n\text{-}1x^{n-2}= 0.v_1 + 0.v_2 + \ldots + (n-1)v_{n-1} + 0.v_n$$

Then matrix of D is

$$m(D)=\begin{bmatrix} 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 2 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 3 & 0 & \cdots & 0 & 0 \\ . & . & . & . & \cdots & . & . \\ 0 & 0 & 0 & . & n-2 & 0 & 0 \\ 0 & 0 & 0 & . & \cdots & n-1 & 0 \end{bmatrix}_{n\times n}$$

Similarly we take another basis $v_1(=x^{n-1})$, $v_2(=x^{n-2})$,..., $v_n(=1)$, then matrix of D under this basis is

$$m_1(D)=\begin{bmatrix} 0 & n-1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & n-2 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 0 & n-3 & \ldots & 0 & 0 \\ 0 & \ldots & \ldots & \ldots & \ldots & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & \ldots & 0 & 1 \\ 0 & 0 & 0 & . & \ldots & \ldots & 0 \end{bmatrix}_{n\times n}$$

If we take the basis $v_1(=1)$, $v_2(=1+x)$, $v_3(=1+x^2)$,.., $v_n(=1+x^{n-1})$ then the matrix of D under this basis is obtained as:

$v_1D=1D=0=0.v_1+0.v_2+\ldots+0.v_n$

$v_2D=(1+x)D=1=1.v_1+0.v_2+\ldots+0.v_n$

$v_3D=(1+x^2)D=2x=-2+2(1+x)=-2.v_1+2.v_2+\ldots+0.v_n$

… … … …

$v_nD=x^{n-1}D=n\text{-}1x^{n-2}=-(n-1)+n\text{-}1(1+x^{n-2})=-(n-1).v_1+\ldots+(n-1)v_{n-1}+0.v_n$

Then matrix of D is

$$m_3(D)=\begin{bmatrix} 0 & 0 & 0 & 0 & \ldots & 0 & 0 \\ 1 & 0 & 0 & 0 & \ldots & 0 & 0 \\ -2 & 2 & 0 & 0 & \ldots & 0 & 0 \\ -3 & 0 & 3 & 0 & \ldots & 0 & 0 \\ . & . & . & . & \ldots & . & . \\ -(n-2) & 0 & 0 & . & n-2 & 0 & 0 \\ -(n-1) & 0 & 0 & . & \ldots & n-1 & 0 \end{bmatrix}_{n\times n}$$

1.6.3 Theorem. If V is n dimensional over F and if $T\in A(V)$ has a matrix $m_1(T)$ in the basis $v_1, v_2,\ldots,v_n$ and the matrix in the basis in the basis $w_1, w_2,\ldots,w_n$ of V over F. Then there is an element $C\in F_n$ such that $m_2(T)= Cm_1(T)C^{-1}$. In fact C is matrix of transformation $S\in A(V)$ where S is defined by $v_iS=w_i$; $1\le i\le n$.

Proof. Let $m_1(T)=(\alpha_{ij})$, therefore, for $1\le i\le n$,

$$v_iT=\alpha_{i1}v_1+\alpha_{i2}v_2+\ldots+\alpha_{in}v_n=\sum_{j=1}^{n}\alpha_{ij}v_j \qquad (1)$$

Similarly, if $m_2(T)=(\beta_{ij})$, therefore, for $1\le i\le n$,

$$w_iT=\beta_{i1}w_1+\beta_{i2}w_2+\ldots+\beta_{in}w_n=\sum_{j=1}^{n}\beta_{ij}w_j \qquad (2)$$

Since $v_iS=w_i$, the mapping one –one and onto. Using $v_iS=w_i$ in (2) we get

$$v_iST=\beta_{i1}(v_1S)+\beta_{i2}(v_2S)+\ldots+\beta_{in}(v_nS)$$
$$=(\beta_{i1}.v_1+\beta_{i2}v_2+\ldots+\beta_{in}v_n)S$$

As S is invertible, therefore, on applying S^{-1} on both sides of above equation we get $v_i\,(STS^{-1})=(\beta_{i1}.v_1+\beta_{i2}v_2+\ldots+\beta_{in}v_n)$. Then by definition of matrix we get $m_1(STS^{-1})=(\beta_{ij})= m_2(T)$. As the mapping $T\rightarrow m(T)$ is an isomorphism from A(V) to F_n, therefore, $m_1(STS^{-1})= m_1(S)m_1(T)m_1(S^{-1})= m_1(S)m_1(T)m_1(S)^{-1} = m_2(T)$. Choose $C= m_1(S)$, then the result follows.

Example. Let V be the vector space of all polynomial of degree 3 or less over the field of reals. Let $T \in A(V)$ is defined as: $(\beta_0+\beta_1x+\beta_2x^2+\beta_3x^3)T =\beta_1+2\beta_2x+3\beta_3x^2$. Then D is a linear transformation on V. The matrix of T in the basis $v_1(=1)$, $v_2(=x)$, $v_3(=x^2)$, $v_4(=x^3)$ as:

$$v_1T=1T=0=0.v_1+0.v_2+0v_3+0.v_4$$
$$v_2T=xT=1=1.v_1+0.v_2+0v_3+0.v_4$$
$$v_3T=x^2T=2x=0.v_1+2.v_2+0v_3+0.v_4$$
$$v_4T=x^3T=3x^2=0.v_1+0.v_2+3v_3+0.v_4$$

Then matrix of t is

$$m_1(D)=\begin{bmatrix}0&0&0&0\\1&0&0&0\\0&2&0&0\\0&0&3&0\end{bmatrix}$$

Similarly matrix of T in the basis $w_1(=1)$, $w_2(=1+x)$, $w_3(=1+x^2)$, $w_4(=1+x^3)$, is

$$m_2(D)=\begin{bmatrix}0&0&0&0\\1&0&0&0\\-2&2&0&0\\-3&0&3&0\end{bmatrix}.$$

If We set $v_iS=w_i$, then

$$v_1S=w_1=1=1.v_1+0.v_2+0v_3+0.v_4$$
$$v_2S=w_2=1+x=1.v_1+1.v_2+0v_3+0.v_4$$
$$v_3S=w_3=1+x^2=1.v_1+0.v_2+1v_3+0.v_4$$
$$v_4T=w_4=1+x^3=1.v_1+0.v_2+0v_3+1.v_4$$

But the C=m(S)= $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$ and C^{-1}= $\begin{bmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{bmatrix}$ and

$$Cm_1(D)C^{-1}=\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{bmatrix}=\begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ -2 & 2 & 0 & 0 \\ -3 & 0 & 3 & 0 \end{bmatrix}$$

$=m_2(D)$ as required.

1.6.3 Note. In above example we see that for given basis of V there always exist a square matrix of order equal to the $\dim_F V$. Converse part is also true. i.e. for given basis and given matrix there always exist a linear transformation. Let V be the vector space of all n-tuples over the field F, then F_n the set of all n×n matrix is an algebra over F. In fact if $v_1=(1,0,0\ldots,0)$, $v_2=(0,1,0\ldots,0)$,…, $v_n=(0,0,0\ldots,n)$, then $(\alpha_{ij})\in F_n$ acts as: $v_1(\alpha_{ij})$= first row of (α_{ij}), …, $v_i(\alpha_{ij})$= i^{th} row of (α_{ij}). We denote M_t is a square matrix of order t such that its each super diagonal entry is one and the rest of the entries are zero. For example

$$M_3=\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}_{3\times 3} \quad \text{and } M_4=\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}_{4\times 4}$$

1.7 SIMILAR TRANSFORMATIONS.

1.7.1 Definition (Similar transformations). Transformations S and T belonging to A(V) are said to similar if there exist R∈A(V) such that $RSR^{-1}=T$.

1.7.2 Definition. A subspace W of vector space V is invariant under T∈A(V) if WT⊆W. In other words wT ∈W ∀ w∈W.

1.7.3 Theorem. If subspace W of vector space is invariant under T, then T induces a linear transformation $\overline{T}$ on $\frac{V}{W}$, defined by $(v+W)\overline{T}=vT+W$. Further if T satisfies the polynomial q(x) over F, then so does $\overline{T}$.

Proof. Since the elements of $\frac{V}{W}$ are the cosets of W in V, therefore, $\overline{T}$ defined by $(v+W)\overline{T} = vT + W$ is a mapping on $\frac{V}{W}$. The mapping is well defined as $v_1 + W = v_2 + W \Rightarrow v_1 - v_2 \in W$. Since W is invariant under T, therefore, $v_1 + W = v_2 + W \Rightarrow (v_1 - v_2)T \in W$ which further implies that $v_1T + W = v_2T + W$ i.e. $(v_1 + W)\overline{T} = (v_2 + W)\overline{T}$. Further $(\alpha(v_1 + W) + \beta(v_2 + W))\overline{T} = ((\alpha v_1 + \beta v_2) + W))\overline{T} = (\alpha v_1 + \beta v_2)T + W$. Since T is linear transformation, therefore, $(\alpha v_1 + \beta v_2)T + W = \alpha(v_1T) + \beta(v_2T) + W = \alpha(v_1T) + \beta(v_2T) + W = \alpha(v_1T + W) + \beta(v_2T + W) = \alpha(v_1 + W)\overline{T} + \beta(v_2 + W)\overline{T}$ i.e. $\overline{T}$ is a linear transformation on $\frac{V}{W}$.

Now we will show that for given polynomial q(x) over F, $\overline{q(T)} = q(\overline{T})$. For given element v+W of $\frac{V}{W}$, $(v+W)\overline{T^2} = vT^2 + W = (vT)T + W = (vT + W)\overline{T} = (v+W)\overline{T}\,\overline{T} = (v+W)\overline{T}^2\ \forall$ v+W $\in \frac{V}{W}$. i.e. $\overline{T^2} = \overline{T}^2$. Similarly we can see that $\overline{T^i} = \overline{T}^i$ $\forall$ i. If $q(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n$, then $q(T) = \alpha_0 + \alpha_1 T + \ldots + \alpha_n T^n$ and $(v+W)\overline{q(T)} = (v+W)\overline{(\alpha_0 + \alpha_1 T + \ldots + \alpha_n T^n)} = v(\alpha_0 + \alpha_1 T + \ldots + \alpha_n T^n) + W = \alpha_0 v + W + \alpha_1(vT + W) + \ldots + \alpha_n(vT^n + W) = \alpha_0(v+W) + \alpha_1(v+W)\overline{T} + \ldots + \alpha_n(v+W)\overline{T^n}$. Using $\overline{T^i} = \overline{T}^i$ we get

$(v+W)\overline{q(T)} = \alpha_0(v+W) + \alpha_1(v+W)\overline{T} + \ldots + \alpha_n(v+W)\overline{T}^n = (v+W)(\alpha_0 + \alpha_1\overline{T} + \ldots + \alpha_n\overline{T}^n) = (v+W)q(\overline{T})$ i.e. $\overline{q(T)} = q(\overline{T})$. Since by given condition q(T)=*0*, therefore, *0* = $\overline{q(T)} = q(\overline{T})$. Hence $\overline{T}$ satisfies the same polynomial as satisfied by T.

1.7.4 Corollary. If subspace W of vector space is invariant under T, then T induces a linear transformation $\overline{T}$ on $\frac{V}{W}$, defined by $(v+W)\overline{T} = vT + W$ and minimal polynomial $p_1(x)$(say) of $\overline{T}$ divides the minimal polynomial $p(x)$ of T.

Proof. Since $p(x)$ is minimal polynomial of T, therefore, $p(T)=0$. But then by Theorem 1.7.3, $p(\overline{T})=0$. Further, $p_1(x)$ is minimal polynomial of $\overline{T}$, therefore, $p_1(x)$ divides $p(x)$.

1.8 CANONICAL FORM(TRIANGULAR FORM)

1.8.1 Definition. Let T be a linear transformation on V over F. The matrix of T in the basis $v_1, v_2, ..., v_n$ is called triangular if

$$v_1T = \alpha_{11} v_1,$$
$$v_2T = \alpha_{21} v_1 + \alpha_{22} v_2$$
$$\cdots \quad \cdots \quad \cdots\cdot \quad \cdots$$
$$v_iT = \alpha_{i1} v_1 + \alpha_{i2} v_2 + ...\alpha_{ii} v_i$$
$$\cdots\cdot \quad \cdots \quad \cdots\cdot\,. \quad \cdots\cdot$$
$$v_nT = \alpha_{n1} v_1 + \alpha_{n2} v_2 + ...\alpha_{nn} v_n$$

1.8.2 Theorem. If $T \in A(V)$ has all its characteristic roots in F, then there exist a basis of V in which the matrix of T is triangular.

Proof. We will prove the result by induction on $\dim_F V = n$.

Let n=1. By Corollary 1.5.3, T has exactly one distinct root λ(say) in F. Let $v(\neq 0)$ be corresponding characteristic root in V. Then $vT = \lambda v$. Since $n=1$. take $\{v\}$ as a basis of V. Now the matrix of T in this basis is $[\lambda]$. Hence the result is true for $n=1$.

Choose $n>1$ and suppose that the result holds for all transformations having all its roots in F and are defined on vector space V* having dimension less then n.

Since T has all its characteristic roots in F; let λ_1 be the root characteristic roots in F and v_1 be the corresponding characteristic vector. Hence $v_1T=\lambda_1 v_1$. Choose $W=\{\alpha v_1 \mid \alpha \in F\}$. Then W is one dimensional subspace of V. Since $(\alpha v_1)T=\alpha(v_1 T)= \alpha\lambda_1 v_1 \in W$, therefore, W is invariant under T. Let $\hat{V} = \frac{V}{W}$. Then $\hat{V}$ is a subspace of V such that $\dim_F \hat{V} = \dim_F V$-

$\dim_F W = n-1$. By Corollary 1.7.4, all the roots of minimal polynomial of induced transformation $\overline{T}$ being the roots of minimal polynomial of T, lies in F. Hence the linear transformation $\overline{T}$ in its action on $\hat{V}$ satisfies hypothesis of the theorem. Further $\dim_F \hat{V} < n$, there fore by induction hypothesis, there is a basis $\overline{v}_2(= v_2 + W)$, $\overline{v}_3(= v_3 + W)$, …, $\overline{v}_n(= v_n + W)$ of $\hat{V}$ over F such that

$$\overline{v}_2\,\overline{T} = \alpha_{22}\overline{v}_2\ ,$$

$$\overline{v}_3\,\overline{T} = \alpha_{32}\overline{v}_2 + \alpha_{33}\,\overline{v}_3\,,$$

$$\ldots.\qquad \ldots.\qquad \ldots.\qquad \ldots$$

$$\overline{v}_i\,\overline{T} = \alpha_{i2}\overline{v}_2 + \alpha_{i3}\,\overline{v}_3 + \ldots + \alpha_{ii}\overline{v}_i$$

$$\ldots.\qquad \ldots\qquad \ldots.\qquad \ldots.$$

$$\overline{v}_n\,\overline{T} = \alpha_{n2}\overline{v}_2 + \alpha_{n3}\,\overline{v}_3 + \ldots + \alpha_{nn}\overline{v}_n$$

i.e matrix of is triangular

Take a set B=$\{v_1, v_2, \ldots, v_n\}$. We will show that B is the required basis which fulfills the requirement of the theorem. As the mapping $V \to \hat{V}$ defined by $v \to \overline{v}(= v + W)\ \forall\ v \in V$ is an onto homomorphism under which $\overline{v}_2$, $\overline{v}_3$, …, $\overline{v}_n$ are the images of v_2, v_3, …, v_n respectively. Since $\overline{v}_2$, $\overline{v}_3$, …, $\overline{v}_n$ are linearly independent over F, then there pre-image vectors i.e. v_2, v_3, …, v_n are also linearly independent over F. More over v_1 can not be lineal combination of vectors v_2, v_3, …, v_n because if it is so then $\overline{v}_2$, $\overline{v}_3$, …, $\overline{v}_n$ will be linearly dependent over F. Hence the vectors v_1, v_2, …, v_n are n linearly independent vectors over F. Choose this set as the basis of V.

Since $v_1T=\lambda_1 v_1 = =\alpha_{11}v_1$ for $\alpha_{11}=\lambda_1$.

Since $\overline{v}_2\,\overline{T} = \alpha_{22}\overline{v}_2$ or $(v_2 + W)\overline{T} = \alpha_{22}v_2 + W$ or $v_2T + W = \alpha_{22}v_2 + W$. But then $v_2T - \alpha_{22}v_2 \in W$ and hence $v_2T - \alpha_{22}v_2 = \alpha_{21}v_1$. Equivalently,

$$v_2T = \alpha_{21}v_1 + \alpha_{22}v_2\,.$$

Similarly

$\overline{v}_3\,\overline{T} = \alpha_{32}\overline{v}_2 + \alpha_{33}\,\overline{v}_3 \Rightarrow v_3T = \alpha_{31}v_1 + \alpha_{32}v_2 + \alpha_{33}v_3\,.$

Continuing in this way we get that

$$\overline{v}_i\,\overline{T} = \alpha_{i2}\overline{v}_2 + \alpha_{i3}\,\overline{v}_3 + \ldots + \alpha_{ii}\overline{v}_i$$

$$\Rightarrow v_iT = \alpha_{i1}v_1 + \alpha_{i2}v_2 + ... + \alpha_{ii}v_i \quad \text{for all i, } 1 \le i \le n.$$

Hence B={v_1, v_2, …, v_n} is the required basis in which the matrix of T is triangular.

1.8.3 Theorem. If the matrix $A \in F_n$(=set of all n order square matrices over F) has all its characteristic roots in F, then there is a matrix $C \in F_n$ such that CAC^{-1} is a triangular matrix.

Proof. Let $A=[a_{ij}] \in F_n$. Further let $F^n= \{(\alpha_1, \alpha_2,\ldots,\alpha_n) | \alpha_i \in F\}$ be a vector space over F and $e_1, e_2,\ldots, e_n$ be a basis of basis of V over F. Define $T:V \to V$ by

$$e_iT = a_{i1}e_1 + a_{i2}e_2 + ... + a_{ii}e_i + ... + a_{in}e_n .$$

Then T is a linear transformation on V and the matrix of T in this basis is $m_1(T)= [a_{ij}]=A$. Since the mapping $A(V) \to F_n$ defined by $T \to m_1(T)$ is an algebra isomorphism, therefore all the characteristic roots of A are in F. Equivalently all the characteristic root of T are in F. Therefore, by Theorem 1.8.2, there exist a basis of V in which the matrix of T is triangular. Let it be $m_2(T)$. By Theorem 1.6.3, there exist an invertible matrix C in F_n such that $m_2(T)= Cm_1(T)C^{-1}= CAC^{-1}$. Hence CAC^{-1} is triangular.

1.8.4 Theorem. If V is n dimensional vector space over F and let the matrix $A \in F_n$ has n distinct characteristic roots in F, then there is a matrix $C \in F_n$ such that CAC^{-1} is a diagonal matrix.

Proof. Since all the characteristic roots of matrix A are distinct, the linear transformation T corresponding to this matrix under a given basis, also has distinct characteristic roots say $\lambda_1, \lambda_2,\ldots, \lambda_n$ in F. Let $v_1, v_2,\ldots, v_n$ be the corresponding characteristic vectors in V . But then

$$v_iT = \lambda_i v_i \;\forall\; 1 \le i \le n \qquad (1)$$

We know that vectors corresponding to distinct characteristic root are linearly independent over F. Since these are n linearly independent vectors over F and dimension of V over F is n, therefore, set B={ $v_1, v_2,\ldots, v_n$ } can be taken as basis set of V over F. Now the matrix of T in this basis is

$\begin{bmatrix} \lambda_1 & 0 & ... & 0 \\ 0 & \lambda_2 & ... & 0 \\ 0 & ... & ... & 0 \\ 0 & 0 & ... & \lambda_n \end{bmatrix}$. Now By above Theorem, there exist C in F_n such that CAC^{-1}= $\begin{bmatrix} \lambda_1 & 0 & ... & 0 \\ 0 & \lambda_2 & ... & 0 \\ 0 & ... & ... & 0 \\ 0 & 0 & ... & \lambda_n \end{bmatrix}$ is diagonal matrix.

1.8.5 Theorem. If V is n dimensional vector space over F and $T\in A(V)$ has all its characteristic roots in F, then T satisfies a polynomial of degree n over F.

Proof. By Theorem 1.8.3, we can find out a basis of V in which matrix of T is triangular i.e. we have a basis $v_1, v_2, \ldots, v_n$ of V over F such that

$$v_1T = \lambda_1 v_1$$
$$v_2T = \alpha_{21}v_1 + \lambda_2 v_2$$
$$\ldots \quad \ldots \quad \ldots \quad \ldots$$
$$v_i\,T = \alpha_{i1}v_1 + \alpha_{i2}\,v_2 + \ldots + \alpha_{i(i-1)}\,v_{i-1} + \lambda_i v_i$$
$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$$
$$v_n\,T = \alpha_{n1}v_1 + \alpha_{n2}\,v_2 + \ldots + \alpha_{n\,(n-1)}\,v_{n-1} + \lambda_n v_n$$

Equivalently,

$$v_1(T - \lambda_1) = 0$$
$$v_2(T - \lambda_2) = \alpha_{21}v_1$$
$$\ldots. \quad \ldots. \quad \ldots$$
$$v_i\,(T - \lambda_i) = \alpha_{i1}v_1 + \alpha_{i2}\,v_2 + \ldots + \alpha_{i\,(i-1)}\,v_{i-1}$$
$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$$
$$v_n\,(T - \lambda_n) = \alpha_{n1}v_1 + \alpha_{n2}\,v_2 + \ldots + \alpha_{n\,(n-1)}\,v_{n-1}\,.$$

Take the transformation

$$S = (T - \lambda_1)(T - \lambda_2)\ldots(T - \lambda_n)\,.$$

Then $v_1S = v_1\,(T - \lambda_1)(T - \lambda_2)\ldots(T - \lambda_n) = 0(T - \lambda_2)\ldots(T - \lambda_n) = 0$

$v_2S = v_2\,(T - \lambda_1)(T - \lambda_2)\ldots(T - \lambda_n) = v_2\,(T - \lambda_2)(T - \lambda_1)\ldots(T - \lambda_n)$

$= \alpha_{21}v_1(T - \lambda_1)\ldots(T - \lambda_n) = 0\,.$

Similarly we can see that $v_iS=0$ for $1\leq i \leq n$. Equivalently, $vS=0\ \forall\ v\in V$. Hence $S=(T-\lambda_1)(T-\lambda_2)...(T-\lambda_n)=0$ i.e. S is zero transformation on V. Consequently T satisfies the polynomial $(x-\lambda_1)(x-\lambda_2)...(x-\lambda_n)$ of degree n over F.

1.9 KEY WORDS

Transformations, similar transformations, characteristic roots, canonical forms.

1.10 SUMMARY

In this chapter, we study about linear transformations, Algebra of linear transformations, characteristic roots and characteristic vectors of linear transformations, matrix of transformation and canonical form (Triangular form).

1.11 SELF ASSESMENT QUESTIONS

(1) If V is a finite dimensional vector space over the field of real numbers with basis v_1 and v_2. Find the characteristic roots and corresponding characteristic vectors for T defined by

(i) $v_1T = v_1 + v_2$, $v_2T = v_1 - v_2$

(ii) $v_1T = 5v_1 + 6v_2$, $v_2T = -7v_2$

(iii) $v_1T = v_1 + 2v_2$, $v_2T = 3v_1 + 6v_2$

(2) If V is two-dimensional vector space over F, prove that every element in A(V) satisfies a polynomial of degree 2 over F

1.12 SUGGESTED READINGS:

(1) Topics in Algebra; I.N HERSTEIN, John wiley and sons, New York.

(2) Modern Algebra; SURJEET SINGH and QAZI ZAMEERUDDIN, Vikas Publications.

(3) Basic Abstract Algebra; P.B. BHATTARAYA, S.K.JAIN, S.R. NAGPAUL, Cambridge University Press, Second Edition.

MAL-521: M. Sc. Mathematics (Advance Abstract Algebra)

Lesson No. 2 **Written by Dr. Pankaj Kumar**

Lesson: Canonical forms **Vetted by Dr. Nawneet Hooda**

STRUCTURE

2.0 OBJECTIVE

Objective of this Chapter is to study Nilpotent Transformations and canonical forms of some transformations on the finite dimensional vector space V over the field F.

2.1 INTRODUCTION

Let $T \in A(V)$, V is finite dimensional vector space over F. In first chapter, we see that every T satisfies some minimal polynomial over F. If T is nilpotent transformation on V, then all the characteristic root of T lies in F. Therefore, there exists a basis of V under which matrix of T has nice form. Some time all the root of minimal polynomial of T does not lies in F. In that case we study, rational canonical form of T.

In this Chapter, in Section 2.2, we study about Nilpotent transformations. In next Section, Jordan forms of a transformation are studied. At the end of this chapter, we study, rational canonical forms.

2.2 NILPOTENT TRANSFORMATION

2.2.1 Definiton. Nilpotent transformation. A transformation $T \in A(V)$ is called nilpotent if $T^n=0$ for some positive integer n. Further if $T^r = 0$ and $T^k \neq 0$ for k<r, then T is nilpotent transformation with index of nilpotence r.

2.2.2 Theorem. Prove that all the characteristic roots of a nilpotent transformation T $\in A(V)$ lies in F.

Proof. Since T is nilpotent, let r be the index of nilpotence of T. Then $T^r=0$. Let λ be the characteristic root of T, then there exist $v(\neq 0)$ in V such that $vT=\lambda v$. As $vT^2=(vT)T= (\lambda v)T=\lambda(vT)= \lambda\lambda v =\lambda^2 v$. Therefore, continuing in this way we get $vT^3=\lambda^3 v$,…, $vT^r=\lambda^r v$. Since $T^r=0$, hence $vT^r=v0 =0$ and hence $\lambda^r v=0$. But $v\neq 0$, therefore, $\lambda^r=0$ and hence $\lambda=0$, which all lies in F.

2.2.3 Theorem. If $T\in A(V)$ is nilpotent and $\beta_0 \neq 0$, then $\beta_0+\beta_1 T+\ldots+ \beta_m T^m$; $\beta_i \in F$ is invertible.

Proof. If S is nilpotent then $S^r=0$ for some integer r. Let $\beta_0 \neq 0$, then

$$(\beta_0 + S)\left(\frac{I}{\beta_0} - \frac{S}{\beta_0^2} + \frac{S^2}{\beta_0^3} + \ldots + (-1)^{r-1}\frac{S^{r-1}}{\beta_0^r}\right)$$

$$= I - \frac{S}{\beta_0} + \frac{S}{\beta_0} - \frac{S^2}{\beta_0^2} + \frac{S^2}{\beta_0^2} + \ldots + (-1)^{r-1}\frac{S^{r-1}}{\beta_0^{r-1}} - (-1)^{r-1}\frac{S^{r-1}}{\beta_0^{r-1}} + (-1)^{r-1}\frac{S^r}{\beta_0^r}$$

= I. Hence $(\beta_0 + S)$ is invertible.

Now if $T^k=0$, then for the transformation

$$S=\beta_1 T+\ldots+ \beta_m T^m,$$

$$vS^k=v(\beta_1 T+\ldots+ \beta_m T^m)^k=vT^k(\beta_1+\ldots+ \beta_m T^{m-1})^k \ \forall\ v\in V.$$

Since $T^k=0$, therefore, $vT^k=0$ and hence $vS^k=0$ $\forall$ $v\in V$ i.e. $S^k=0$. Equivalently, S^k is a nilpotent transformation. But then by above discussion $\beta_0+S=\beta_0+\beta_1 T+\ldots+ \beta_m T^m$ is invertible if $\beta_0 \neq 0$. It proves the result.

2.2.4 Theorem. If $V= V_1\oplus V_2\oplus\ldots\oplus V_k$ where each subspace V_i of V is of dimension n_i and is invariant under $T\in A(V)$. Then a basis of V can be found so that the matrix of T in this basis is of the form $\begin{bmatrix} A_1 & 0 & 0 & \dots & 0 \\ 0 & A_2 & 0 & \dots & 0 \\ 0 & 0 & A_3 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & A_k \end{bmatrix}$ where each A_i is an $n_i \times n_i$ matrix and is the matrix of linear transformation T_i induced by T on V_i.

Proof. Since each V_i is of dimension n_i, let $\{v_1^{(1)}, v_2^{(1)}, \dots, v_{n_1}^{(1)}\}$, $\{v_1^{(2)}, v_2^{(2)}, \dots, v_{n_2}^{(2)}\}, \dots, \{v_1^{(i)}, v_2^{(i)}, \dots, v_{n_i}^{(i)}\}, \dots, \{v_1^{(k)}, v_2^{(k)}, \dots, v_{n_k}^{(k)}\}$ are the basis of V_1, V_2, …, V_i,…, V_k respectively, over F. We will show that $\{v_1^{(1)}, v_2^{(1)}, \dots, v_{n_1}^{(1)}, v_1^{(2)}, v_2^{(2)}, \dots, v_{n_2}^{(2)}, \dots, v_1^{(i)}, v_2^{(i)}, \dots, v_{n_i}^{(i)}, \dots, v_1^{(k)}, v_2^{(k)}, \dots, v_{n_k}^{(k)}\}$ is the basis of V. First we will show that these vectors are linearly independent over F. Let

$$\overbrace{\alpha_1^{(1)}v_1^{(1)} + \alpha_2^{(1)}v_2^{(1)} + \dots + \alpha_{n_1}^{(1)}v_{n_1}^{(1)}} + \overbrace{\alpha_1^{(2)}v_1^{(2)} + \alpha_2^{(2)}v_2^{(2)} + \dots + \alpha_{n_2}^{(2)}v_{n_2}^{(2)}} + \dots +$$

$$\overbrace{\alpha_1^{(i)}v_1^{(i)} + \alpha_2^{(i)}v_2^{(i)} + \dots + \alpha_{n_i}^{(i)}v_{n_i}^{(i)}} + \dots + \overbrace{\alpha_1^{(k)}v_1^{(k)} + \alpha_2^{(k)}v_2^{(k)} + \dots + \alpha_{n_k}^{(k)}v_{n_k}^{(k)}} = 0.$$

But V is direct sum of V_i's therefore, zero has unique representation i.e.

$0=0+0+\dots+0+\dots0$. Hence $\overbrace{\alpha_1^{(i)}v_1^{(i)} + \alpha_2^{(i)}v_2^{(i)} + \dots + \alpha_{n_i}^{(i)}v_{n_i}^{(i)}} = 0$ for $1 \le i \le k$. But for $1 \le i \le k$, $v_1^{(i)}, v_2^{(i)}, \dots, v_{n_i}^{(i)}$ are linearly independent over F. Hence $\alpha_1^{(i)} = \alpha_2^{(i)} = \dots = \alpha_{n_i}^{(i)} = 0$ and hence $v_1^{(1)}, v_2^{(1)}, \dots, v_{n_1}^{(1)}$, $v_1^{(2)}, v_2^{(2)}, \dots, v_{n_2}^{(2)}, \dots,$ $v_1^{(i)}, v_2^{(i)}, \dots, v_{n_i}^{(i)}, \dots, v_1^{(k)}, v_2^{(k)}, \dots, v_{n_k}^{(k)}$ are linearly independent over F. More over for $v \in V$, there exist $v_i \in V_i$ such that $v = v_1 + v_2 + \dots + v_i + \dots + v_k$. But for $1 \le i \le k$, $v_i = \alpha_1^{(i)}v_1^{(i)} + \alpha_2^{(i)}v_2^{(i)} + \dots + \alpha_{n_i}^{(i)}v_{n_i}^{(i)}$; for $1 \le t_i \le n_i$, $\alpha_j^{(i)} \in F$. Hence $v = \alpha_1^{(1)}v_1^{(1)} + \dots + \alpha_{n_1}^{(1)}v_{n_1}^{(1)} + \dots + \alpha_1^{(k)}v_1^{(k)} + \dots + \alpha_{n_k}^{(k)}v_{n_k}^{(k)}$. In other words we can say that every element of V is linear combination of $v_1^{(1)}, v_2^{(1)}, \dots, v_{n_1}^{(1)}$,

$v_1^{(2)}, v_2^{(2)},..., v_{n_2}^{(2)},\ldots, v_1^{(i)}, v_2^{(i)},..., v_{n_i}^{(i)},\quad \ldots, v_1^{(k)}, v_2^{(k)},..., v_{n_k}^{(k)}$ over F. Hence $\{v_1^{(1)}, ..., v_{n_1}^{(1)}, v_1^{(2)}, v_2^{(2)},..., v_{n_2}^{(2)},\ldots,\ v_1^{(i)}, v_2^{(i)},..., v_{n_i}^{(i)},\ \ldots, v_1^{(k)}, v_2^{(k)},..., v_{n_k}^{(k)}\}$ is a basis for V over F. Define T_i on V_i by setting $v_iT_i=v_iT\ \forall\ v_i\in V_i$. Then T_i is a linear transformation on V_i. Since V_i are linealy independent, therefore, For obtaining m(T) we proceed as:

$$v_1^{(1)}T = \alpha_{11}^{(1)}v_1^{(1)} + \alpha_{12}^{(1)}v_1^{(1)} ... + \alpha_{1n_1}^{(1)}v_{n_1}^{(1)}$$

$$= \overbrace{\alpha_{11}^{(1)}v_1^{(1)} + \alpha_{12}^{(1)}v_1^{(1)} ... + \alpha_{1n_1}^{(1)}v_{n_1}^{(1)}} + 0.v_1^{(2)} + ... + 0.v_{n_2}^{(2)} + 0.v_1^{(k)} + ... + 0.v_{n_k}^{(k)}.$$

$$v_2^{(1)}T = \alpha_{21}^{(1)}v_1^{(1)} + \alpha_{22}^{(1)}v_1^{(1)} ... + \alpha_{2n_1}^{(1)}v_{n_1}^{(1)}$$

$$= \overbrace{\alpha_{21}^{(1)}v_1^{(1)} + \alpha_{22}^{(1)}v_1^{(1)} ... + \alpha_{2n_1}^{(1)}v_{n_1}^{(1)}} + 0.v_1^{(2)} + ... + 0.v_{n_2}^{(2)} + 0.v_1^{(k)} + ... + 0.v_{n_k}^{(k)}.$$

$$\ldots \qquad \ldots \qquad \ldots \qquad \ldots.. \qquad \ldots$$

$$v_{n_1}^{(1)}T = \alpha_{n_11}^{(1)}v_1^{(1)} + \alpha_{n_12}^{(1)}v_1^{(1)} ... + \alpha_{n_1n_1}^{(1)}v_{n_1}^{(1)}$$

$$= \overbrace{\alpha_{n_11}^{(1)}v_1^{(1)} + \alpha_{n_12}^{(1)}v_1^{(1)} ... + \alpha_{n_1n_1}^{(1)}v_{n_1}^{(1)}} + 0.v_1^{(2)} + ... + 0.v_{n_2}^{(2)} + 0.v_1^{(k)} + ... + 0.v_{n_k}^{(k)}.$$

Since it is easy to see that $m(T_1)= [\alpha_{ij}^{(1)}]_{n_1\times n_1} = A_1$. Therefore, role of T on V_1 produces a part of m(T) given by $[A_1\ 0]$, here 0 is a zero matrix of order $n_1\times n-n_1$. Similarly part of m(T) obtained by the roll of T on V_2 is $[0\ A_2\ 0]$, here first 0 is a zero matrix of order $n_1\times n_1$, $A_2=[\alpha_{ij}^{(2)}]_{n_2\times n_2}$ and the last zero is a zero matrix of order $n_1\times n-n_1-n_2$. Continuing in this way we get that

$$\begin{bmatrix} A_1 & 0 & 0 & \ldots & 0 \\ 0 & A_2 & 0 & \ldots & 0 \\ 0 & 0 & A_3 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & A_k \end{bmatrix} \text{ as required.}$$

2.2.5 Theorem. If $T\in A(V)$ is nilpotent with index of nilpotence n_1, then there always exists subspaces V_1 and W invariant under T so that $V = V_1\oplus W$.

Proof. For proving the theorem, first we prove some lemmas:

Lemma 1. If $T\in A(V)$ is nilpotent with index of nilpotence n_1, then there always exists subspace V_1 of V of dimension n_1 which is invariant under T.

Proof. Since index of nilpotence of T is n_1 , therefore, $T^{n_1}=0$ and $T^k \neq 0$ for $1\leq k \leq n_1-1$. Let $v(\neq 0)\in V$. Consider the elements v, vT, vT^2, … vT^{n_1-1} of V. Take $\alpha_1 v+\alpha_2 vT+\ldots+\alpha_s vT^{(s-1)}+\ldots+\alpha_{n_1} vT^{n_1-1}=0$, $\alpha_i \in F$ and let α_s be the first non zero element in above equation. Hence $\alpha_s vT^{(s-1)}+\ldots+\alpha_{n_1} vT^{n_1-1}=0$. But then $vT^{(s-1)}(\alpha_s+\ldots+\alpha_{n_1} T^{n_1-s})=0$. As $\alpha_s \neq 0$ and T is nilpotent, therefore, $(\alpha_s+\ldots+\alpha_{n_1} T^{n_1-s})$ is invertible and hence $vT^{(s-1)}=0\ \forall\, v\in V$ i.e. $T^{(s-1)}$ *=0* for some integer less than n_1, a contradiction. Hence each $\alpha_i=0$. It means elements v, vT, vT^2,…, vT^{n_1-1} are linearly independent over F. Let V_1 be the space generated by the elements v, vT, vT^2, …, vT^{n_1-1}. Then the dimension of V_1 over F is n_1. Let $u\in V_1$, then

$$u=\beta_1 v+\ldots+\beta_{n_1-1} vT^{n_1-2}+\beta_{n_1} vT^{n_1-1} \text{ and}$$

$$uT=\beta_1 v+\ldots+\beta_{n_1-1} vT^{n_1-1}+\beta_{n_1} vT^{n_1}=\beta_1 v+\ldots+\beta_{n_1-1} vT^{n_1-1}$$

i.e. uT is also a linear combination of v, vT, vT^2, …, vT^{n_1-1} over F. Hence $uT\in V_1$. i.e. V_1 is invariant under T.

Lemma(2). If V_1 is subspace of V spanned by v, vT, vT^2, …, vT^{n_1-1}, $T\in A(V)$ is nilpotent with index of nilptence n_1 and $u\in V_1$ is such that $uT^{n_1-k}=0$; $0<k\leq n_1$, then $u=u_0T^k$ for some $u_0\in V_1$.

Proof. For $u\in V_1$, $u=\alpha_1 v+\ldots+\alpha_k vT^{(k-1)}+\alpha_{k+1} vT^k\ldots+\alpha_{n_1} vT^{n_1-1}$; $\alpha_i \in F$.

$$\text{and}\, 0=uT^{n_1-k}=(\alpha_1 v+\ldots+\alpha_k vT^{(k-1)}+\alpha_{k+1} vT^k\ldots+\alpha_{n_1} vT^{n_1-1})T^{n_1-k}$$

$$=\alpha_1 vT^{n_1-k}+\ldots+\alpha_k vT^{n_1-1}+\alpha_{k+1} vT^{n_1}\ldots+\alpha_{n_1} vT^{2n_1-k-1}$$

$=\alpha_1 vT^{n_1-k}+\ldots+\alpha_k vT^{n_1-1}$. Since $vT^{n_1-k}+\ldots+vT^{n_1-1}$ are linearly independent over F, therefore, $\alpha_1=\ldots=\alpha_k=0$. But then u=$\alpha_{k+1}vT^k + \ldots + \alpha_{n_1}vT^{n_1-1} = (\alpha_{k+1}v + \ldots + \alpha_{n_1}vT^{n_1-k})T^k$. Put $\alpha_{k+1}v + \ldots + \alpha_{n_1}vT^{n_1-k} = u_0$. Then u=$u_0T^k$. It proves the lemma.

Proof of Theorem. Since T is nilpotent with index of nilpotence n_1, then by Lemma 3, there always exist a subspace V_1 of V generated by v, vT, vT^2,…, vT^{n_1-1}. Let W be the subspace of V of maximal dimension such that

(i) $V_1 \cap W=(0)$ and (ii) W is invariant under T.

We will show that V=V_1+W. Let if possible V≠V_1+W. then there exist z∈V such that z∉V_1+W. Since $T^{n_1}=0$, therefore, $zT^{n_1} = 0$. But then there exist an integer 0 < k ≤n_1 such that $zT^k \in V_1 + W$ and $zT^i \notin V_1 + W$ for 0<i<k. Let $zT^k = u + w$. Since $0 = zT^{n_1} = z(T^kT^{n_1-k}) = (zT^k)T^{n_1-k} = (u+w)T^{n_1-k} = uT^{n_1-k} + wT^{n_1-k}$, therefore, $uT^{n_1-k} = -wT^{n_1-k}$. But then $uT^{n_1-k} \in V_1$ and W. Hence $uT^{n_1-k} = 0$. By Lemma 3, u=u_0T^k for some $u_0 \in V_1$. Hence $zT^k = u_0T^k + w$ or $(z-u_0)T^k \in W$. Take z_1=z-u_0, then $z_1T^k \in W$. Further, for i<k, $z_1T^i \notin W$ because if $z_1T^i \in W$, then $zT^i - u_0T^i \in W$. Equivalently, $zT^i \in V_1 + W$, a contradiction to our earlier assumption that i<k, $zT^i \notin V_1 + W$.

Let W_1 be the subspace generated by W, z_1, z_1T, z_1T^2,…, z_1T^{k-1}. Since z_1 does not belongs to W, therefore, W is properly contained in W_1 and hence $\dim_F W_1 > \dim_F W$. Since W is invariant under T, therefore, W_1 is also invariant under T. Now by induction hypothesis, $V_1 \cap W_1 \neq (0)$. Let $w + \alpha_1 z_1 + \alpha_2 z_1 T + \ldots + \alpha_k z_1 T^{k-1}$ be a non zero element belonging to $V_1 \cap W_1$. Here all α_i 's are not zero because then $V_1 \cap W \neq (0)$. Let α_s be the first non zero α_i. Then

$$w + \alpha_s z_1 T^{s-1} + \ldots + \alpha_k z_1 T^{k-1} = w + z_1 T^{s-1}(\alpha_s + \ldots + \alpha_k T^{k-s}) \in V_1.$$

Since $\alpha_s \neq 0$, therefore , $R = (\alpha_s + \ldots + \alpha_k T^{k-s})$ is invertible and hence

$wR^{-1} + z_1T^{s-1} \in V_1R^{-1} \subseteq V_1$. Equivalently, $z_1T^{s-1} \in V_1 + W$, a contradiction. This contradiction proves that $V=V_1+W$. Hence $V=V_1\oplus W$.

2.2.6 Theorem. If $T\in A(V)$ is nilpotent with index of nilpotence n_1, then there exist subspace $V_1, V_2, \ldots, V_r$, of dimensions $n_1, n_2,\ldots,n_r$ respectively, each V_i is invariant under T such that $V= V_1\oplus V_2\oplus\ldots\oplus V_r$, $n_1\geq n_2 \geq\ldots\geq n_r$ and dim V = $n_1+n_2+\ldots+n_r$. More over we can find a basis of V over F in which matrix of T

is of the form $\begin{bmatrix} M_{n1} & 0 & 0 & \ldots & 0 \\ 0 & M_{n2} & 0 & \ldots & 0 \\ 0 & 0 & M_{n3} & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & M_{nr} \end{bmatrix}$.

Proof. First we prove a lemma. If $T\in A(V)$ is nilpotent with index of nilpotence n_1, V_1 is a subspace of V spanned by v, vT, $vT^2, \ldots, vT^{n_1-1}$ where $v\in V$. Then M_{n_1} will be the matrix of T on V_1 under the basis $v_1 = v$, $v_2 = vT, \ldots, v_{n_1} = vT^{n_1-1}$.

Proof. Since

$$v_1T = 0.v_1+1.v_2+\ldots+0.\ v_{n_1}$$

$$v_2T=(vT)T=vT^2= v_3= 0.v_1+0.v_2+1.v_3+\ldots+0.\ v_{n_1}$$

$$\ldots \qquad \ldots \qquad \ldots \qquad \ldots$$

$$v_{n_1-1}T = (vT^{n_1-2})T = vT^{n_1-1} = v_{n_1} = 0.v_1 + 0.v_2 + \ldots + 1.v_{n_1} \text{ and}$$

$$v_{n_1}T_1 = (vT^{n_1-1})T = vT^{n_1} = 0 = 0.v_1 + 0.v_2 + \ldots + 0.v_{n_1}, \text{ therefore,}$$

the matrix of T under the basis v, vT, $vT^2, \ldots, vT^{n_1-1}$ is

$$\begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & & 1 \\ 0 & 0 & 0 & \ldots & 0 \end{bmatrix}_{n_1\times n_1} = M_{n_1}.$$

Proof of main theorem. Since by Theorem 2.2.5**,** If $T\in A(V)$ is nilpotent with index of nilpotence n_1, then there always exists subspaces V_1 and W, invariant under T so that $V = V_1\oplus W$. Now let T_2 be the transformation induced by T on W. Then $T_2^{n_1} = 0$ on W. But then there exist an integer n_2 such that $n_2 \le n_1$ and n_2 is index of nilpotene of T_2. But then we can write $W = V_2\oplus W_1$ where V_2 is subspace of V spanned by u, uT_2, $uT_2^2, \ldots, uT_2^{n_2-1}$ where $u\in V$ and W_1 is invariant subspace of V. Continuing in this way we get that

$$V= V_1\oplus V_2\oplus \ldots \oplus V_k$$

Where each V_i is n_i dimensional invariant subspace of V on which the matrix of T (i.e. matrix of T obtained by using basis of V_i) is M_{n_i} where $n_1 \ge n_2 \ge \ldots \ge n_k$ and $n_1 + n_2 + \ldots + n_k = n = \dim V$. Since $V = V_1\oplus V_2\oplus \ldots \oplus V_k$, therefore, by Theorem 2.2.4, the matrix of T i.e.

$$m(T)=\begin{bmatrix} A_1 & 0 & 0 & \ldots & 0 \\ 0 & A_2 & 0 & \ldots & 0 \\ 0 & 0 & A_3 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & A_k \end{bmatrix}$$ where each $A_i = M_{n_i}$. It proves the theorem.

2.2.8 Definition. Let $T\in A(V)$ is nilpotent transformation with index of nilpotence n_1. Then there exist subspace $V_1, V_2, \ldots, V_k$ of dimensions $n_1, n_2, \ldots, n_k$ respectively, each V_i is invariant under T such that $V = V_1\oplus V_2\oplus \ldots \oplus V_k$, $n_1 \ge n_2 \ge \ldots \ge n_k$ and $\dim V = n_1+n_2+\ldots+n_k$. These integers $n_1, n_2, \ldots, n_k$ are called invariants of T.

2.2.9 Definition. Cyclic subspace. A subspace M of dimension m is called cyclic with respect to $T \in A(V)$ if

(i) $MT^m=0$, $MT^{m-1}\neq 0$ (ii) there exist x in M such that $x, xT, \ldots, xT^{m-1}$ forms basis of M.

2.2.10 Theorem. If M is cyclic subspace with respect to T then the dimension of MT^k is m-k for all $k \le m$.

Proof. Since M is cyclic with respect to T, therefore, there exist x in M such that x, xT, …, xT^{m-1} is a basis of M. But then $z\in M$,

$$z= a_1x+ a_2xT+ \ldots+ a_m xT^{m-1};\ a_i\in F$$

Equivalently, $zT^k= a_1xT^k+ a_2xT^{k+1}+ \ldots+ a_{m-k}xT^{m-1} +..+a_m xT^{m+k}= a_1xT^k+ a_2xT^{k+1}+ \ldots+ a_{m-k}xT^{m-1}$. Hence every element z of MT^k is linear combination of m-k elements xT^k, xT^{k+1}, …,xT^{m-1} . Being a subset of linearly independent set these are linearly independent also. Hence the dimension of MT^k is m-k for all k.

2.2.11 Theorem. Prove that invariants of a nilpotent transformation are unique.

Proof. Let if possible there are two sets of invariant $n_1, n_2, \ldots, n_r$ and $m_1, m_2, \ldots, m_r$ of T. Then $V= V_1\oplus V_2\oplus\ldots\oplus V_r$ and $V= W_1\oplus W_2\oplus\ldots\oplus W_s$, where each V_i and W_i's are cyclic subspaces of V of dimension n_i and m_i respectively, We will show that r=s and $n_i=m_i$. Suppose that k be the first integer such that $n_k\neq m_k$. i.e. $n_1=m_1, n_2=m_2,\ldots, n_{k-1}=m_{k-1}$. Without loss of generality suppose that $n_k>m_k$. Consider VT^{m_k} . Then

$$VT^{m_k} = V_1T^{m_k} \oplus V_2T^{m_k} \oplus \ldots \oplus V_rT^{m_k} \text{ and}$$

$\dim(VT^{m_k})=\dim(V_1T^{m_k})+\dim(V_2T^{m_k})+\ldots+\dim(V_rT^{m_k})$. As by Theorem 2.2.10, $\dim(V_iT^{m_k})=n_i-m_k$, therefore,

$$\dim(VT^{m_k})\geq(n_1-m_k)+\ldots+(n_{k-1}-m_k) \qquad (1)$$

Similarly $\dim(VT^{m_k})=\dim(W_1T^{m_k})+\dim(W_2T^{m_k})+\ldots+\dim(W_sT^{m_k})$. As $m_j \leq m_k$ for $j \geq k$, therefore, $W_jT^{m_k}=\{0\}$ subspace and then $\dim(W_jT^{m_k})=0$. Hence $\dim(VT^{m_k})\geq(m_1-m_k)+\ldots+(m_{k-1}-m_k)$. Since $n_1=m_1$, $n_2=m_2,\ldots,n_{k-1}=m_{k-1}$, therefore, $\dim(VT^{m_k})=(n_1-m_k)+\ldots+(n_{k-1}-m_k)$, contradicting (1). Hence $n_i=m_i$. Further $n_1+n_2+\ldots+n_r=\dim V=m_1+m_2+\ldots+m_s$ and $n_i=m_i$ for all i implies that r=s. It proves the theorem.

2.2.12 Theorem. Prove that transformations S and $T\in A(V)$ are similar iff they have same invariants.

Proof. First suppose that S and T are similar i.e. there exist a regular mapping R such that $RTR^{-1}=S$. Let $n_1, n_2,\ldots, n_r$ be the invariants of S and m_1 , m_2, …, m_s are that of T. Then $V= V_1\oplus V_2\oplus\ldots\oplus V_r$ and $V= W_1\oplus W_2\oplus\ldots\oplus W_s$, where each V_i and W_i's are cyclic and invariant subspaces of V of dimension n_i and m_i respectively, We will show that r=s and $n_i=m_i$.

As $V_iS \subseteq V_i$, therefore, $V_i (RTR^{-1})\subseteq V_i \Rightarrow (V_iR)(TR^{-1}) \subseteq V_i$. Put $V_i R= U_i$. Since R is regular, therefore, dim $U_i=\dim V_i=n_i$. Further $U_iT= V_i RT= V_i SR$. As $V_iS \subseteq V_i$, therefore, $U_iT\subseteq U_i$. Equivalently we have shown that U_i is invariant under T. More over

$$V=VR= V_1R\oplus V_2R\oplus\ldots\oplus V_rR=U_1\oplus U_2\oplus\ldots\oplus U_r.$$

Now we will show that each U_i is cyclic with respect to T. Since each V_i is cyclic with respect to S and is of dimension n_i, therefore, for $v\in V_i$, v, $vS,\ldots, vS^{n_i-1}$ is basis of V_i over F. As R is regular transformation on V, therefore, vR, $vSR,\ldots, vS^{n_i-1}R$ is also a basis of V. Further $S=RTR^{-1} \Rightarrow SR=RT \Rightarrow S^2R=S(SR)=S(RT)=(SR)T=RTT= RT^2$. Similarly we have $S^tR=RT^t$. Hence $\{vR, vSR,\ldots, vS^{n_i-1}R\} = \{vR, vRT,\ldots, vRT^{n_i-1}\}$. Now vR lies in U_i whose dimension is n_i and $vR, vRT,\ldots, vRT^{n_i-1}$ are n_i elements linearly independent in U_i, the set $\{vR, vRT,\ldots, vRT^{n_i-1}\}$ becomes a basis of U_i. Hence U_i is cyclic with respect to T. Hence invariant of T are $n_1, n_2,\ldots,n_r$. As by Theorem 2.2.11, the invariants of nilpotents transformations are unique, therefore, $n_i=m_i$ and r=s.

Conversely, suppose that two nilpotent transformations R and S have same invariants. We will show that they are similar. As they have same invariants, therefore, there exist two basis say $X=\{x_1, x_2,\ldots, x_n\}$ and $Y=\{y_1, y_2,\ldots, y_n\}$of V such that the matrix of S under X is equal to matrix of T under Y is same. Let it be $A=[a_{ij}]_{n\times n}$. Define a regular mapping $R:V\to V$ by $x_iR=y_i$.

As $x_i(RTR^{-1})= x_i R(TR^{-1})= y_i TR^{-1} = (y_i T)R^{-1} =(\sum_{j=1}^{n} a_{ij}y_j)R^{-1}=$ $= \sum_{j=1}^{n} a_{ij}(y_jR^{-1}) = \sum_{j=1}^{n} a_{ij}x_j = x_i S$. Hence $RTR^{-1}=S$ i.e. S and T are similar.

2.3 CANONICAL FORM(JORDAN FORM)

2.3.1 Definition. Let W be a subspace of V invariant under $T\in A(V)$, then the mapping T_1 defined by $wT_1=wT$ is called the transformation induced by T on W.

2.3.2 Note.(i) Since W is invariant under T and $wT=wT_1$, therefore, $wT^2=(wT)T=(wT)T_1=(wT_1)T_1=wT_1^2$ $\forall$ $w\in W$. Hence $T^2=T_1^2$. Continuing in this way we get $T^k=T_1^k$. Hence on W, $q(T)=q(T_1)$ for all $q(x)\in F[x]$.

(ii) Further it is easy to see that if p(x) is minimal polynomial of T and r(T)=0, then p(x) always divides r(x).

2.3.3 Lemma. Let V_1 and V_2 be two invariant subspaces of finite dimensional vector space V over F such that $V=V_1\oplus V_2$. Further let T_1 and T_2 be the linear transformations induced by T on V_1 and V_2 respectively. If p(x) and q(x) are minimal polynomials of T_1 and T_2 respectively, then the minimal polynomial for T over F is the least common multiple of p(x) and q(x).

Proof. Let h(x)= lcm(p(x), q(x)) and r(x) be the minimal polynomial of T. Then r(T)=*0*. By Note 3.2(i), $r(T_1)=0$ and $r(T_2)=0$. By Note 3.2(ii), $p(x)|r(x)$ and $q(x)|r(x)$. Hence $h(x)|r(x)$. Now we will show that $r(x)|h(x)$. By the assumptions made in the statement of lemma we have $p(T_1)=0$ and $q(T_2)=0$. Since h(x) = lcm(p(x), q(x)), therefore, $h(x)= p(x)t_1(x)$ and $h(x)= p(x)t_2(x)$, where $t_1(x)$ and $t_2(x)$ belongs to F[x].

As $V=V_1\oplus V_2$, therefore, for $v\in V$ we have unique $v_1 \in V_1$ and $v_2 \in V_2$ such that $v = v_1 + v_2$. Now $vh(T) = v_1h(T) + v_2h(T) = v_1h(T_1) + v_2h(T_2) = v_1p(T_1)t_1(T_1) +v_2p(T_2)t_2(T_2)=0+0=0$. Since the result holds for all $v\in V$, therefore, h(T)=*0* on V. But then by Note 2.3.2(ii), $r(x)|h(x)$. Now $h(x)|r(x)$ and $r(x)|h(x)$ implies that h(x)=r(x). It proves the lemma.

2.3.4 Corollary. Let V_1, V_2 , …, V_k are invariant subspaces of finite dimensional vector space V over F such that $V=V_1\oplus V_2 \oplus\ldots \oplus V_k$.. Further let T_1 , T_2 , …, T_k be the linear transformations induced by T on V_1, V_2, …, V_k respectively. If $p_1(x)$, $p_2(x)$,…, $p_k(x)$ are their respective minimal polynomials. Then the minimal polynomial for T over F is the least common multiple of $p_1(x)$, $p_2(x),\ldots, p_k(x)$.

Proof. It's proof is trivial.

2.3.5 Theorem. If $p(x)=p_1(x)^{t_1}p_2(x)^{t_2}...p_k(x)^{t_k}$; $p_i(x)$ are irreducible factors of p(x) over F, is the minimal polynomial of T, then for $1\leq i \leq k$, the set $V_i=\{v\in V \mid vp_i(T)^{t_i}=0\}$ is non empty subspace of V invariant under T.

Proof. We will show that V_i is a subspace of V. Let v_1 and v_2 are two elements of V_i. Then by definition, $v_1p_i(T)^{t_i}=0$ and $v_2p_i(T)^{t_i}=0$. Now using linearity property of T we get $(v_1-v_2)p_i(T)^{t_i}=v_1p_i(T)^{t_i}-v_2p_i(T)^{t_i}=0$. Hence $v_1 - v_2 \in V_i$. Since minimal polynomial of T over F is p(x), therefore, $h_i(T)=p_1(T)^{t_1}...p_{i-1}(T)^{t_{i-1}}p_{i+1}(T)^{t_{i+1}}...p_k(T)^{t_k}\neq 0$. Hence there exist u in V such that $uh_i(T)\neq 0$. But $uh_i(T)p_i(T)^{t_i}=0$, therefore, $uh_i(T)\in Vi$. Hence $V_i\neq 0$. More over for $v\in V_i$, $vT(p_i(T)^{t_i})=vp_i(T)^{t_i}(T)=0T=0$. Hence vTV_i for all $v\in V_i$. Hence V_i is invariant under T. It proves the lemma.

2.3.6 Theorem. If $p(x)=p_1(x)^{t_1}p_2(x)^{t_2}...p_k(x)^{t_k}$; $p_i(x)$ are irreducible factors of p(x) over F, is the minimal polynomial of T, then for $1\leq i \leq k$, $V_i=\{v\in V \mid vp_i(T)^{t_i}=0\}\neq(0)$, $V= V_1\oplus V_2 \oplus\ldots \oplus V_k$. and the minimal polynomial for T_i is $p_i(x)^{t_i}$.

Proof. If k=1 i.e. number of irreducible factors in p(x) is one then V=V1 and the minimal polynomial of T is $p_1(x)^{t_1}$ i.e. the result holds trivially. Therefore, suppose k >1. By Theorem 2.3.5, each V_i is non zero subspace of V invariant under T. Define

$$h_1(x)=p_2(x)^{t_2}p_3(x)^{t_3}...p_k(x)^{t_k},$$

$$h_2(x)=p_1(x)^{t_1}p_3(x)^{t_3}...p_k(x)^{t_k},$$

… …. … … … …

$$h_i(x) = \prod_{\substack{j=1 \\ j \neq ij}}^{k} p_j(x)^{t_j} .$$

The polynomials $h_1(x), h_2(x), \ldots, h_k(x)$ are relatively prime. Hence we can find polynomials $a_1(x), a_2(x), \ldots, a_k(x)$ in F[x] such that

$a_1(x) h_1(x) + a_2(x) h_2(x) + \ldots + a_k(x) h_k(x) = 1$. Equivalently, we get

$a_1(T) h_1(T) + a_2(T) h_2(T) + \ldots + a_k(T) h_k(T) = I$(identity transformation).

Now for $v \in V$,

$$v = vI = v(a_1(T) h_1(T) + a_2(T) h_2(T) + \ldots + a_k(T) h_k(T))$$
$$= va_1(T) h_1(T) + va_2(T) h_2(T) + \ldots + va_k(T) h_k(T).$$

Since $va_i(T)h_i(T)p_i(T)^{t_i} = 0$, therefore, $va_i(T)h_i(T) \in V_i$. Let $va_i(T)h_i(T) = v_i$. Then $v = v_1 + v_2 + \ldots + v_k$. Thus $V = V_1 + V_2 + \ldots + V_k$. Now we will show that if $u_1 + u_2 + \ldots + u_k = 0$, $u_i \in V_i$ then each $u_i = 0$.

As $u_1 + u_2 + \ldots + u_k = 0 \Rightarrow u_1h_1(T) + u_2h_1(T) + \ldots + u_kh_1(T) = 0h_1(T) = 0$. Since $h_1(T) = p_2(T)^{t_2} p_3(T)^{t_3} \ldots p_k(T)^{t_k}$, therefore, $u_jh_1(T) = 0$ for all $j = 2, 3, \ldots, k$. But then $u_1h_1(T) + u_2h_1(T) + \ldots + u_kh_1(T) = 0 \Rightarrow u_1h_1(T) = 0$. Further $u_1p_1(T)^{t_1} = 0$. Since $\gcd(h_1(x), p_1(x)) = 1$, therefore, we can find polynomials r(x) and g(x) such that $h_1(x)r(x) + p_1(x)^{t_1} g(x) = 1$. Equivalently, $h_1(T)r(T) + p_1(T)^{t_1} g(T) = I$. Hence $u_1 = u_1I = u_1(h_1(T)r(T) + p_1(T)^{t_1} g(T))$ $= u_1h_1(T)r(T) + u_1p_1(T)^{t_1} g(T) = 0$. Similarly we can show that if $u_1 + u_2 + \ldots + u_k = 0$ then each $u_i = 0$. It proves that $V = V_1 \oplus V_2 \oplus \ldots \oplus V_k$.

Now we will prove that $p_i(x)^{t_i}$ is the minimal polynomial of T_i on V_i. Since $V_ip_i(T)^{t_i} = (0)$, therefore, $p_i(T)^{t_i} = 0$ on V_i. Hence the minimal polynomial of T_i divides $p_i(x)^{t_i}$. But then the minimal polynomial of T_i is $p_i(x)^{r_i}$; $r_i \leq t_i$ for each $i = 1, 2, \ldots, k$. By Corollary 2.3.4, the minimal polynomial of T on V is least common multiple of $p_1(x)^{r_1}, p_2(x)^{r_2}, \ldots, p_k(x)^{r_k}$ which is $p_1(x)^{r_1} p_2(x)^{r_2} \ldots p_k(x)^{r_k}$. But the minimal polynomial is in fact $p_1(x)^{t_1} p_2(x)^{t_2} \ldots p_k(x)^{t_k}$, therefore, $t_i \leq r_i$ for each $i = 1, 2, \ldots, k$. Hence we get that the minimal polynomial of T_i on V_i is $p_i(x)^{t_i}$. It proves the result.

2.3.7 Corollary. If all the distinct characteristic roots $\lambda_1, \lambda_2, \ldots, \lambda_k$ of T lies in F, then V can be written as $V = V_1 \oplus V_2 \oplus \ldots \oplus V_k$ where $V_i = \{v \in V \mid v(T-\lambda_i)^{t_i} = 0\}$ and where T_i has only one characteristic root λ_I on V_i.

Proof. As we know that if all the distinct characteristic roots of T lies in F, then every characteristic root of T is a root of its minimal polynomial and vice versa. Since the distinct characteristic roots $\lambda_1, \lambda_2, \ldots, \lambda_k$ of T lies in F. Let the multiplicity of these roots are $t_1, t_2, \ldots, t_k$. Then the minimal polynomial of T over F is $(x-\lambda_1)^{t_1}(x-\lambda_2)^{t_2}\ldots(x-\lambda_k)^{t_k}$. If we define $V_i = \{v \in V \mid v(T-\lambda_i)^{t_i} = 0\}$, then by Theorem 3.6, the corollary follows.

2.3.8 Definition. The matrix $\begin{bmatrix} \lambda & 1 & 0 & \ldots & 0 \\ 0 & \lambda & 1 & \ldots & 0 \\ 0 & 0 & \lambda & \ldots & 0 \\ \vdots & \vdots & \vdots & & 1 \\ 0 & 0 & 0 & \ldots & \lambda \end{bmatrix}_{t \times t}$ of order t is called Jordan block of order t belonging to λ. For example, $\begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$ is the Jordan block of order 2 belonging to λ.

2.3.9 Theorem. If all the distinct characteristic roots $\lambda_1, \lambda_2, \ldots, \lambda_k$ of $T \in A(V)$ lies in F, then a basis of V can be found in which the matrix of T is of the form $\begin{bmatrix} J_1 & 0 & 0 & 0 \\ 0 & J_2 & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & J_k \end{bmatrix}$ where each $J_i = \begin{bmatrix} B_{i1} & 0 & 0 & 0 \\ 0 & B_{i2} & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & B_{ir_i} \end{bmatrix}$ and where $B_{i1}, B_{i2}, \ldots, B_{ir_i}$ are basic Jordan block belonging to λ.

Proof. Since all the characteristic roots of T lies in F, the minimal polynomial of T over F will be of the form $(x-\lambda_1)^{t_1}(x-\lambda_2)^{t_2}\ldots(x-\lambda_k)^{t_k}$. If we define $V_i = \{v \in V \mid v(T-\lambda_i)^{t_i} = 0\}$, then for each i, $V_i \neq (0)$ is a subspace of V which is invariant under T and $V = V_1 \oplus V_2 \oplus \ldots \oplus V_k$ such that $(x-\lambda_i)^{t_i}$ will be the minimal polynomial of T_i. As we know that if V is direct sum of its subspaces invariant under T, then we can find a basis of V in which the matrix of T is of the form $\begin{bmatrix} J_1 & 0 & 0 & 0 \\ 0 & J_2 & 0 & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & J_k \end{bmatrix}$, where each J_i is the $n_i \times n_i$ matrix of T_i (the transformation induced by T on V_i) under the basis of V_i. Since the minimal polynomial of T_i on V_i is $(x-\lambda_i)^{t_i}$, therefore, $(T-\lambda_i I)$ is nilpotent transformation on V_i with index of nilpotence t_i. But then we can obtain a basis X_i of V_i in which the matrix of $(T-\lambda_i I)$ is of the form.

$$\begin{bmatrix} M_{i1} & 0 & 0 & 0 \\ 0 & M_{i2} & 0 & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & M_{ir_i} \end{bmatrix}_{n_i \times n_i}$$

where $i1 \geq i2 \geq \dots \geq ir_i$; $i1 + i2 + \dots + ir_i = n_i = \dim V_i$. Since $T_i = \lambda_i I + T_i - \lambda_i I$, therefore, the matrix of T_i in the basis X_i of V_i is $J_i =$ matrix of $\lambda_i I$ under the basis X_i + matrix of $T_i - \lambda_i I$ under the basis X_i. Hence

$$J_i = \begin{bmatrix} \lambda & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \lambda \end{bmatrix}_{n_i \times n_i} + \begin{bmatrix} M_{i1} & 0 & 0 & 0 \\ 0 & M_{i2} & 0 & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & M_{ir_i} \end{bmatrix}_{n_i \times n_i}$$

$= \begin{bmatrix} B_{i1} & 0 & 0 & 0 \\ 0 & B_{i2} & 0 & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & B_{ir_i} \end{bmatrix}$, B_{ij} are basic Jordan blocks. It proves the result.

2.4 CANONICAL FORM(RATIONAL FORM)

2.4.1 Definition. An abelian group M is called module over a ring R or R-module if $rm \in M$ for all $r \in R$ and $m \in M$ and

(i) $(r + s)m = rm + rs$

(ii) $r(m_1 + m_2) = rm_1 + rm_2$

(iii) $(rs)m = r(sm)$ for all $r, s \in R$ and $m, m_1, m_2 \in M$.

2.4.2 Definition. Let V be a vector space over the field F and $T\in A(V)$. For $f(x) \in F[x]$, define, $f(x)v=vf(T)$, $f(x) \in F[x]$ and $v\in V$. Under this multiplication V becomes an F[x]-module.

2.4.3 Definition. An R-module M is called cyclic module if $M =\{rm_0 \mid r\in R$ and some $m_0\in M$.

2.4.4 Result. If M is finitely generated module over a principal ideal domain R. Then M can be written as direct sum of finite number of cyclic R-modules. i.e. there exist x_1 , x_2, …, x_n in M such that

$$M=Rx_1 \oplus Rx_2 \oplus \ldots \oplus Rx_n.$$

2.4.5 Definition. Let $f(x)= a_0 + a_1x + \ldots+a_{m-1} x^{m-1} + x^m$ be a polynomial over the field F. Then the companion matrix of f(x) is $\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ \cdots & \cdots & \cdots & 1 \\ -a_0 & -a_1 & \cdots & -a_{m-1} \end{bmatrix}_{m\times m}$.

It is a square matrix $[b_{ij}]$ of order m such that $b_{i,\,i+1}=1$ for $1 \le i \le m-1$, $b_{m,\,j}= a_{j-1}$ for $1 \le j \le m$ and for the rest of entries $b_{ij}=0$. The above matrix is called companion matrix of f(x). It is denoted by C(f(x)). For example companion matrix of $1+2x -5x^2 +4x^3 + x^4$ is $\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & -2 & 5 & -4 \end{bmatrix}_{4\times 4}$

2.4.6 Note. Every F[x]-module M becomes a vector space over F.Under the multiplication $f(x)v = vf(T)$, $T\in A(V)$ and $v \in V$, V becomes a vector space over F.

2.4.7 Theorem. Let V be a vector space over F and $T\in A(V)$. If $f(x) = a_0 + a_1x + \ldots+a_{m-1} x^{m-1} + x^m$ is minimal polynomial of T over F and V is cyclic F[x]-module, then there exist a basis of V under which the matrix of T is companion matrix of f(x).

Proof. Clearly V becomes F[x]-module under the multiplication defined by $f(x)v= vf(T)$ for all $v\in V$, $T\in A(V)$. As V is cyclic F[x]-module, therefore, there exist $v_0\in V$ such that $V = F[x]v_0 =\{ f(x)v_0 \mid f(x)\in F[x]\}= \{ v_0f(T) \mid f(x)\in F[x]\}$. Now we will show that if $v_0s(T)=0$, then s(T) is zero transformation on V. Since $v = f(x)v_0$, then $vs(T) = (f(x)v_0)s(T)= (v_0 f(T))s(T) = (v_0 s(T))f(T)= 0f(T)=0$. i.e. every element of v is taken to 0 by s(T). Hence s(T) is zero transformation on V. In other words T also satisfies s(T). But then f(x) divides s(x). Hence we have shown that for a polynomial $s(x)\in F[x]$, if $v_0s(T) =0$, then $f(x) \mid s(x)$.

Now consider the set $A=\{v_0, v_0T,\ldots, v_0T^{m-1} \}$ of elements of V. We will show that it is required basis of V. Take $r_0v_0 + r_1 (v_0T) +\ldots+ r_{m-1} (v_0T^{m-1}) =0$, $r_i\in F$. Further suppose that at least one of r_i is non zero. Then $r_0v_0 + r_1 (v_0T) + \ldots + r_{m-1} (v_0T^{m-1}) = 0 \Rightarrow v_0 (r_0+ r_1 T + \ldots + r_{m-1} T^{m-1}) =0$. Then by above discussion $f(x)\mid (r_0+ r_1 T + \ldots + r_{m-1} T^{m-1})$, a contradiction. Hence if $r_0v_0 + r_1 (v_0T) +\ldots+ r_{m-1} (v_0T^{m-1}) =0$ then each $r_i =0$. ie the set A is linearly independent over F.

Take $v\in V$. Then $v = t(x)v_0$ for some $t(x)\in F[x]$. As we can write $t(x)= f(x)q(x) + r(x)$, $r(x) = r_0+ r_1x + \ldots + r_{m-1}x^{m-1}$, therefore, $t(T)= f(T)q(T) + r(T)$ where $r(T)= r_0+ r_1 T + \ldots + r_{m-1} T^{m-1}$. Hence $v = t(x)v_0 = v_0t(T) = v_0(f(T)q(T) +r(T)) = v_0f(T)q(T) + v_0r(T) = v_0r(T) = v_0 (r_0+ r_1 T + \ldots + r_{m-1} T^{m-1})= r_0v_0 + r_1 (v_0T) + \ldots + r_{m-1} (v_0T^{m-1})$. Hence every element of V is linear combination of element of the set A over F. Therefore, A is a basis of V over F.

Let $v_1 =v_0$, $v_2 =v_0T$, $v_3 =v_0T^2$, …, $v_{m-1} =v_0T^{m-2}$, $v_m =v_0T^{m-1}$. Then

$$v_1T= v_2 = 0.v_1 + 1.v_2 + 0.v_3 + \ldots+0.\, v_{m-1} +0v_m,$$
$$v_2T= v_3 = 0.v_1 + 0.v_2 + 1.v_3 + \ldots+0.\, v_{m-1} +0v_m,$$
$$\ldots \qquad \ldots \qquad \ldots \qquad \ldots,$$
$$v_{m-1}T= v_m = 0.v_1 + 0.v_2 + 0.v_3 + \ldots+0.\, v_{m-1} +1v_m.$$

Since $f(T)=0 \Rightarrow v_0 f(T) = 0 \Rightarrow v_0(a_0 + a_1T + \ldots+a_{m-1}T^{m-1} + T^m) = 0$

$$\Rightarrow a_0 v_0+ a_1 v_0T + \ldots+a_{m-1} v_0T^{m-1} + v_0T^m=0$$
$$\Rightarrow v_0T^m= -a_0 v_0 - a_1 v_0T - \ldots- a_{m-1} v_0T^{m-1} .$$

As $v_mT= v_0T^{m-1}T=v_0T^m = -a_0 v_0 - a_1 v_0T - \ldots- a_{m-1} v_0T^{m-1}$

$= -a_0 v_1 - a_1 v_2 - \ldots - a_{m-1} v_m.$

Hence the matrix under the basis $v_1 = v_0$, $v_2 = v_0T$, $v_3 = v_0T^2$, …, $v_{m-1} = v_0T^{m-2}$,

$v_m = v_0T^{m-1}$ is $\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 1 \\ -a_0 & -a_1 & \cdots & -a_{m-1} \end{bmatrix}_{m\times m}$ $= C(f(x))$. It proves the result.

2.4.8 Theorem. Let V be a finite dimensional vector space over F and $T \in A(V)$. Suppose $q(x)^t$ is the minimal polynomial for T over F, where $q(x)$ is irreducible monic polynomial over F . Then there exist a basis of V such that the matrix of T under this basis is of the form

$$\begin{bmatrix} C(q(x)^{t_1}) & 0 & \cdots & 0 \\ 0 & C(q(x)^{t_2}) & \cdots & 0 \\ 0 & 0 & \cdots & \vdots \\ 0 & 0 & \cdots & C(q(x)^{t_k}) \end{bmatrix}$$ where $t = t_1 \geq t_2 \geq \ldots \geq t_k$.

Proof. Since we know that if M is a finitely generated module over a principal ideal domain R, then M can be written as direct sum of finite number of cyclic R-submodules. We know that V is a vector space over F[x] with the scalar multiplication defined by $f(x)v = vf(T)$. As V is a finite dimensional vector space over F, therefore, it is finitely dimensional vector space over F[x] also. Thus, it is finitely generated module over F[x] (because each vector space is a module also). But then we can obtain cyclic submodules of V say $F[x]v_1$, $F[x]v_2$, …, $F[x]v_k$ such that $V = F[x]v_1 \oplus F[x]v_2 \oplus \ldots \oplus F[x]v_k$, $v_i \in V$.

Since $(F(x)v_i)\ T = (v_i\ F[T])\ T = = v_i\ (F[T]\ T) = = (v_i\ g(T)) = g(x)v_i \in F[x]v_i$. Hence each $F[x]v_i$ is invariant under T. But then we can find a basis of V in which the matrix of T is $\begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ 0 & 0 & \cdots & \vdots \\ 0 & 0 & \cdots & A_k \end{bmatrix}$ where A_i is the matrix of T under the basis of V_i. Now we claim that $A_i = C(q(x)^{t_i})$. Let $p_i(x)$ be the minimal polynomial of T_i (i.e of T on V_i). Since $w_i\, q(T)^t = 0$ for all $w_i \in F[x]v_i$, therefore, $p_i(x)$ divides $q(x)^t$. Thus $p_i = q(x)^{t_i}$. $1 \leq t_i \leq t$. Re indexing V_i, we can find $t_1 \geq t_2 \geq \ldots \geq t_k$. Since $V = F[x]v_1 \oplus F[x]v_2 \oplus \ldots$

$\oplus F[x]v_k$, therefore, the minimal polynomial of T on V is $\mathrm{lcm}(q(x)^{t_1}, q(x)^{t_2}, ..., q(x)^{t_k}) = q(x)^{t_1}$. Then $q(x)^t = q(x)^{t_1}$. Hence $t = t_1$. By Theorem 2.4.7, the matrix of T on V_i is companion matrix of monic minimal polynomial of T on V_i. Hence $A_i = C(q(x)^{t_i})$. It proves the result.

2.4.9 Theorem. Let V be a finite dimensional vector space over F and $T \in A(V)$. Suppose $q_1(x)^{t_1} q_2(x)^{t_2} ... q_k(x)^{t_k}$ is the minimal polynomial for T over F, where $q_i(x)$ are irreducible monic polynomial over F . Then there exist a basis of V such that the matrix of T under this basis is of the form

$$\begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ 0 & 0 & \cdots & \vdots \\ 0 & 0 & \cdots & A_k \end{bmatrix}_{n \times n} \quad \text{where} \quad A_i = \begin{bmatrix} C(q_i(x)^{t_{i1}}) & 0 & \cdots & 0 \\ 0 & C(q_i(x)^{t_{i2}}) & \cdots & 0 \\ 0 & 0 & \cdots & \vdots \\ 0 & 0 & \cdots & C(q_i(x)^{t_{ir_i}}) \end{bmatrix}$$

where $t_i = t_{i1} \geq t_{i2} \geq ... \geq t_{ir_i}$ for each i, $1 \leq i \leq k$, $\sum\limits_{j=1}^{r_i} t_{ij} = n_i$ and $\sum\limits_{i=1}^{r} n_i = n$.

Proof. Let $V_i = \{ v \in V \mid v\, q_i(T)^{t_i} = 0 \}$. Then each V_i is non zero invariant (under T) subspace of V and $V = V_1 \oplus V_2 \oplus \ldots \oplus V_k$. Also the minimal polynomial of T on V_i is $q_i(x)^{t_i}$. For such a V, we can find a basis of V under which the matrix of T is of the form $\begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ 0 & 0 & \cdots & \vdots \\ 0 & 0 & \cdots & A_k \end{bmatrix}_{n \times n}$. In this matrix, each A_i is a square matrix and is the matrix of T in V_i. As T has $q_i(x)^{t_i}$ as its minimal polynomial, therefore, by Theorem, 2.4.8, A_i = $\begin{bmatrix} C(q_i(x)^{t_{i1}}) & 0 & \cdots & 0 \\ 0 & C(q_i(x)^{t_{i2}}) & \cdots & 0 \\ 0 & 0 & \cdots & \vdots \\ 0 & 0 & \cdots & C(q_i(x)^{t_{ir_i}}) \end{bmatrix}$. Rest part of the result is easy to prove.

2.4.10 Definition. The polynomials $q_1(x)^{t_{11}}, ..., q_1(x)^{t_{1r_1}}, ..., q_k(x)^{t_{k1}}, ..., q_k(x)^{t_{kr_k}}$ are called elementary divisors of T.

2.4.11 Theorem. Prove that elementary divisors of T are unique.

Proof. Let $q(x) = q_1(x)^{l_1} q_2(x)^{l_2} ... q_k(x)^{l_k}$ be the minimal polynomial of T where each $q_i(x)$ is irreducible and $l_i \geq 1$. Let $V_i = \{ v \in V | \ vq_i(T)^{l_i} = 0\}$. Then V_i is a non zero invariant subspace of V, $V = V_1 \oplus V_2 \oplus \ldots \oplus V_k$ and the minimal polynomial of T on V_i i.e. of T_i, is $q_i(x)^{l_i}$. More over we can find a basis of V such that the matrix of T is $\begin{bmatrix} R_1 & \\ & R_k \end{bmatrix}$, where R_i is the matrix of T on V_i.

Since V becomes an F[x] module under the operation f(x)v=vf(T), therefore, each V_i is also an F[x]-module. Hence there exist $v_1, v_2, \ldots, v_{r_i} \in V_i$ such that $V_i = F[x]v_1 + \ldots + F[x]v_{r_i} = V_{i1} + V_{i2} + \ldots + V_{ir_i}$ where each V_{ij} is a subspace of V_i and hence of V . More over V_{ij} is cyclic F[x] module also. Let $q(x)^{l_{ij}}$ be the minimal polynomials of T on V_{ij}. Then $q(x)^{l_{ij}}$ becomes elementary divisors of T, $1 \leq i \leq k$ and $1 \leq j \leq r_i$. Thus to prove that elementary divisors of T are unique, it is sufficient to prove that for all i, $1 \leq i \leq k$, the polynomials $q_i(x)^{l_{i1}}$, $q_i(x)^{l_{i2}}, \ldots, q_i(x)^{l_{ir_i}}$ are unique. Equivalently, we have to prove the result for $T \in A(V)$, with $q(x)^l$, q(x) is irreducible as the minimal polynomial have unique elementary divisor.

Suppose $V = V_1 \oplus V_2 \oplus \ldots \oplus V_r$ and $V = W_1 \oplus W_2 \oplus \ldots \oplus W_s$ where each V_i and W_i is a cyclic F[x]-module. The minimal polynomial of T on V_i is have unique elementary divisors $q(x)^{l_i}$ where $l = l_1 \geq l_2 \geq \ldots \geq l_r$ and $l = l^*_1 \geq l^*_2 \geq \ldots \geq l^*_s$. Also $\sum_{i=1}^{r} l_i d = n = \dim V$ and $\sum_{i=1}^{s} l_i^* d = \dim V$, d is the degree of q(x). We will sow that $l_i = l^*_i$ and r=s. Suppose t is first integer such that $l_1 = l^*_1$, $l_2 = l^*_2$, …, $l_{t-1} = l^*_{t-1}$ and $l_t \neq l^*_t$. Since each V_i and W_i are invariant under T, therefore, $Vq(T)^{l^*_t} = V_1 q(T)^{l^*_t} \oplus \ldots \oplus V_r q(T)^{l^*_t}$. But then the dimension $Vq(T)^{l^*_t} = \sum_{j=1}^{r} \dim V_j q(T)^{l^*_t} \geq \sum_{j=1}^{i} \dim V_j q(T)^{l^*_t}$. Since $l_t \neq l^*_t$, without loss of generality, suppose that $l_t > l^*_t$. As $V_j q(T)^{l^*_t} = d(l_j - l^*_t)$, therefore, dim $Vq(T)^{l^*_t} \geq \sum_{j=1}^{i-1} d(l_j - l^*_t)$. Similarly dimension of $Vq(T)^{l^*_i} = \sum_{j=1}^{i-1} d(l^*_j - l^*_t) < \sum_{j=1}^{i} d(l_j - l^*_t) \leq Vq(T)^{l^*_i}$, a contradiction. Thus $l_t \leq l^*_t$. Similarly, we can show that $l_t \geq l^*_t$. Hence $l_t = l^*_t$. It holds for all t. But then r = s.

2.5 KEY WORDS

Nilpotent Transformations, similar transformations, characteristic roots, canonical forms.

2.6 SUMMARY

For T $\in$A(V), V is finite dimensional vector space over F, we study nilpotent transformation, Jordan forms and rational canonical forms.

2.7 SELF ASSESMENT QUESTIONS

(1) Show that all the characteristic root of a nilpotent transformations are zero

(2) If S and T are nilpotent transformations, then show that S+T and ST are also nilpotent.

(3) Show that S and T are similar if and only they have same elementary divisors.

2.8 SUGGESTED READINGS:

(1) Modern Algebra; SURJEET SINGH and QAZI ZAMEERUDDIN, Vikas Publications.

(2) Basic Abstract Algebra; P.B. BHATTARAYA, S.K.JAIN, S.R. NAGPAUL, Cambridge University Press, Second Edition.

MAL-521: M. Sc. Mathematics (Advance Abstract Algebra)

Lesson No. 3 **Written by Dr. Pankaj Kumar**

Lesson: Modules I **Vetted by Dr. Nawneet Hooda**

STRUCTURE

3.0 OBJECTIVE

Objective of this chapter is to study another algebraic system (modules over an arbitrary ring R) which is generalization of vector spaces over field F.

3.1 INTRODUCTION

A vector space is an algebraic system with two binary operations over a field F which satisfies certain conditions. If we take an arbitrary ring, then vector space V becomes an R-module or a module over ring R.

In first section of this chapter we study definitions and examples of modules. In section 3.3, we study about simple modules (i.e. modules having no proper submodule). In next section, semi-simple modules are studied. Free modules are studied in section 3.5. We also study ascending and descending chain conditions for submodules of given module. There are certain modules which satisfies ascending chain conditions (called as noetherian module) and descending chain conditions (called as artinian modules). Such type of modules are studied in section 3,6. At last we study noetherian and artinian rings.

3.2 MODULES(CYCLIC MODULES)

3.2.1 Definition. Let R be a ring. An additive abelian group M together with a scalar multiplication μ: $R\times M\rightarrow M$, is called a left R module if for all r, $s\in R$ and x, y $\in M$

(i) $\mu(r, (x + y)) = \mu(r, x) + \mu(r, y)$

(ii) $\mu((r + s), x) = \mu(r, x) +\mu(s, x)$

(iii) $\mu(r, sx))= \mu (rs, x)$

If we denote $\mu(r, x)$ =rx, then above conditions are equivalent to

(i) $r(x + y)) = rx + ry$

(ii) $(r + s) x = r x +s x$

(iii) $r (sx) = (rs) x$.

If R has an identity element 1 and

(iv) 1x=x for all x $\in$M. Then M is called Unitary (left) R-module

Note. If R is a division ring, then a unital (left) R-module is called as left vector space over R.

Example (i) Let Z be the ring of integer and G be any abelian group with nx defined by

$nx = x + x +...+ x$(n times) for positive n and

$nx=-x-x-...-x$(n times) for negative n and zero other wise.

Then G is an Z-module.

(ii) Every extension K of a field F is also an F-module.

(iii) R[x], the ring of polynomials over the ring R, is an R-module

3.2.2 Definition. Submodule. Let M be an R-module. Then a subset N of M is called R-submodule of M if N itself becomes a module under the same scalar multiplication defined on R and M. Equivalently, we say that if

(i) $x-y\in N$

(ii) $rx\in N$ for all x, $y\in N$ and $r\in R$.

Example (i) {0} and M are sub modules of R-module M. These are called trivial submodules.

(ii) Since 2Z (set of all even integers) is an Z-module. Then 4Z, 8Z are its Z submodules.

(iii) Each left ideal of a ring R is an R-submodule of left R-module and vice versa.

3.2.3 Theorem. If M is an left R-module and $x \in M$, then the set $Rx=\{rx| x\in R\}$ is an R-submodule of M.

Proof. As $Rx =\{rx| x\in R\}$, therefore, for r_1 and r_2 belonging to R, r_1x and r_2x belongs to Rx. Since $r_1-r_2 \in R$, therefore, $r_1x - r_2x= (r_1 - r_2)x \in Rx$. More over for r and $s\in R$, $s(rx)=(sr)x\in Rx$. Hence Rx is an R-submodule of M.

3.2.4 Theorem. If M is an R-module and $K=\{rx + nx| r\in R, n\in Z\}$ is an R-submodule of M containing x . Further if M is unital R-module then K=Rx.

Proof. Since for r_1, $r_2 \in R$ and n_1, $n_2 \in Z$ we have $r_1-r_2 \in R$ and $n_1-n_2 \in Z$, therefore, $r_1x+n_1x-(r_2x+n_2x) = r_1x - r_2x + n_1x - n_2x = (r_1-r_2)x+(n_1- n_2)x \in K$. More over for $s\in R$, $s(rx + nx) = s(rx + x +\ldots + x) = s(rx) + sx +\ldots+ sx = (sr)x + sx +\ldots+ sx= ((sr) + s + \ldots + s)x$. Since $((sr) + s + \ldots + s)\in R$, therefore, $((sr) + s +\ldots+ s)x + 0.x \in K$. Hence K is an R-submodule. As $x = 0x + 1x\in K$, therefore, K is an R-submodule containing x. Let S be another R-submodule containing x, then rx and nx $\in S$. Hence $K \subseteq S$. Therefore, K is the smallest R-submodule containing x.

If M is unital R-module, then $1\in R$ such that $1.m=m\forall m\in M$. Hence for $x \in M$, $x=1.x \in Rx$. As by Theorem 3.2.3, Rx is an R-submodule. But K is the smallest R-submodule of M containing x. Hence $K\subseteq Rx$. Now For $rx\in Rx$, $rx=rx + 0x\in K$. Hence K=Rx. It proves the theorem.

3.2.5 Definition. Let S be a subset of an R-module M. The submodule generated by S, denoted by <S> is the smallest submodule of M containing S.

3.2.6 Theorem. Let S be a subset of an R-module M. Then <S> ={0} if S=ϕ, and is $C(S)=\{ r_1 x_1+r_2 x_2 + \ldots+ r_n x_n| r_i \in R\}$ if $S=\{x_1, x_2, \ldots, x_n\}$.

Proof. Since < S > is the smallest submodule containing S, therefore, for the case when S=ϕ, < S >= {0}. Suppose that $S=\{x_1, x_2,\ldots, x_n\}$. Let x and y$\in$C(S). Then $x= r_1 x_1+r_2 x_2 + \ldots+ r_n x_n$, $y= t_1 x_1+t_2 x_2 + \ldots+ t_n x_n$, r_i and $t_i \in R$ and x-y $= (r_1-t_1)x_1+(r_2-t_2)x_2+\ldots+(r_n-t_n)x_n \in C(S)$. Similarly rx$\in$C(S) for all r$\in$R and x$\in$C(S). Therefore, C(S) is a submodule of M. Further if N is another submodule containing S then $x_1, x_2, \ldots, x_n \in N$ and hence $r_1 x_1+r_2 x_2 + \ldots+ r_n x_n \in N$ i.e. C(S) $\subseteq$ N. It shows that C(S) =<S>is the smallest such submodule.

3.2.7 Definition. Cyclic module. An R-module M is called cyclic module if it is generated by single element of M. The cyclic module generated by x is and is {rx+nx| r$\in$ R , n$\in$Z}. Further if M is an unital R-module, then < x > ={rx | r$\in$R}.

Example.(i) Every finite additive abelian group is cyclic Z-module.

(ii) Every field F as an F-module is cyclic module.

3.3 SIMPLE MODULES

3.3.1 Definition. A module M is said to be simple R-module if RM$\neq$\{0\} and the only submodules of it are {0} and M.

3.3.2 Theorem. Let M be an unital R-module. Then M is said to be simple if and only if M =Rx for every non zero x$\in$M. In other words M is simple if and only if it is generated by every non zero element x $\in$ M.

Proof. First suppose that M is simple. Consider Rx={rx | r$\in$R}. By Theorem 3.2.3, it is an R-submodule of M. As M is unital R-module, therefore, there exist 1$\in$R such that 1.m=m for all m$\in$M. Hence x($\neq$0)=1.x $\in$Rx, therefore Rx is non zero unital R-module. Since M is simple, therefore, M=Rx. It proves the result.

Conversely, suppose that M=Rx for every non zero x in M. Let A be any non zero submodule of M. Then A $\subseteq$ M. Let y be a non zero element in A. Then y$\in$M. Hence by our assumption, M=Ry. By Theorem 3.2.3, Ry is the smallest submodule containing y, therefore, $Ry \subseteq A$. hence $M \subseteq A$. Now $A \subseteq M$, $M \subseteq A$ implies that M=A i.e. M has no non zero submodule. Hence M is simple.

3.3.3 Corollary. If R is a unitary ring. Then R is a simple R-module if and only if R is a division ring.

Proof. First suppose that R is simple R-module. We will show that R is a division ring. Let x be a non zero element in R. As R is a unitary simple ring, therefore, by Theroem 3.2.8, R=Rx. As $1 \in R$ and R=Rx, therefore, $1 \in Rx$. Hence there exist a non-zero y in R such that 1=yx. i.e. inverse of non zero element exist in R. Hence R is a division ring.

Conversely suppose that R is a division ring. Since ideals of a ring are R-submodules of that ring and vice versa, therefore ideals of R will be submodules of M. But R has two ideal {0} and R itself. Hence R has only trivial submodules. Therefore, R is simple R-module.

3.3.4 Definition. A f be a mapping from an R-module M to an R-module N is called homomorphism if

(i) $f(x + y)=f(x) + f(y)$ (ii) $f(rx)=rf(x)$ for all x, $y \in M$ and $r \in R$.

It is easy to see that $f(0)=0$, $f(-x)= -f(x)$ (iii) $f(x-y)=f(x) -f(y)$.

3.3.5 Theorem (Fundamental Theorem on Homomorphism). If f is an homomorphism from R-modules M into N, then $\frac{M}{\ker f} \cong f(M)$.

3.3.6 Problem. Let R be a ring with unity and M be an R-module. Show that M is cyclic if and only if $M \cong \frac{R}{I}$, where I is left ideal of R.

Solution. First let M be cyclic i.e. M=Rx for some $x \in M$. Define a mapping $\phi: R \to M$ by $\phi(r) = rx$, $r \in R$. Since $\phi(r_1 + r_2)= (r_1 + r_2)x=r_1x + r_2x =\phi(r_1) + \phi(r_2)$ and $\phi(sr)= (sr)x = s(rx)=s\phi(r)$ for all r_1, r_2, s and r belonging to R, therefore, ϕ is an homomorphism from R to M. As M=Rx, therefore, for $rx \in M$, there exist $r \in R$ such that $\phi(r) = rx$ i.e. the mapping is onto also. Hence by Fundamental theorem on homorphism, $\frac{R}{\text{Ker}\,\phi} \cong M$. But Ker ϕ is an left ideal of R, therefore, taking Ker ϕ=I we get $M \cong \frac{R}{I}$.

Conversely suppose that $M \cong \frac{R}{I}$. Let $f : \frac{R}{I} \to M$ be an isomorphism such that f(1+I)=x. Then for r∈R, f(r+I) = f(r(1+I))=r f(1+I)=rx. i.e. we have shown that img f = {rx| r∈R}=Rx. Since image of f is M, therefore, Rx =M for some x∈M. Thus M is cyclic. It proves the result.

3.3.7 Theorem. Let N be a submodule of M. Prove that the submodules of the quotient module $\frac{M}{N}$ are of the form $\frac{U}{N}$, where U is submodule of M containing N.

Proof. Define a mapping f: $M \to \frac{M}{N}$ by f(m)=m+N ∀ m∈M. Let X be an submodule of $\frac{M}{N}$. Define U={x∈M| f(x)∈X}= { x∈M | m + N ∈X }. Let x, y∈U. Then f(x), f(y) ∈X . But then f(x−y) = f(x)−f(y) ∈X and for r∈R, f(rx)=rf(x) ∈X . Hence by definition of U, x−y and rx∈U. i.e. U is an R-submodule. Also N ⊆ U, because for all x∈N, f(x) = x + N = N = identity of X, therefore, f(x)∈M. Because f is an onto mapping, therefore, for x∈X, there always exists y ∈M, such that f(y)=x. By definition of U, y∈U. Hence X ⊆ f(U). Clearly f(U) ⊆ X. Thus X=f(U). But f(U) = $\frac{U}{N}$. Hence X =$\frac{U}{N}$. It proves the result.

3.3.8 Theorem. Let M be an unital R-module. Then the following are equivalent

(i) M is simple R-module

(ii) Every non zero element of M generates M

(iii) $M \cong \frac{R}{I}$, where I is maximal left ideal of R.

Proof. (i)⇒(ii) follows from Theroem 3.2.8.

(ii) $\Rightarrow$(iii). As every non zero element of M generates M, therefore, M is cyclic and by Problem 3.2.12, $M \cong \frac{R}{I}$. Now we have to show that I is maximal. Since M is simple, therefore, $\frac{R}{I}$ is also simple. But then I is maximal ideal of R. It proves (iii)

(iii) $\Rightarrow$(i). By (iii) $M \cong \frac{R}{I}$, I is maximal left ideal of R. Since I is maximal ideal of R, therefore, $I \neq R$. Further $1+I \in \frac{R}{I}$ and $R(\frac{R}{I}) \neq \{I\}$ implies that RM $\neq\{0\}$. Let N be a submodule of M and f is an isomorphism from M to $\frac{R}{I}$. Since f(N) is a submodule of $\frac{R}{I}$, therefore, by Theorem 3.3.7, $f(N) = \frac{J}{I}$. But I is maximal ideal of R, therefore, J=I or J=R. If J=I, then $f(N) = \{I\}$ implies that $N=\{0\}$. If J=R, then $f(N)= \frac{R}{I}$ implies that N=M. Hence M has no non-trivial submodule i.e. M is simple.

3.3.9 Theorem. (**Schur's lemma**). For a simple R-module M, $Hom_R(M, M)$ is a division ring.

Proof. Since the set of all homomorphism from M to M form the ring under the operation defines by $(f+g)(x)=f(x) + g(x)$ and $(f.g)(x)=f(g(x))$ for all f and g belonging to the set of all homomorphism and for all x belonging to M. In order to show that $Hom_R(M, M)$ is a division ring we have to show that every non zero homomorphism f has an inverse in $Hom_R(M, M)$. i.e. we have to show that f is one-one and onto. As $f : M \to M$. consider Ker f and img f. Both are submodules of M. But M is simple, therefore, ker f=$\{0\}$ or M. If ker f =M, then f becomes a zero homomorphism. But f is non zero homomorphism. Hence ker f =$\{0\}$. i.e. f is one-one.

Similarly img f=$\{0\}$ or M. If img f=$\{0\}$, then f becomes an zero mapping which is not true. Hence img f =M i.e. mapping is onto also. Hence f is invertible. Therefore, we have shown that every non zero element of $Hom_R(M, M)$ is invertible. It mean $Hom_R(M, M)$ is division ring.

3.4 SEMI-SIMPLE MODULES

3.4.1 Definition. Let M be an R-module and (N_i), $1\leq i\leq t$ be a family of submodules of M. The submodule generated by $\bigcup_{i=1}^{t} N_i$ is the smallest submodule containing all the submodules N_i. It is also called the sum of submodules N_i and is denoted by $\sum_{i=1}^{t} N_i$.

3.4.2 Theorem. Let M be an R-module and (N_i), $1\leq i\leq t$ be a family of submodules of M. Show that $\sum_{i=1}^{t} N_i = \{x_1+ x_2 + \ldots +x_t \mid x_i\in N_i\}$.

Proof. Let $S=\{x_1+ x_2 + \ldots +x_t \mid x_i\in N_i\}$. Further let x and $y\in S$. Then $x= x_1+ x_2 + \ldots + x_n$, $y= y_1 +y_2 + \ldots + y_n$, x_i and $y_i \in S$. Then $x-y =(x_1 + x_2 + \ldots + x_n) - (y_1 + y_2 + \ldots + y_n)= (x_1-y_1) + (x_2-y_2) +\ldots+(x_n-y_n) \in S$. Similarly $rx\in S$ for all $r\in R$ and $x\in S$. Therefore, S is an submodule of M.

Further if N is another left submodule containing S then $x_1, x_2, \ldots, x_n \in N$ and hence $x_1+ x_2 + \ldots + x_n \in N$ i.e. $S \subseteq N$. It shows that S is the smallest module containing each N_i. Therefore, by Definition 3.4.1, $\sum_{i=1}^{t} N_i = S=\{x_1+ x_2 + \ldots +x_t \mid x_i\in N_i\}$.

3.4.3 Note. If $\cup N_i$ is a family of submodules of M, then $\sum_{i\in\Lambda} N_i = \{ \sum_{\text{finite}} x_i \mid x_i \in N_i\}$.

3.4.4 Definition. Let $(N_i)_{i\in\Lambda}$ be a family of submodule M. The sum $\sum_{i\in\Lambda} N_i$ is called direct sum if each element x of $\sum_{i\in\Lambda} N_i$ can be uniquely written as $x =\sum x_i$, where $x_i \in N_i$ and $x_i =0$ for almost all i in index set Λ. In other words, there are finite number of x_i that are non zero in $\sum x_i$. It is denoted by $\oplus \sum_{i\in\Lambda} N_i$. Each N_i in $\oplus \sum_{i\in\Lambda} N_i$ is called a direct summand of the direct sum $\oplus \sum_{i\in\Lambda} N_i$.

3.4.5 Theroem. Let $(N_i)_{i\in\Lambda}$ be a family of submodule M. Then the following are equivalent.

(i) $\sum\limits_{i\in\Lambda} N_i$ is direct

(ii) $N_i \cap \sum\limits_{\substack{j\in\Lambda \\ j\neq i}} N_j = \{0\}$ for all i

(iii) $0=\sum x_i \in \sum\limits_{i\in\Lambda} N_i \Rightarrow x_i = 0$ for all i.

Proof. These results are easy to prove.

3.4.6 Definition. (Semi-simple module). An R-module M is called semi-simple or completely reducible if $M = \sum\limits_{i\in\Lambda} N_i$, where N_i's are simple R-submodules of M.

Example. R^3 is a semi-simple R-module.

3.4.7 Theorem. Let $M = \sum\limits_{\alpha\in\Lambda} M_\alpha$ be a sum of simple R-submodules M_α and K be a submodule of M. Then there exist a subset $\Lambda^* \subseteq \Lambda$ such that $\sum\limits_{\alpha\in\Lambda^*} M_\alpha$ is a direct sum and $M=K\oplus(\oplus \sum\limits_{\alpha\in\Lambda^*} M_\alpha)$.

Proof. Let $S=\{\Lambda^{**} \subseteq \Lambda \mid \sum\limits_{\alpha\in\Lambda^{**}} M_\alpha$ is a direct sum and $K \cap \sum\limits_{\alpha\in\Lambda^{**}} M_\alpha = \{0\}\}$. Since $\phi \subseteq \Lambda$ and $\sum\limits_{\alpha\in\phi} M_\alpha = \{0\}$, therefore, $K \cap \sum\limits_{\alpha\in\phi} M_\alpha = K\cap\{0\}=\{0\}$. Hence $\phi\in S$. Therefore, S is non empty. Further S is partial order set under the relation that for A, B $\in$S, A is in relation with B iff either $A \subseteq B$ or $B \subseteq A$. More over every chain (A_i) in S has an upper bound $\cup A_i$ in S. Thus by Zorn's lemma S has maximal element say Λ^*. Let $N=K\oplus(\oplus \sum\limits_{\alpha\in\Lambda^*} M_\alpha)$. We will show that N=M. Let $\omega \in\Lambda$. Since M_ω is simple, therefore, either $N\cap M_\omega = \{0\}$ or M_ω. If $N\cap M_\omega = \{0\}$, then $M_\omega \cap(\oplus \sum\limits_{\alpha\in\Lambda^*} M_\alpha) = \{0\}$. But then $\sum\limits_{\alpha\in\Lambda^*\cup\{\omega\}} M_\alpha$ is a direct sum having non empty intersection with K. But this contradicts the maximality of Λ^*. Thus $N \cap M_\omega = M_\omega$ i.e. $M_\omega \subseteq N$, proving that N=M.

3.4.8 **Note.** If we take K={0} module in Theorem 3.4.7, then we get the result that "If $M = \sum_{\alpha\in\Lambda} M_\alpha$ is the sum of simple R-submodules M_α, then there exist a subset $\Lambda^* \subseteq \Lambda$ such that $\sum_{\alpha\in\Lambda^*} M_\alpha$ is a direct sum and $M=\oplus \sum_{\alpha\in\Lambda^*} M_\alpha$ ".

3.4.9 **Theorem.** Let M be an R-module. Then the following conditions are equivalents

(i) M is semi-simple

(ii) M is direct sum of simple modules

(iii) Every submodule of M is direct summand of M.

Proof. (i)$\Rightarrow$(ii). Since M is semi-simple, then by definition, $M = \sum_{\alpha\in\Lambda} M_\alpha$, where N_i's are simple submodules. Also by Theorem 3.4.7, if $M = \sum_{\alpha\in\Lambda} M_\alpha$ is a sum of simple R-submodules M_α's and K be a submodule of M, then there exist a subset $\Lambda^* \subseteq \Lambda$ such that $\sum_{\alpha\in\Lambda^*} M_\alpha$ is a direct sum and $M=K\oplus(\oplus \sum_{\alpha\in\Lambda^*} M_\alpha)$. By Note 3.4.8, if we take K={0}, then $M = \oplus \sum_{\alpha\in\Lambda^*} M_\alpha$ i.e. M is direct sum of simple submodules.

(ii) $\Rightarrow$(iii). Let $M = \oplus \sum_{\alpha\in\Lambda} M_\alpha$, where each M_α is simple. Then M is sum of simple R-submodules. But then by Theorem 3.4.7, for given submodule K of M we can find a subfamily Λ^* of given family Λ of submodules such that $M=K\oplus(\oplus \sum_{\alpha\in\Lambda^*} M_\alpha)$. Take $\oplus \sum_{\alpha\in\Lambda^*} M_\alpha = M^*$. Then $M=K\oplus M^*$.Therefore, K is direct summand of M.

(iii) $\Rightarrow$(i). First we will show that M has simple submodule. Let N=Rx be a submodule of M. Since N is finitely generated module, therefore, N has a maximal element N* (say) (because every finitely generated module has a maximal element). Consider the quotient module $\frac{N}{N^*}$. Since N* is simple, therefore, $\frac{N}{N^*}$ is simple. Being a submodule of N, N* is submodule of M also. Hence N* is a direct summand of M. Therefore, there exist submodule

M_1 of M such that $M=N^*\oplus M_1$. But then $N \subseteq N^*\oplus M_1$. If $y\in N$, then $y = x + z$ where $x\in N^*$ and $z\in M_1$. Since $z = y-x \in N$ (because $y \in N$ and $x\in N^*\subseteq N$), therefore, $y-x \in N\cap M_1$. Equivalently, $y\in N^* + N\cap M_1$. Hence $N\subseteq N^* + N\cap M_1$. Since N^* and $N\cap M_1$ both are subset of N, therefore, $N^* + N\cap M_1 \subseteq N$. By above discussion we conclude that $N^* + N\cap M_1 = N$. Since $M = N^*\oplus M_1$, $(N^*\cap M_1) = \{0\}$, therefore, $N^*\cap(N\cap M_1) = (N^*\cap M_1)\cap N = \{0\}$. Hence $N= N^* \oplus (N\cap M_1)$.

$$\text{Now } \frac{N}{N^*} = \frac{N^*+N\cap M_1}{N^*} \cong \frac{N\cap M_1}{N^*\cap(N\cap M_1)} = \frac{N\cap M_1}{\{0\}} \approx N\cap M_1 .$$

Since $\frac{N}{N^*}$ is simple submodule, therefore, $(N\cap M_1)$ is also simple submodule of N and hence of M also. By above discussion we conclude that M always has a simple submodule. Take $f=\{M_\omega\}_{\omega\in\Lambda}$ as the family of all simple submodules of M. Then by above discussion $f \neq \phi$. Let $X= \sum\limits_{\omega\in\Lambda} M_\omega$. Then X is a submodule of M. By (iii), X is direct summand of M, therefore, there exist M^* such that $M=X\oplus M^*$. We will show that $M^*=\{0\}$. If M^* is non zero, then M^* has simple submodule say Y. Then $Y\in f$. Hence $Y\subseteq X$. But then $Y=X\cap M^*$, a contradiction to the result $M=X\oplus M^*$. Hence $M^*=\{0\}$ and $M= X= \sum\limits_{\omega\in\Lambda} M_\omega$ i.e. M is semi-simple and (i) follows.

3.4.10 Theorem. Prove that submodule and factor modules of a semi-simple module are again a semi-simple.

Proof. Let M be semi-simple R-module and N be a submodule of M. As M is semi-simple, therefore, every submodule of M is direct summand of M. Hence for given submodule X, there exist M^* such that $M = X\oplus M^*$. But then $N=M\cap N= X\oplus M^*\cap N=(X\cap N)\oplus(M^*\cap N)$. Hence $X\cap N$ is direct summand of N. Therefore N is semi-simple.

Now we will show that $\frac{M}{N}$ is also semi-simple. Since M is semi-simple and N is a submodule of M, therefore, N is direct summand of of M i.e. $M= N\oplus M^*$. Since $N\cap M^*=\{0\}$, therefore,

$\frac{M}{N} = \frac{N \oplus M^*}{N} \cong \frac{M^*}{N \cap M^*} = \frac{M^*}{\{0\}} = M^*$. Being a submodule of semi-simple module M, M* is semi-simple and hence $\frac{M}{N}$ is semi-simple. It proves the result.

3.5 FREE MODULES

3.5.1 Definition. Let M be an R module. A subset S of M is said to be linearly dependent over R if and only if there exist distinct elements $x_1, x_2, \ldots, x_n$ in S and elements $r_1, r_2, \ldots, r_n$ in R, not all zero such that $r_1x_1+r_2x_2+\ldots+r_nx_n=0$.

3.5.2 Definition. If the elements $x_1, x_2, \ldots, x_n$ of M are not linearly dependent over R, then we say that $x_1, x_2, \ldots, x_n$ are linearly independent over R. A subset S= $\{x_1, x_2, \ldots, x_t\}$of M is called linearly independent over ring R if elements $x_1, x_2, \ldots, x_t$ are linearly independent over R.

3.5.3 Definition. Let M be an R-module. A subset S of M is called basis of M over R if

(i) S is linearly independent over R,

(ii) $\langle S \rangle = M$. i.e. S generates M over R.

3.5.4 Definition. An R-module M is said to be free module if and only it has a basis over R

Example(i) Every vector space V over a field F is a free F-module.

(ii) Every unitary R-module, R is a free R-module.

(iii) Every Infinite abelian group is a free Z-module.

Example of an R-module M which is not free module. Show that Q (the field of rational numbers) is not a free Z-module.(Here Z is the ring of integers).

Solution. Take two non-zero rational numbers $\frac{p}{q}$ and $\frac{r}{s}$. Then there exist two integers qr and -ps such that $qr\frac{p}{q}+(-ps\frac{r}{s})=0$. i.e. every subset S of Q having two elements is Linearly dependent over Z. Hence every super set of S i.e. every subset of Q having at least two elements is linearly dependent over Z. Therefore, basis of Q over Z has at most one element. We will show the set containing single element can not be a basis of Q over Z. Let $\frac{p}{q}$ be the basis element. Then by definition of basis, $Q=\{n\frac{p}{q}, n\in Z\}$. But $\frac{p}{2q}$ belongs to Q such that $\frac{p}{2q}=\frac{1}{2}\frac{p}{q}\neq n\frac{p}{q}$. Hence $Q\neq\{n\frac{p}{q}, n\in Z\}$. In other word Q has no basis over Z. Hence Q is not free module over Z.

3.5.5 Theorem. Prove that every free R-module M with basis $\{x_1, x_2, \ldots, x_t\}$ is isomorphic to $R^{(t)}$. (Here $R^{(t)}$ is the R-module of t-tuples over R).

Proof. Since $\{x_1, x_2, \ldots, x_t\}$ is the basis of M over R, therefore, $M=\{r_1x_1+ r_2x_2 +\ldots + r_tx_t \mid r_1, r_2 ,\ldots, r_t\in R\}$. As $R^{(t)}=\{(r_1, r_2, \ldots, r_t)\mid r_1, r_2 ,\ldots, r_t\in R \}$. Define a mapping $f : M\to R^{(t)}$ by setting $f(r_1x_1+ r_2x_2 +\ldots + r_tx_t)=(r_1, r_2, \ldots, r_t)$. We will show that f is an isomorphism.

Let x and y $\in M$, then $x= r_1x_1+ r_2x_2 +\ldots + r_tx_t$ and $y= s_1x_1+ s_2x_2 +\ldots + s_tx_t$ where for each i, s_i and $r_i \in R$. Then

$$f(x+y)= f((r_1+s_1) x_1+ (r_2 + s_2)x_2 +\ldots + (r_t + s_t)x_t)$$
$$=((r_1+s_1), (r_2+s_2), \ldots , (r_t+s_t)) = (r_1 , r_2, \ldots , r_t) + (s_1, s_2 , \ldots , s_t)$$
$$= f(x)+f(y)$$

and $f(rx)= f(r(r_1x_1+ r_2x_2 +\ldots + r_tx_t)= f(rr_1x_1+r r_2x_2 +\ldots + rr_tx_t)= (rr_1, rr_2, \ldots rr_t)$ $= r(r_1, r_2, \ldots r_t)= rf(x)$. Therefore, f is an R-homomorphism.

This mapping f is onto also as for $(r_1, r_2, \ldots r_t)\in R^{(t)}$, there exist $x = r_1x_1+ r_2x_2 +\ldots + r_tx_t\in M$ such that $f(x)= (r_1, r_2, \ldots r_t)$. Further $f(x)=f(y)\Rightarrow (r_1, r_2, \ldots r_t) =(s_1, s_2 , \ldots , s_t) \Rightarrow r_i =s_i$ for each i. Hence x=y i.e. the mapping f is one-one also and hence the mapping f is an isomorphism from M to $R^{(t)}$.

3.6 NOETHERIAN AND ARTINIAN MODULES

3.6.1 Definition. Let M be a left R-module and $\{M_i\}_{i\geq 1}$ be a family of submodules of M . The family $\{M_i\}_{i\geq 1}$ is called ascending chain if $M_1 \subseteq M_2 \subseteq \ldots \subseteq M_n \subseteq \ldots$ Similarly if $M_1 \supseteq M_2 \supseteq \ldots \supseteq M_n \supseteq \ldots$, then family $\{M_i\}_{i\geq 1}$ is called descending chain.

3.6.2 Definition. An R-module M is called Noetherian if for every ascending chain of submodules of M, there exist an integer k such that $M_k = M_{k+t}$ for all $t \geq 0$. In other words $M_k = M_{k+1} = M_{k+2} = \ldots$. Equivalently, an R-module M is called Noetherian if every ascending chain becomes stationary or terminates after a finite number of terms.

If the left R-module M is Noetherian, then M is called left Noetherian and if right R-module M is Noetherian, then M is called right Noetherian.

Example. Show that Z as Z-module is Noetherian.

Solution. Since we know that Z is principal ideal ring and in a ring every ideal is submodule of Z-module Z. Consider the submodule generated by $\langle n \rangle$, $n \in Z$. Further $\langle n \rangle \subseteq \langle m \rangle$ iff $m|n$. As the number of divisors of n are finite, therefore, the number of distinct member in the ascending chain of family of submodules are finite. Hence Z is noetherian Z-module.

3.6.3 Theorem. Prove that for an left R-module M, following conditions are equivalent:

(i) M is Noetherian (ii) Every non empty family of R -module has a maximal element (iii) Every submodule of M is finitely generated.

Proof. (i) $\Rightarrow$(ii). Let f be a non empty family of submodules of M. If possible f does not have a maximal element, then for $M_1 \in f$, there exist M_2 such that $M_1 \subseteq M_2$. By our assumption, there exist M_3, such that $M_1 \subseteq M_2 \subseteq M_3$. Continuing in this way we get an non terminating ascending chain $M_1 \subseteq M_2 \subseteq M_3 \ldots$, of submodules of M, a contradiction to the fact that M is Noetherian . Hence f always have a maximal element.

(ii)$\Rightarrow$(iii). Consider a submodule N of M. Let $x_i \in N$ for i=1, 2, 3, … Consider the family f of submodules $M_1 = \langle x_1 \rangle$, $M_2 = \langle x_1, x_2 \rangle$, $M_3 = \langle x_1, x_2, x_3 \rangle$, … , of N or equivalently of M. By (ii), f has maximal element M_k(say). Definitely M_k is finitely generated. In order to show that N is finitely generated, it is sufficient to show that M_k=N. Trivially $M_k \subseteq N$. Let $x_i \in N$. Then $x_i \in M_i \subseteq M_k$ for all i. Hence $N \subseteq M_k$ i.e. M_k=N. It proves (iii).

(ii)⇒(iii). Let f be an ascending chain of submodules of M. and ascending chain is $M_1 \subseteq M_2 \subseteq M_3 \ldots$. Consider $N = \bigcup_{i \geq 1} M_i$. Then N is a submodule of M. By (iii), N is finitely generated i.e. $N = \langle x_1, x_2, \ldots, x_k \rangle$. Let M_t be the submodule in the ascending chain $M_1 \subseteq M_2 \subseteq M_3 \ldots$. such that each x_i is contained in M_t. Then $N \subseteq M_r$ for all $r \geq t$. But $M_r \subseteq N$. Then $N = M_r$. Hence $M_t = M_{t+1} = M_{t+2} = \ldots$ and hence M is Noetherian. It proves (i).

3.6.4 Definition. Let M be an left R-module and $\zeta = \{M_\lambda\}_{\lambda \in \Lambda}$ be a non empty family of submodules of M. M is called finitely co-generated if for every non empty family ζ having {0} intersection has a finite subfamily with {0} intersection.

3.6.5 Definition. Left R-module M is called Left Artinian module if every descending chain $M_1 \supseteq M_2 \supseteq M_3 \ldots$ of submodules of M becomes stationary after a finite number of steps. i.e there exist k such that $M_k = M_{k+t}$ for all $t \geq 0$.

3.6.6 Theorem. Prove that for an left R-module M, following conditions are equivalent:

(i) M is Artinian (ii) Every non empty family of R-module has a minimal element (iii) Every quotient module of M is finitely co-generated.

Proof. (i)⇒(ii). Let f be a non empty family of submodules of M. If possible f does not have a minimal element, then for $M_1 \in f$, there exist M_2 such that $M_1 \supseteq M_2$. By our assumption, there exist M_3, such that $M_1 \supseteq M_2 \supseteq M_3$. Continuing in this way we get an non terminating discending chain $M_1 \supseteq M_2 \supseteq M_3 \ldots$. , of submodules of M, a contradiction to the fact that M is Artinian. Hence f always have a minimal element.

(ii)$\Rightarrow$(iii). For a submodule N, consider the quotient module $\frac{M}{N}$. Let $\{\frac{M_\lambda}{N}\}_{\lambda\in\Lambda}$ be a family of submodules of $\frac{M}{N}$ such that $\bigcap_{\lambda\in\Lambda}\frac{M_\lambda}{N}$={N}. Since $N=\bigcap_{\lambda\in\Lambda}\frac{M_\lambda}{N}=\frac{\bigcap_{\lambda\in\Lambda}M_\lambda}{N}$, therefore $\bigcap_{\lambda\in\Lambda}M_\lambda=N$. Let $\zeta=\{M_\lambda\}_{\lambda\in\Lambda}$ and for every finite subset $\Lambda^*\subseteq\Lambda$ let $f=\{A=\bigcap_{\lambda\in\Lambda^*}M_\lambda\}$. As $M_\lambda\in f$ for all $\lambda\in\Lambda$, therefore, $\zeta\subseteq f$. i.e. $f\neq\phi$. By given condition f has a minimal element say A. Then $A=M_{\lambda_1}\cap M_{\lambda_2}\cap\ldots\cap M_{\lambda_n}$. Let $\lambda\in\Lambda$. Then $A\cap M_\lambda\subseteq A$. But A is minimal element of the collection f, therefore, $A\cap M_\lambda\neq(0)$. Hence $A\cap M_\lambda=A$ $\forall$ $\lambda\in\Lambda$. But then $A\subseteq\bigcap_{\lambda\in\Lambda}M_\lambda=N$. Since N is contained in each M_λ, therefore, $N\subseteq M_{\lambda_1}\cap M_{\lambda_2}\cap\ldots\cap M_{\lambda_n}=A$. Hence $N=A=\bigcap_{i=1}^{n}M_{\lambda_i}$. Now $\bigcap_{i=1}^{n}\frac{M_{\lambda_i}}{N}=\frac{\bigcap_{i=1}^{n}M_{\lambda_i}}{N}=\frac{N}{N}=N$. Hence there exist a subfamily $\{\frac{M_{\lambda_i}}{N}\}_{1\le i\le n}$ of the family $\{\frac{M_\lambda}{N}\}_{\lambda\in\Lambda}$ such that $\bigcap_{i=1}^{n}\frac{M_{\lambda_i}}{N}=N$. It shows that every quotient module is finitely co-generated. It proves (iii).

(iii)$\Rightarrow$(i). Let $M_1\supseteq M_2\supseteq\ldots\supseteq M_n\supseteq M_{n+1}\supseteq\ldots$be a descending chain of submodules of M. Let $N=\bigcap_{i\ge1}M_i$. Then N is a submodule of M. Consider the family $\{\frac{M_i}{N}\}_{i\ge1}$ of submodules of $\frac{M}{N}$. Since $\bigcap_{\lambda\in\Lambda}\frac{M_i}{N}=\frac{\bigcap_{i\ge1}M_i}{N}=\frac{N}{N}=N$ and $\frac{M}{N}$ is finitely co-generated, therefore, there exist a subfamily $\{\frac{M_{\lambda_i}}{N}\}_{1\le i\le n}$ of the family $\{\frac{M_i}{N}\}_{i\ge1}$ such that $\bigcap_{i=1}^{n}\frac{M_{\lambda_i}}{N}=N$. Let k= max={$\lambda_1$, λ_2, …λ_n}. Then $N=\bigcap_{i=1}^{n}\frac{M_{\lambda_i}}{N}=\frac{\bigcap_{i=1}^{n}M_{\lambda_i}}{N}=\frac{M_k}{N}\Rightarrow M_k=N$. Now $N=\bigcap_{i\ge1}M_i\subseteq M_{k+i}\subseteq M_k\subseteq N\Rightarrow$ $M_{k+i}\subseteq M_k$ for all $i\ge0$. Hence M is Artinian.

3.6.7 Theorem. Let M be Noetherian left R-module. Show that every submodule and factor module of M are also Noetherian.

Proof. Since M is Noetherian, therefore, it is finitely generated. Being a submodule of finitely module, N is also finitely generated. Hence N is also Noetherian.

Consider factor module $\frac{M}{N}$. Let $\frac{A}{N}$ be its submodule. Then A is submodule of M is Noetherian, therefore, A is finitely generated. Suppose A is generated by $x_1, x_2, \ldots, x_n$. Take arbitrary element x + N of $\frac{A}{N}$. Then $x \in A$. Therefore, $x = r_1x_1 + r_2x_2 + \ldots r_nx_n$, $r_i \in R$. But then $x + N = (r_1x_1 + r_2 x_2 + \ldots + r_nx_n) + N = r_1 (x_1 + N) + r_2 (x_2 + N) + \ldots + r_n (x_n + N)$ i.e. x +N is linear combination of $(x_1 + N)$, $(x_2 + N)$, …, $(x_n + N)$ over R. Equivalently, we have shown that $\frac{A}{N}$ is finitely generated. Hence $\frac{A}{N}$ is Noetherian. It proves the result.

3.6.8 Theorem. Let M be an left R-module. If N is a submodule of M such that N and $\frac{M}{N}$ both are Noetherian, then M is also Noetherian.

Proof. Let A be a submodule of M. In order to show M is Noetherian we will show that A is finitely generated. Since A+N is a submodule of M conting N, therefore, $\frac{A+N}{N}$ is submodule of $\frac{M}{N}$. Being a submodule of Noetherian module $\frac{A+N}{N}$ is finitely generated. As $\frac{A+N}{N} \cong \frac{A}{A \cap N}$, therefore, $\frac{A}{A \cap N}$ is also finitely generated. Let $\frac{A}{A \cap N} = \langle y_1 + (A \cap N), y_2 + (A \cap N), \ldots, y_k + (A \cap N) \rangle$. Further $A \cap N$ is a submodule of Noetherian module N, therefore, it is also finitely generated. Let $(A \cap N) = \langle x_1, x_2, \ldots, x_t \rangle$. Let $x \in A$. Then $x + (A \cap N) \in \frac{A}{A \cap N}$. Hence $x + (A \cap N) = r_1(y_1 + (A \cap N)) + r_2(y_2 + (A \cap N)) + \ldots + r_k(y_k + (A \cap N))$, $r_i \in R$. Then $x + (A \cap N) = (r_1y_1 + r_2y_2 + \ldots + r_ky_k + (A \cap N))$ or $x - (r_1y_1 + r_2y_2 + \ldots + r_ky_k) \in (A \cap N)$. Since $(A \cap N) = \langle x_1, x_2, \ldots, x_t \rangle$, therefore, $x - (r_1y_1 + r_2y_2 + \ldots + r_ky_k) = s_1x_1 + s_2x_2 + \ldots + s_tx_t$.

Equivalently $x = (r_1y_1 + r_2y_2 + \ldots + r_ky_k) + s_1x_1 + s_2x_2 + \ldots + s_tx_t$, $s_i \in R$. Now we have shown that every element of A is linear combination of elements of the set $\{r_1, r_2, \ldots, r_k, s_1, s_2, \ldots, s_t\}$ i.e. A is finitely generated. It proves the result.

3.6.9 Theorem. Let M be an left R-module and N be a submodule of M. Then M is artinian iff both N and $\frac{M}{N}$ are Artinian.

Proof. Suppose that M is Artinian. We will show that every submodule and quotient modules of M are Artinian.

Let N be a submodule of N. Consider the deccending chain $N_1 \supseteq N_2 \supseteq \ldots \supseteq N_k \supseteq N_{k+1} \supseteq \ldots$ of submodules of N. But then it becomes a descending chain of submodules of M also. Since M is Artinian, therefore, there exist a positive integer k such that $N_k = N_{k+i}$ $\forall$ $i \geq 0$. Hence N is Artinian.

Let $\frac{M}{N}$ be a factor module of M. Consider a descending chain

$\frac{M_1}{N} \supseteq \frac{M_2}{N} \supseteq \ldots \supseteq \frac{M_k}{N} \supseteq \frac{M_{k+1}}{N} \supseteq \ldots$, M_i are submodules of M containing N and are contained in M_{i-1}. Thus we have a descending chain

$M_1 \supseteq M_2 \supseteq \ldots \supseteq M_k \supseteq M_{k+1} \supseteq \ldots$ of submodules of M. Since M is Artinian, therefore, there exist a positive integer K such that $M_k = M_{k+i}$ $\forall$ $i \geq 0$. But then $\frac{M_k}{N} = \frac{M_{k+i}}{N}$ $\forall$ $i \geq 0$. Hence $\frac{M}{N}$ is Artinain.

Conversely suppose that both N and $\frac{M}{N}$ are Artinian submodules of M. We will show that M is Artinian. Let $N_1 \supseteq N_2 \supseteq \ldots \supseteq N_k \supseteq N_{k+1} \supseteq \ldots$ be the deccending chain of submodules of M. Since N_i+N is a submodule of M containing N, therefore, for each i, $\frac{N_i + N}{N}$ is a submodule of $\frac{M}{N}$ such that $\frac{N_i + N}{N} \supseteq \frac{N_{i+1} + N}{N}$. Consider descending chain $\frac{N_1 + N}{N} \supseteq \frac{N_2 + N}{N} \supseteq \ldots \supseteq \frac{N_k + N}{N} \supseteq \frac{N_{k+1} + N}{N} \supseteq \ldots$ of submodules of $\frac{M}{N}$. As $\frac{M}{N}$ is Artinian, therefore, there exist a positive integer k_1 such that

$\frac{N_{k_1}+N}{N} = \frac{N_{k_1+i}+N}{N}$ for all i ≥ 0. But then $N_{k_1}+N = N_{k_1+i}+N$ for all i ≥ 0.

Since $N_i \cap N$ is a submodule of an Artinian module N and $N_i \cap N \supseteq N_{i+1} \cap N$ for all i, therefore, for descending chain $N_1 \cap N \supseteq N_2 \cap N \supseteq ... \supseteq N_k \cap N \supseteq ... N_l \cap N$ of submodules of N, there exist a positive integer k_2 such that $N_{k_2} \cap N = N_{k_2+i} \cap N$ for all i ≥ 0. Let $k=\max\{k_1, k_2\}$. Then $N_k + N = N_{k+i}+N$ and $N_k \cap N = N_{k+i} \cap N$ for all i ≥ 0. Now we will show that if $N_k + N = N_{k+i}+N$ and $N_k \cap N = N_{k+i} \cap N$, then $N_k = N_{k+i}$ for all i ≥ 0. Let $x \in N_k$, then $x \in N_k + N = N_{k+i}+N$. Thus $x = y+z$ where $y \in N_{k+i}$ and $z \in N$. Equivalently, $x-y=z \in N$. Since $y \in N_{k+i}$, therefore, $y \in N_k$ also. But then $x-y=z$ also belongs to N_k. Hence $z \in N_k \cap N = N_{k+i} \cap N$ and hence $z=x-y \in N_{k+i}$. Now $x-y \in N_{k+i}$ and $y \in N_{k+i}$ implies that $x \in N_{k+i}$. In other words we have shown that $N_k \subseteq N_{k+i}$. But then $N_k = N_{k+i}$ for all i ≥ 0. It proves the result.

3.6.10 Theorem. Prove that R-homomorphic image of Noetherian(Artinian) left R-module is again Noetherian(Artinian).

Proof. Since homomorphic image of an Noetherian(Artinian) module M is f(M) where f is an homomorphism from M to R-module N. Being a factor module of M, $\frac{M}{\mathrm{Ker} f}$ is Noetherian(Artinian). As $f(M) \cong \frac{M}{\mathrm{Ker} f}$, therefore, f(M) is also Noetherian(Artinian).

3.7 NOETHERIAN AND ARTINIAN RINGS

3.7.1 Definition. A ring R is said to satisfy ascending (descending) chain condition denoted by acc(dcc) for ideals if and only if given any sequence of ideals I_1, I_2, I_3… of R with $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots (I_1 \supseteq I_2 \supseteq \ldots \supseteq I_n \supseteq \ldots)$, there exist an positive integer n such that $I_n = I_m$ for all $m \geq n$.

Similarly a ring R is said to satisfy ascending (descending) chain condition for left (right) ideals if and only if given any sequence of left ideals

$I_1, I_2, I_3\ldots$ of R with $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots(I_1 \supseteq I_2 \supseteq \ldots \supseteq I_n \supseteq \ldots)$, there exist an positive integer n such that $I_n=I_m$ for all $m \geq n$.

3.7.2 Definition. A ring R is said to be Notherian(Artinian) ring if and only if it satisfies the ascending ()chain conditions for ideals of R. Similarly for non commutative ring , a ring R is said to be left-Notherian(left-Notherian) ring if and only if it satisfies the ascending chain conditions for left ideals (right ideals) of R.

3.7.3 Definition. A ring R is said to satisfies the maximum condition if every non empty set of ideals of R , partially ordered by inclusion, has a maximal element.

3.7.4 Theorem. Let R be a ring then the following conditions are equivalent:

(i) R is Noetherian (ii) Maximal condition (for ideals) holds in R (iii) every ideal of R is finitely generated.

Proof. (i) ⇒(ii). Let f be a family of non empty collection of ideals of R and $I_1 \in$f. If $I_1 \in$ is not maximal element in f, then ther exist $I_2 \in f$ such that $I_1 \subseteq I_2$. Again if I_2 is not maximal then there exist $I_3 \in f$ such that $I_1 \subseteq I_2 \subseteq I_3$. If f has no maximal element, then continuing in this way we get an non terminating ascending chain of ideal of R. But it is contradiction to (i) that R is noehterian. Hence f has maximal element.

(ii) ⇒(iii). Let I be an ideal of R and f={A | A is an ideal of R, A is finitely generated and $A \subseteq I$}. As $\{0\} \subseteq I$ which is finitely generated ideal of R, therefore, $\{0\} \in$f. By (ii), f has maximal element say M. We will show that M=I. Suppose that $M \neq I$, then there exist an element $a \in I$ such that $a \notin M$. Since M is finitely generated, therefore, $M=< a_1, a_2, \ldots, a_k >$. But then $M^*=< a_1, a_2, \ldots, a_k, a >$ is also finitely generated submodule of I containing M properly. By definition M* belongs to f, a contradiction to the fact that M is maximal ideal of f. Hence M=I. But then I is finitely generated. It proves (iii).

(iii) ⇒(i). $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots \subseteq I_n \subseteq \ldots$ be an ascending chain of ideals of R. Then $\bigcup_{i \geq 1} I_i$ is an ideal of R. By (iii) it is finitely generated. Let $\bigcup_{i \geq 1} I_i =<a_1, a_2,\ldots,a_k>$.

Now each a_i belongs to some I_{λ_i} of the given chain. Let $n=\max\{\lambda_1, \lambda_2, \ldots,\lambda_k\}$.

Then each $a_i \in I_n$. Consequently, for $m \geq n$, $\bigcup_{i\geq 1} I_i = \langle a_1, a_2,\ldots,a_k\rangle \subseteq I_n \subseteq I_m \subseteq \bigcup_{i\geq 1} I_i$.

Hence $I_n=I_m$ for $m\geq n$ implies that the given chain of ideals becomes stationary at some point i.e. R is Noetherian.

3.8 KEY WORDS

Modules, simple modules, semi simple modules, Noethrian, Artinian.

3.9 SUMMARY

In this chapter, we study about modules, simple modules (i.e. modules having no proper submodule), semi-simple modules , Free modules, Noetherian and Artinian rings and modules.

3.10 SELF ASSESMENT QUESTIONS

(1) Let R be a noethrian ring**.** Show that the ring of square matrices over R is also noetherian.

(2) Show that if R_i, i=1, 2, 3, … is an infinite family of non zero rings and if R is direct sum of member of this family. Then R can not be noetherian.

(3) Let M be a completely reducible module, and let K be a non zero submodule of M. Show that K is completely reducible. Also show that K is direct summand of M.

3.11 SUGGESTED READINGS

(1) Modern Algebra; SURJEET SINGH and QAZI ZAMEERUDDIN, Vikas Publications.

(2) Basic Abstract Algebra; P.B. BHATTARAYA, S.K.JAIN, S.R. NAGPAUL, Cambridge University Press, Second Edition.

MAL-521: M. Sc. Mathematics (Advance Abstract Algebra)

Lesson No. 4 **Written by Dr. Pankaj Kumar**

Lesson: Modules II **Vetted by Dr. Nawneet Hooda**

STRUCTURE

4.0 OBJECTIVE

Objective of this paper is to study some more properties of modules

4.1 INTRODUCTION

In last chapter, we have studied some more results on modules and rings. In Section, 4.2, we study more results on noetherian and artinian modules and rings. In next section, Weddernburn theorem is studied. Uniform modules, primary modules, noether-laskar theorem and smith normal theorem are studied in next two section. The last section is contained with finitely generated abelian groups.

4.2 MORE RESULTS ON NOETHERIAN AND ARTINIAN MODULES AND RINGS

4.2.1 Theorem. Every principal ideal domain is Noetherian.

Solution. Let D be a principal ideal domain and $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots \subseteq I_n \subseteq \ldots$ be an ascending chain of ideals of D. Let $I = \bigcup_{i \geq 1} I_i$. Then I is an ideal of D. Since D is principal ideal domain, therefore, there exist $b \in D$ such that $I = \langle b \rangle$. Since $b \in D$, therefore, $b \in I_n$ for some n. Consequently, for $m \geq n$, $I \subseteq I_n \subseteq I_m \subseteq I$. Hence $I_n = I_m$ for $m \geq n$ implies that the given chain of ideals becomes stationary at some point i.e. R is Noetherian.

(2) (Z,+,.) is a Notherian ring.

(3) Every field is Notherian ring.

(4) Every finite ring is Notherian ring.

4.2.2 Theorem. (**Hilbert basis Theorem**). If R is Noetherian ring with identity, then R[x] is also Noetherian ring.

Proof. Let I be an arbitrary ideal of R[x]. To prove the theorem, it is sufficient to show that I is finitely generated. For each integer $t \geq 0$, define;

$$I_t = \{r \in R : a_0 + a_1 x + \ldots + r x^t\} \cup \{0\}$$

Then I_t is an ideal of R such that $I_t \subseteq I_{t+1}$ for all t. But then $I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$ is an ascending chain of ideals of R. But R is Noetherian, therefore, there exist an integer n such $I_n = I_m$ for all $m \geq 0$. Also each ideal I_i of R is finitely generated. Suppose that $I_i = \langle a_{i1}, a_{i2}, \ldots, a_{im_i} \rangle$ for i=0, 1, 2, 3, …, n, where a_{ij} is the leading coefficient of a polynomial $f_{ij} \in I$ of degree i. We will show that $m_0 + m_1 + \ldots + m_n$ polynomials $f_{01}, f_{02}, \ldots, f_{0m_0}, f_{11}, f_{12}, \ldots, f_{1m_1}, \ldots, f_{n1}, f_{n2}, \ldots, f_{nm_n}$ generates I. Let $J = \langle f_{01}, f_{02}, \ldots, f_{0m_0}, f_{11}, f_{12}, \ldots, f_{1m_1}, \ldots, f_{n1}, f_{n2}, \ldots, f_{nm_n} \rangle$. Trivially $J \subseteq I$. Let $f(\neq 0) \in R[x]$ be such that $f \in I$ and of degree t (say): $f = b_0 + b_1 x + \ldots + b_{t-1} x^{t-1} + b x^t$. We now apply induction on t. For t=0, $f = b_0 \in I_0 \subseteq J$. Further suppose that every polynomial of I whose degree less than t also belongs to J. Consider following cases:

Case 1. $t > n$. As $t > n$, therefore, leading coefficient b (of f)$\in I_t = I_n$ (because $I_t = I_n \ \forall \ t \geq n$). But then $b = r_1 a_{n1} + r_2 a_{n1} + \ldots + r_{m_n} a_{nm_n}$, $r_i \in R$. Now $g = f - (r_1 f_{n1} + r_2 f_{n1} + \ldots + r_{m_n} f_{nm_n}) x^{t-n} \in I$ having degree less than t (because the coefficient of x^t in g is $b - r_1a_{n1} + r_2a_{n1} + ... + r_{m_n}a_{nm_n}$ =0, therefore, by induction, f∈J.

Case (2). $t \le n$. As $b \in I_t$, therefore, $b = s_1a_{t1} + s_2a_{t2} + ... + s_{m_t}a_{tm_t}$; $s_i \in R$. Then h=f-$(s_1f_{n1} + s_2f_{n1} + ... + s_{m_n}f_{nm_n}) \in I$, having degree less than t. Now by lsinduction hypothesis, $h \in J \Rightarrow f \in J$. Consequently, in either case $I \subseteq J$ and hence I=J. Thus I is finitely generated and hence R[x] is Noetherian. It prove the theorem.

4.2.3 Definition. A ring R is said to be an Artinian ring iff it satisfies the descending chain condition for ideals of R.

4.2.4 Definition. A ring R is said to satisfy the minimum condition (for ideals) iff every non empty set of ideals of R, partially ordered by inclusion, has a minimal element.

4.2.5 Theorem. Let R be a ring. Then R is Artinian iff R satisfies the minimum condition (for ideals).

Proof. Let R be Artinian and *f* be a nonempty set of ideal of R. If I_1 is not a minimal element in *f*, then we can find another ideal I_2 in *f* such that $I_1 \supset I_2$. If *f* has no minimal element, the repetition of this process we get a non terminating descending chain of ideals of R, contradicting to the fact that R is Artinian. Hence *f* has minimal element.

Conversely suppose that R satisfies the minimal condition. Let $I_1 \supseteq I_2 \supseteq I_3\ldots$ be an descending chain of ideals of R. Consider **F** $=\{I_t : t=1, 2, 3, \ldots\}$. $I_1 \in$ **F** $\Rightarrow$ **F** is non empty. Then by hypothesis, F has a minimal element I_n for some positive integer $n \Rightarrow I_m \subseteq I_n\ \forall\ m \ge n$.

Now $I_m \neq I_n \Rightarrow I_m \notin F$ (By the minimality of I_n) , which is not possible. Hence $I_m = I_n\ \forall\ m \ge n$ i.e. R is Artinian.

4.2.6 Theorem. Prove that an homomorphic image of a Noetherian(Artinian) ring is also Noetherian(Artinian).

Proof. Let f be a homomorphic image of a Noetherian ring R onto the ring S. Consider the ascending chain of ideals of S:

$$J_1 \subseteq J_2 \subseteq \ldots \subseteq \ldots \qquad (1)$$

Suppose $I_r=f^{-1}(J_r)$, for r=1, 2, 3, ….

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq \ldots \qquad (2)$$

Relation shown in (2) is an ascending chain of ideals of R. Since R is Noehterian, therefore, there exist positive integer n such that $I_m=I_n$ $\forall$ m≥n. This shows that $J_m=J_n$ $\forall$ m≥n. But then S becomes Noetherian and the result follows.

4.2.7 Corollary. If I is an ideal of a Noetherian(Artinian) ring, then factor module $\frac{R}{I}$ is also Noetherian(Artinian).

Proof. Since $\frac{R}{I}$ is homomorphic image of R, therefore, by Theorem 4.2.10, $\frac{R}{I}$ is Noehterian.

4.2.8 Theorem. Let I be an ideal of a ring R. If R and $\frac{R}{I}$ are both Noehterian rings, then R is also Noetherian.

Proof. Let $I_1 \subseteq I_2 \subseteq \ldots \subseteq \ldots$ be an ascending chain of ideals of R. Let f: R→ $\frac{R}{I}$. It is an natural homomorphism. But then $f(I_1) \subseteq f(I_2) \subseteq \ldots \subseteq$ is an ascending chain of ideals in $\frac{R}{I}$. Since $\frac{R}{I}$ is Noetherian, therefore, there exist a positive integer n such that $f(I_n) = f(I_{n+i})$ $\forall$ i ≥ 0. Also $(I_1 \cap I) \subseteq (I_2 \cap I) \subseteq \ldots \subseteq \ldots$ is an ascending chain of ideals of I. As I is Noehterian, therefore, there exsit a positive integer m such that $(I_m \cap I) = (I_{m+i} \cap I)$. Let r=max{m, n}. Then $f(I_r) = f(I_{r+i})$ and $(I_r \cap I) = (I_{r+i} \cap I)$ $\forall$ i ≥ 0. Let $a \in I_{r+i}$, then there exist $x \in I_r$ such that f(a)=f(x) i.e. a+I=x+I. Then $a-x \in I$ and also $a-x \in I_{r+i}$. This shows that $a-x \in (I_{r+i} \cap I) = (I_r \cap I)$. Hence $a-x \in I_r \Rightarrow a \in I_r$ i.e. $I_{r+i} \subseteq I_r$. But then $I_{r+i} = I_r$ for all i≥0. Now we have shown that every ascending chain of ideals of R terminates after a finite number of steps. It shows that R is Noetherian.

4.2.9 Definition. An Artinian domain R is an integral domain which is also an Artinian ring.

4.2.10 Theorem. Any left Artinian domain is a division ring.

Proof. Let a is a non zero element of R. Consider the ascending chain of ideals of R as: $\langle a\rangle \supseteq \langle a^2\rangle \supseteq \langle a^3\rangle \supseteq$......Since R is an Artinian ring, therefore, $\langle a^n\rangle = \langle a^{n+i}\rangle\ \forall\ i \geq 0$. Now $\langle a^n\rangle = \langle a^{n+1}\rangle \Rightarrow a^n = ra^{n+1} \Rightarrow ar = 1$ i.e. a is invertible $\Rightarrow$ R is a division ring.

4.2.11 Theorem. Let M be a finitely generated free module over a commutative ring R. Then all the basis of M are finite.

Proof. let $\{e_i\}_{i\in\Lambda}$ be a basis and $\{x_1, x_2, \ldots, x_n\}$ be a generator of M. Then each x_j can be written as $x_j = \sum_i \beta_{ij} e_i$ where all except a finite number of β_{ij}'s are zero. Thus the set of all e_i's that occurs in the expression of x_j's, j=1,2,…,n.

4.2.12 Theorem. Let M be finitely generated free module over a commutative ring R. Then all the basis of M has same number of element.

Proof. Let M has two bases X and Y containing m and n elements respectively. But then $M \cong R^n$ and $M \cong R^m$. But then $R^m \cong R^n$. Now we will show that m=n. Let m< n, f is an isomorphism from R^m to R^n and $g=f^{-1}$. Let $\{x_1, x_2, \ldots, x_m\}$ and $\{y_1, y_2, \ldots, y_n\}$ are basis element of R^m and R^n respectively. Define

$f(x_i) = a_{1i}\, y_1 + a_{2i}\, y_2 + \ldots + a_{ni}\, y_n$ and $g(y_j) = b_{1j}\, x_1 + b_{2j}\, x_2 + \ldots + b_{mj}\, x_m$. Let $A(a_{ji})$ and $B=(b_{kj})$ be n×m and m×n matrices over R. Then g $f(x_i) = g(\sum_{j=1}^{n} a_{ji} y_j) = \sum_{j=1}^{n} a_{ji} g(y_j) = \sum_{k=1}^{m}\sum_{j=1}^{n} b_{kj} a_{ji} x_k$. $1 \leq i \leq m$. Since gf=I , therefore, $x_i = \sum_{k=1}^{m}\sum_{j=1}^{n} b_{kj} a_{ji} x_k$ i.e. $\sum_{j=1}^{n} b_{1j} a_{ji} x_1 + \ldots + \sum_{j=1}^{n} (b_{ij} a_{ji} - 1) x_i + \ldots + \sum_{j=1}^{n} b_{mj} a_{ji} x_m = 0$. As x_i's are linearly independent, therefore,

$\sum_{j=1}^{n} b_{kj}a_{ji}x_k = \delta_{ki}$. Thus BA=$I_m$ and AB=I_n. Let A*=[A 0] and B*=$\begin{bmatrix} B \\ 0 \end{bmatrix}$, then A*B*= I_n and B*A*= $\begin{bmatrix} I_m & 0 \\ 0 & 0 \end{bmatrix}$. But then det(A*B*)=$I_n$ and det(B*A*)=0. Since A* and B* are matrices over commutative ring R, so det(A*B*) det(B*A*), which yield a contradiction. Hence M ≥ N. By symmetry N ≥ M i.e. M=N.

4.3 RESULT ON H_R(M, M) AND WEDDENBURN ARTIN THEOREM

4.3.1 Theorem 4. Let M=$\oplus \sum_{i=1}^{k} M_i$ be a direct sum of R-modules M_i. Then

$$\mathrm{Hom}_R(M,\ M) \cong \begin{bmatrix} \mathrm{Hom}_R(M_1,M_1) & \mathrm{Hom}_R(M_2,M_1) & \ldots & \mathrm{Hom}_R(M_k,M_1) \\ \mathrm{Hom}_R(M_1,M_2) & \mathrm{Hom}_R(M_2,M_2) & \cdots & \mathrm{Hom}_R(M_k,M_2) \\ \vdots & \vdots & \vdots & \vdots \\ \mathrm{Hom}_R(M_1,M_k) & \mathrm{Hom}_R(M_2,M_k) & & \mathrm{Hom}_R(M_k,M_k) \end{bmatrix}$$ as a

ring (Here right hand side is a ring T(say) of K×K matrices f=(f_{ij}) under the usual matrix addition and multiplication, where f_{ij} is an element of $\mathrm{Hom}_R(M_j, M_i)$).

Proof. We know that for are submodules X and Y, Hom_R(X, Y) (=set of all homomorphisms from X to Y) becomes a ring under the operations (f +g) x=f(x) +g(x) and fg(x)=f(g(x)), f , g $\in \mathrm{Hom}_R$(X, Y) and x∈X. Further λ_j: $M_j \to M$ and π_i: M→M_i are two mappings defined as:

$\lambda_j(x_j)=(0, \ldots, x_j,\ldots,0)$ and $\pi_i(x_1, \ldots, x_i, \ldots,x_k) = x_i$. (These are called inclusion and projection mappings). Both are homomorphisms. Clearly, $\pi_i \phi \lambda_j$: $M_j \to M_i$ is an homomorphism, therefore, $\pi_i \phi \lambda_j \in \mathrm{Hom}_R(M_j , M_i)$. Define a mapping σ : Hom_R(M, M)→T by σ(ϕ)= ($\pi_i \phi \lambda_j$), ϕ ∈ Hom_R(M , M) and ($\pi_i \phi \lambda_j$) is k×k matrix whose (i, j)th enrty is $\pi_i \phi \lambda_j$. We will show that σ is an isomorphism. Let $\phi_1, \phi_2 \in \mathrm{Hom}_R$(M , M). Then

$$\sigma(\phi_1 + \phi_2) = (\pi_i (\phi_1+ \phi_2)\lambda_j)= (\pi_i \phi_1\lambda_j + \pi_i \phi_2\lambda_j) = (\pi_i \phi_1\lambda_j) + (\pi_i \phi_2\lambda_j)$$

$=\sigma(\phi_1) + \sigma(\phi_2)$ and $\sigma(\phi_1)\,\sigma(\phi_2) = (\pi_i \phi_1 \lambda_j)(\pi_i \phi_2 \lambda_j) = \sum_{l=1}^{k} \pi_i \phi_1\lambda_l\pi_l\phi_2\lambda_j$

$=\pi_i\,\phi_1\lambda_1\pi_1\phi_2\lambda_j+\pi_i\,\phi_1\lambda_2\pi_2\phi_2\lambda_j+\ldots+\pi_i\,\phi_1\lambda_k\pi_k\phi_2\lambda_j$

$=\pi_i\,\phi_1(\lambda_1\pi_1+\ldots+\lambda_k\pi_k)\phi_2\lambda_j$. Since for $(x_1,\ldots, x_i, \ldots,x_k) = x \in M$, $\lambda_i\pi_i\ (x) = \lambda_i(x_i)= (0,\ldots, x_i, \ldots,0)$, therefore, $(\lambda_1\pi_1+\lambda_2\pi_2+\ldots+\lambda_k\pi_k)(x)= (\lambda_1\pi_1(x)+\lambda_2\pi_2(x)+\ldots+\lambda_k\pi_k(x)= (x_1, \ldots,0)+ (0, x_2, \ldots,0)+\ldots+ (0,\ldots, x_k)= (x_1, x_2, \ldots,x_k) = x$. Hence $(\lambda_1\pi_1+\lambda_2\pi_2+\ldots+\lambda_k\pi_k)=I$ on M. Thus $\sigma(\phi_1)\sigma(\phi_2)=\pi_i\,\phi_1\phi_2\lambda_j = \sigma\ (\phi_1\phi_2)$. Hence σ is an homomorphism. Now we will show that σ is one-one. For it let $\sigma(\phi)= (\pi_i\ \phi\ \lambda_j)=0$. Then $\pi_i\ \phi\ \lambda_j=0$ for each i, j ; $1 \leq i, j \leq k$. But then $\pi_1\ \phi\ \lambda_j + \pi_2\ \phi\ \lambda_j +\ldots+ \pi_k\ \phi\ \lambda_j =0$. Since $\sum_{i=1}^{k}\pi_i$ is an identity mapping on M, therefore, $(\sum_{i=1}^{k}\pi_i)\phi\lambda_j \Rightarrow \phi\lambda_j= 0$. But then $\phi\sum_{j=1}^{k}\lambda_j = 0$ and hence $\phi=0$. Therefore, the mapping is one-one. Let $f = (f_{ij})\in T$, where $f_{ij} : M_j \rightarrow M_i$ is an R-homomorphism. Set $\psi = \sum_{i,j}\lambda_i f_{ij}\pi_j$. Since for each i and j, $\lambda_i f_{ij}\pi_j$ is an homomorphism from M to M, therefore, $\sum_{i,j}\lambda_i f_{ij}\pi_j$ is also an element of Hom(M, M). Since $\sigma(\phi)$ is a square matrix of order k, whose (s, t) entry is f_{st}, therefore, $\sigma(\psi)=(\pi_s(\ \sum_{i,j}\lambda_i f_{ij}\pi_j\ )\lambda_t)$. As $\pi_p\ \lambda_q = \delta_{pq}$, therefore, $\pi_s(\ \sum_{i,j}\lambda_i f_{ij}\pi_j\ )\lambda_t = f_{st}$. Hence $\sigma(\psi)=(f_{ij})=f$ i.e. mapping is onto also. Thus σ is an isomorphism. It proves the result.

4.3.2 Definition. Nil Ideal. A left ideal A of R is called nil ideal if each element of it nilpotent.

Example. Every Nilpotent ideal is nil ideal.

4.3.3 Theorem. If J is nil left ideal in an Artinian ring R, then J is nilpotent.

Proof. Suppose $J^k\neq(0)$. For some positive integer k. Consider a family {J, J^2, … }. Because R is Artinian ring, this family has minimal element say $B=J^m$. Then $B^2=J^{2m}=J^m=B$ implies that $B^2=B$. Now consider another family f={A| A is left ideal contained in B with BA≠(0). As BB=B≠(0), therefore, f is non empty. Since it is a family of left ideals of an Artinian ring R, therefore, it has minimal element. Let A be that minimal element in f. Then BA $\neq(0)$ i.e. there exist a in A such that Ba$\neq(0)$ Because A is an ideal, therefore, Ba $\subseteq$ A and $B(Ba)=B^2a=Ba \neq(0)$. Hence Ba$\in f$. Now the minimality of A implies that Ba=A. Thus ba=a for some b$\in$B. But then $b^ia = a\ \forall\ i \geq 1$. Since b is nilpotent element, therefore, a=0, a contradiction. Hence for some integer k, $J^k=(0)$.

Theorem. Let R be Noetherian ring. Then the sum of nilpotent ideals in R is a nilpotent ideal.

Proof. Let B = $\sum_{i\in\Lambda} A_i$ be the sum of nilpotent ideals in R. Since R is noetherian, therefore, every ideal of R is finitely generated. Hence B is also finitely generated. Let $B=\langle x_1, x_2, \ldots, x_t\rangle$. Then each x_i lies in some finite number of A_i's say $A_1, A_2, \ldots, A_n$. Thus $B=A_1+A_2+\ldots+A_n$. But we know that finite sum of nilpotent ideals is nilpotent. Hence B is nilpotent.

4.3.4 Lemma. Let A be a minimal left ideal in R. Then either $A^2=(0)$ or A=Re.

Proof. Suppose that $A^2\neq(0)$. Then there exist a$\in$A sucht that Aa$\neq(0)$. But Aa $\subseteq$A and the minimality of A shows that Aa =A. From this it follows that there exist e in A such that ea=a. As a is non zero, therefore, ea$\neq$0 and hence e$\neq$0. Let $B=\{c\in A \mid ca=0\}$, then B is a left ideal of A. Since ea $\neq$ 0 , therefore, $e\notin$ B. Hence B is proper ideal of A. Again minimality of A implies that B=(0). Since $e^2a=eea=ea \Rightarrow (e^2-e)a=0$, therefore, $(e^2-e) \in B=(0)$. Hence $e^2=e$. i.e e is an idempotent in R. As $0\neq e=e^2= e.e\in Re$, therefore, Re is a non zero subset of A. But then Re=A. It proves the result.

4.3.5 Theorem. (Wedderburn-Artin). Let R be a left (or right) artinian ring with unity and no nonzero nilpotent ideals. Then R is isomorphic to a finite direct sum of matrix rings over the division ring.

Proof. First we will show that each non zero left ideal in R is of the form Re for some idempotent. Let A be a non-zero left ideal in R. Since R is artinian, therefore, A is also artinian and hence every family of left ideal of A contains a minimal element i.e. A has a minimal ideal M say. But then $M^2=(0)$ or M=Re for some idempotent e of R. If $M^2=(0)$, then

$(MR)^2=(MR)(MR)=M(RM)R=MMR=M^2R=(0)$. But then MR is nilpotent. Thus by given hypothesis MR=(0). Now MR = (0) implies that M = (0), a contradiction. Hence M=Re. This yields that each non zero left ideal contains a nonzero idempotent. Let $f=\{R(1-e)\cap A \mid e$ is a non-zero idempotent in $A\}$. Then f is non empty. Because M is artinian, f has a minimal member say $R(1-e)\cap A$. We will show that $R(1-e)\cap A=(0)$. If $R(1-e)\cap A\neq(0)$ then it has a non zero idempotent e_1. Since $e_1 = r(1-e)$, therefore, $e_1e=r(1-e)e= r(e-e^2)=0$. Take $e^* = e + e_1 - ee_1$. Then $(e^*)^2 =(e + e_1 - ee_1)(e + e_1 - ee_1)= ee + e_1e - ee_1e + ee_1 + e_1e_1 - ee_1e_1 -eee_1- e_1ee_1 + ee_1ee_1= e + 0 – e0 + ee_1 + e_1 - ee_1 -ee_1- 0e_1 + e0e_1= e + e_1 - ee_1 = e^*$ i.e. we have shown that e^* is an idempotent. But $e_1e^*=e_1e + e_1e_1 - e_1ee_1= e_1\neq 0$ implies that $e_1 \notin R(1-e^*) \cap A$. (Because if $e_1\in R(1-e^*) \cap A$, then $e_1 = r(1-e^*)$ for some $r\in R$ and then $e_1e^*= r(1-e^*) e^*= r(e^*- e^*e^*)=0$). More over for $r(1-e^*)\in R(1-e^*)$, $r(1-e^*)= r(1- e - e_1 + ee_1)= r(1- e - e_1(1- e))= r(1-e_1)(1- e)= s(1-e)$ for $s = r(1-e_1)\in R$, therefore, Hence $R(1-e^*)\cap A$ is proper subset of $R(1-e)\cap A$. But it is a contradiction to the minimality of $R(1-e)\cap A$ in f. Hence $R(1-e)\cap A=(0)$. Since for $a\in A$, $a(1-e)\in R(1-e)\cap A$, therefore, $a(1-e)=(0)$ i.e. $a=ae$. Then $A \supseteq Re \supseteq Ae \supseteq A \Rightarrow A=Re$.

For an idempotent e of R, $Re\cap R(1-e)=(0)$. Because if $x\in Re\cap R(1-e)$, then $x=re$ and $x=s(1-e)$ for some r and s belonging to R. But then $re=s(1-e)\Rightarrow ree=s(1-e)e \Rightarrow re= s(e-e^2)=0$ i.e. $x=0$. Hence $Re \cap R(1-e)=(0)$. Now let S be the sum of all minimal left ideals in R. Then S=Re for some idempotent e in R. If $R(1-e)\neq(0)$, then there exist a minimal left ideal A in R(1-e). But then $A \subseteq Re \cap R(1-e)=(0)$, a contradiction. Hence , $R(1-e)=(0)$ i.e $R=Re=S=\sum_{i\in\Lambda} A_i$ where $(A_i)_{i\in\Lambda}$ is the family of minimal left ideals in R. But then there exist a subfamily $(A_i)_{i\in\Lambda^*}$ of the family $(A_i)_{i\in\Lambda}$ such that $R=\oplus\sum_{i\in\Lambda^*} A_i$. Let $1=e_{i_1}+e_{i_2}+...+e_{i_n}$. Then $R= Re_{i_1}\oplus...\oplus Re_{i_n}$ (because for $r\in R$, $1=e_{i_1}+e_{i_2}+...+e_{i_n} \Rightarrow r=re_{i_1}+re_{i_2}+...+re_{i_n}$). After reindexing if necessary, we may write $R=Re_1\oplus Re_2\oplus...\oplus Re_n$, a direct sum of minimal left ideals. In this family of minimal left ideals $Re_1, Re_2, ..., Re_n$, choose a 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 $Re_1, Re_2, ..., Re_k$. Suppose the number of left ideal in the family (Re_i), $1\leq i \leq n$, that are isomorphic to Re_i is n_i. Then

$$R = \overbrace{[Re_1\oplus ...]}^{n_1 \text{ summands}} \oplus \overbrace{[Re_2\oplus ...]}^{n_2 \text{ summands}} \oplus ... \oplus \overbrace{[Re_k\oplus ...]}^{n_k \text{ summands}}$$

where each set of brackets contains pair wise isomorphic minimal left ideals, and no minimal left ideal in any pair of bracket is isomorphic to minimal left ideal in another pair. Since $Hom_R(Re_i , Re_j)=(0)$ for $i\neq j$, $1\leq i , j\leq k$ and $Hom_R(Re_i , Re_i) =D_i$ is a division ring(by shcur's lemma). Thus by Theorem 4, we get $Hom_R(R,R)\cong$

$$\begin{bmatrix} \begin{vmatrix} D_1 & \cdots & D_1 \\ \vdots & & \vdots \\ D_1 & \cdots & D_1 \end{vmatrix} & 0 & 0 \\ 0 & \begin{vmatrix} D_2 & \cdots & D_2 \\ \vdots & & \vdots \\ D_2 & \cdots & D_2 \end{vmatrix} \ddots & \\ 0 & & \begin{vmatrix} D_k & \cdots & D_k \\ \vdots & & \vdots \\ D_k & \cdots & D_k \end{vmatrix} \end{bmatrix} \cong \begin{bmatrix} (D_1)_{n_1} & & \\ & \ddots & \\ & & (D_k)_{n_k} \end{bmatrix}$$

$\cong (D_1)_{n_1} \oplus ... \oplus (D_k)_{n_k}$. But since $Hom_R(M, M) \cong R^{op}$ (under the mapping $f: R^{op} \rightarrow Hom_R(M, M)$ given by $f(a)=a^*$ where $a^*(x)=a\circ x=xa$) as rings and the opposite ring of a division ring is a division ring. Since $R^{op} \cong R$, therefore, R is finite direct sum of matrix rings over division rings.

4.4 UNIFORM MODULES, PRIMARY MODULES AND NOETHER-LASKAR THOEREM

4.4.1 Definition. Uniform module. A non zero module M is called uniform if any two nonzero submodules of M have non zero intersection.

Example. Z as Z-module is uniform as: Since Z is principal ideal domain, therefore, the two sub-modules of it are <a> and <b> say, then <ab> is another submodule which is contained in both <a> and <b> . Hence intersection of any two nonzero sub-modules of M is non zero. Thus Z is a uniform module over Z.

4.4.2 Definition. If U and V are uniform modules, we say U is sub-isomorphic to V provided that U and V contains non zero isomorphic sub-modules.

4.4.3 Definition. A module M is called primary if each non zero sub-module of M has uniform sub-module and any two uniform sub-modules of M are sub-isomorphic.

Example. Z is a primary module over Z.

4.4.4 Theorem. Let M be a Noetherian module or any module over a Noetherian ring. Then each non zero submodule contains a uniform module.

Proof. Let N be a non zero submodule of M. Then there exist $x(\neq 0) \in N$. Consider the submodule xR of N. Then it is enough to prove that xR contains a uniform module. If M is Noetherian, then the every submodule of M is noetherian and hence xR is also noetherian and if R is Noethrian then, being a homomorphic image of Noetherian ring R, xR is also Noetherian. Thus, for both cases, xR is Noetherian.

Consider a family ***f*** of submodules of xR as: ***f*** $=\{N \mid$ N has a zero intersection with at least one submodule of xR$\}$. Then $\{0\} \in$ ***f***. Since xR is noetherian, therefore, ***f*** has maximal element K(say). Then there exist an submodule U of xR such that $K \cap U=\{0\}$. We claim U is uniform. Otherwise, there exist submodules A, B of U such that $A \cap B=\{0\}$. Since $K \cap U=\{0\}$, therefore, we can talk about $K \oplus A$ as a submodule of xR such that $K \oplus A \cap B=\{0\}$. But then $K \oplus A \in$ ***f***, a contradiction to the maximality of K. This contradiction show that U is uniform. Hence $U \subseteq xR \subseteq N$. Thus every submodule N contains a uniform submodule.

4.4.5 Definition. If R is a commutative noetherian ring and P is a prime ideal of R, then P is said to be associated with module M if R/P imbeds in M or equivalently, $P=r(x)$ for some $x \in M$, where $r(x)=\{a \in R \mid xa = 0\}$.

4.4.6 Definition. A module M is called P- primary for some prime ideal P if P is the only prime associated with M.

4.4.7 Theorem. Let U be a uniform module over a commutative noetherain ring R. Then U contains a submodule isomorphic to R/P for precisely one prime ideal P. In other words U subisomorphic to R/P for precisely one ideal P.

Proof. Consider the family f of annihilators of ideals r(x) for non zero x $\in$U. Being a family of ideals of noetherian ring R, f has a maximal element r(x) say. We will show that P=r(x) is prime ideal of R. For it let ab$\in$r(x), a$\notin$r(x). As ab$\in$r(x) $\Rightarrow$ (ab)x = 0. Since xa $\neq$ 0, therefore, b(xa) = 0 $\Rightarrow$ b$\in$r(xa). More over for t$\in$r(xa) $\Rightarrow$ t(xa)=0 $\Rightarrow$ (ta)x=0 $\Rightarrow$ r(xa) $\in$ f. Clearly r(x) $\subseteq$ r(xa). Thus the maximality of r(x) in f implies that r(xa)=r(x) i.e. b$\in$r(x). Hence r(x) is prime ideal of R. Define a mapping from R to xR by θ(r)=xr. Then it is an homomorphism from R to xR. Kernal θ ={ r$\in$R | xr=0}. Then Kernal θ = r(x). Hence by fundamental theorem on homomorphism, R/ r(x) $\cong$ xR = R/P. Therefore R/P is embeddable in U. Hence [R/P]=[R/Q]. this implies that there exist cyclic submodules xR and yR of R/P and R/Q respectively such that xR$\cong$yR. But then R/P$\cong$R/Q, which yields P=Q. It prove the theorem.

4.4.8 Note. The ideal in the above theorem is called the prime ideal associated with the uniform module U.

4.4.9 Theorem. Let M be a finitely generated ideal over a commutative noetherian ring R. Then there are only a finite number of primes associated with M.

Proof. Take a family f consisting of the direct sum of cyclic uniform submodules of M. Since every submodule M over a noehtrian ring contains a uniform submdule, therefore, f is non empty. Define a relation $\leq$, on the set of elements of f by $\oplus \sum_{i\in I} x_i R \leq \oplus \sum_{j\in J} x_j R$ iff I $\subseteq$ J and $x_iR \subseteq y_jR$ for some j$\in$J.

This relation is a partial order relation on f. By Zorn's lemma F has a maximal member $K = \oplus \sum_{i\in I} x_i R$. Since M is noetherian, therefore, K is finitely generated. Thus $K = \oplus \sum_{i=1}^{t} x_i R$. By theorem, 4.2.7, there exist $x_ia_i \in x_i$ R such that $r(x_ia_i)=P_i$, the ideal associated with x_iR. Set $x_i^* = x_ia_i$ and $K^* = \oplus \sum_{i=1}^{t} x_i^* R$.

Let $Q = r(x)$ be the prime ideal associated with M. We shall show that $Q = P_i$ for some i, $1 \leq i \leq t$.

Since K is a maximal member of f, therefore, K as well as K^* has the property that each has non zero intersection with each submodule L of M. Now let $0 \neq y \in xR \cap K^*$. Write $y = \oplus \sum_{i=1}^{t} x_i^* b_i = xb$. We will show that $r(x_i^* b_i) = r(x_i^*)$ whenever $x_i^* b_i \neq 0$. Clearly, $r(x_i^*) \subseteq r(x_i^* b_i)$. Let $x_i^* b_i c = 0$. Then $b_i c$ $r(x_i^*) = P_i$ and so $c \in P_i$ since $b_i \notin P_i$. Hence, $c \in r(x_i^*)$.

Further, we note $Q = r(x) = r(y) = \bigcap_{i=1}^{t} r(x_i^* b_i) = \bigcap_{i \in \Lambda} P_i$, omitting those terms from $x_i^* b_i = 0$, where $\Lambda \subset \{1, 2, ..., t\}$. Therefore, $Q \subseteq P_i$ for all $i \in \Lambda$. Also $\prod_{i \in \Lambda} P_i \subset \bigcap_{i \in \Lambda} P_i = Q$. Since Q is a prime ideal, at least one P_i appearing in the product $\prod_{i \in \Lambda} P_i$ must be contained in Q. Hence $Q = P_i$ for some i.

4.4.10 Theorem.(Noether-Laskar theorem). Let M be a finitely generated ideal over a commutative noetherian ring R. Then there exist a finite family $N_1, N_2, \ldots, N_t$ of submodules of M such that

(a) $\bigcap_{i=1}^{t} N_i = (0)$ and $\bigcap_{\substack{i=1 \\ i \neq i_0}}^{t} N_i \neq (0)$ for $1 \leq i_0 \leq t$.

(b) Each quotient module 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 iff P_i does not contain P_j for some $j \neq i$.

Proof. Let U_i , $1 \leq i \leq t$, be a uniform sub module obtained as in the proof of the Theorem 4.4.9. Consider the family { K | K is a subset of M and K contains no submodule subisomorphic to U_i }. Let N_i be a maximal member of this family, then with this choice of N_i, (a), (b) and (c) follows directly.

4.5 SMITH NORMAL FORM

4.5.1 Theorem. Obtain Smith normal form of given matrix. Or if A is m×n matrix over a principal ideal domain R. Then A is equivalent to a matrix that has the diagonal form $\begin{bmatrix} a_1 & & & & \\ & a_2 & & & \\ & & \ddots & & \\ & & & a_r & \\ & & & & \ddots \end{bmatrix}$ where $a_i \neq 0$ and $a_1 \mid a_2 \mid a_3 \mid \ldots \mid a_r$.

Proof. For non zero a, define the length $l(a)$=no of prime factors appearing in the factorizing of , $a=p_1p_2 \ldots p_r$ (p_i need not be distinct primes). We also take l(a) if a is unit in R. If A=0, then the result is trivial otherwise, let a_{ij} be the non zero element with minimum $l(a_{ij})$. Apply elementary row and column operation to bring it (1, 1) position. Now a_{11} entry of the matrix so obtained is of smallest l value i.e. the non zero element of this matrix at (1, 1) position. Let a_{11} does not divide a_{1k}. Interchanging second and k^{th} column so that we may suppose that 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 $a_{11}=du$, $a_{12}=dv$ and $l(d) < l(a_{11})$. As $d=(a_{11}, a_{12})$, therefore we can find s and $t \in R$ such that $d=(sa_{11}+ta_{12})= d(su + vt)$. Then we get that $A\begin{bmatrix} u & t & & & \\ v & -s & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 1 \end{bmatrix}$ is a matrix whose first row is $(d, 0, b_{13}, b_{14}, \ldots b_{1n})$ where $l(d) < l(a_{11})$. If $a_{11} \mid a_{12}$, then $a_{12}=ka_{11}$. On applying, the operation $C_2 - kC_1$ and $\frac{1}{u}C_1$ we get the matrix whose first row is again of the form $(d, 0, b_{13}, b_{14}, \ldots b_{1n})$. Continuing in this way we get a matrix whose first row and first column has all its entries zero except the first entry. This matrix is $P_1AQ_1 \begin{bmatrix} a_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A_1 & \\ 0 & & & \end{bmatrix}$, where A_1 is $(m-1)\times(n-1)$ matrix, and P_1 and Q_1 are $m\times m$ and $n\times n$ invertible matrices respectively. Now applying the same process of A_1, we get that $P_2'A_1Q_2' = \begin{bmatrix} a_2 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A_2 & \\ 0 & & & \end{bmatrix}$, where A_2 is $(m-2)\times(n-2)$ matrix, and P_2' and Q_2' are $(m-1)\times(m-1)$ and $(n-1)\times(n-1)$ invertible matrices respectively. Let $P_2 = \begin{bmatrix} 1 & 0 \\ 0 & P_2' \end{bmatrix}$ and $Q_2 = \begin{bmatrix} 1 & 0 \\ 0 & Q_2' \end{bmatrix}$. Then $P_2P_1AQ_1Q_2=$

$$\begin{bmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & & \\ \vdots & & A_2 & \\ 0 & & & \end{bmatrix}$$

. Continuing in this way we get matrices P and Q such that

PAQ=diag(a_1, a_2,…, a_r, 0, …0). Finally we show that we can reduce PAQ so that $a_1| a_2 | a_3|$…. For it if a_1 does not divide a_2, then add second row to the first row and obtain the matrix whose first row is (a_1, a_2, 0, 0,…,0). Again multiplying PAQ by a matrix of the form

$$\begin{bmatrix} u & t & & & \\ v & -s & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 1 \end{bmatrix}$$

we can obtain a matrix such that $a_1|a_2$. Hence we can always obtain a matrix of required form.

4.5.2 Example. Obtain the normal smith form for a matrix $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 0 \end{bmatrix}$.

Solution.

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 0 \end{bmatrix} \xrightarrow{R_2-4R_1}$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 0 & -3 & -12 \end{bmatrix} \xrightarrow{C_2-2C_1, C_3-3C_1}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & -3 & -12 \end{bmatrix} \xrightarrow{C_3-4C_2}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & -3 & -12 \end{bmatrix} \xrightarrow{C_3-4C_2} \begin{bmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \end{bmatrix} \xrightarrow{-R_2} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \end{bmatrix}.$$

4.6 FINITELY GENERATED ABELIAN GROUPS

4.6.1 Note. Let $G_1, G_2,\ldots G_n$ be a family of subgroup of G and let $G^* = G_1\ldots G_n$. Then the following are equivalent.

(i) $G_1\times\ldots\times G_n \cong G^*$ under the mapping $(g_1, g_2, \ldots, g_n)$ to $g_1g_2\ldots g_n$

(ii) G_i is normal in G^* and every element x belonging to G^* can be uniquely expressed as $x=g_1g_2 \ldots g_n$, $g_i\in G_i$.

(iii) G_i is normal in G^* and if $e = g_1 g_2 \dots g_n$, then each x_i=e.

(iv) G_i is normal in G^* and $G_i \cap G_1 \dots G_{i-1} G_{i+1} \dots G_n = \{e\}$, $1 \le i \le n$.

4.6.2 Theorem.(Fundamental theorem of finitely generated abelian groups). Let G be a finitely generated abelian group. Then G can be decomposed as a direct sum of a finite number of cyclic groups C_i i.e. $G = C_1 \oplus C_2 \oplus \dots \oplus C_t$ where either all C_i's are infinite or for some j less then k, $C_1, C_2, \dots C_j$ are of order $m_1, m_2, \dots m_j$ respectively, with $m_1 | m_2 | \dots | m_j$ and rest of C_i's are infinite.

Proof. Let $\{a_1, a_2, \dots, a_t\}$ be the smallest generating set for G. If t=1, then G is itself a cyclic group and the theorem is trivially true. Let t > 1 and suppose that the result holds for all finitely generated abelian groups having order less then t. Let us consider a generating set $\{a_1, a_2, \dots, a_t\}$ of element of G with the property that , for all integers $x_1, x_2, \dots, x_t$, the equation

$$x_1 a_1 + x_2 a_2 + \dots + x_t a_t = 0$$

implies that

$$x_1 = 0,\ x_2 = 0, \dots,\ x_t = 0.$$

But this condition implies that every element in G has unique representation of the form

$$g = x_1 a_1 + x_2 a_2 + \dots + x_t a_t,\ x_i \in Z.$$

Thus by Note 4.6.1,

$$G = C_1 \oplus C_2 \oplus \dots \oplus C_t$$

where $C_i = \langle a_i \rangle$ is cyclic group generated by a_i, $1 \le i \le t$. By our choice on element of generated set each C_i is infinite set (because if C_i is of finite order say r_i , then $r_i a_i = 0$). Hence in this case G is direct sum of finite number of infinite cyclic group.

Now suppose that that G has no generating set of t elements with the property that $x_1 a_1 + x_2 a_2 + \dots + x_t a_t = 0 \Rightarrow x_1 = 0,\ x_2 = 0, \dots,\ x_t = 0$. Then, given any generating set $\{a_1, a_2, \dots, a_t\}$ of G, there exist integers $x_1, x_2, \dots, x_t$ not all zero such that

$$x_1 a_1 + x_2 a_2 + \dots + x_t a_t = 0.$$

As $x_1 a_1 + x_2 a_2 + \dots + x_t a_t = 0$ implies that $-x_1 a_1 - x_2 a_2 - \dots - x_t a_t = 0$, therefore, with out loss of generality we can assume that $x_i > 0$ for at least one i. Consider all possible generating sets of G containing t elements with the property that $x_1 a_1 + x_2 a_2 + \ldots + x_t a_t = 0$ implies that at least one of $x_i > 0$. Let X is the set of all such $(x_1, x_2, \ldots x_t)$ t -tuples. Further let m_1 be the least positive integers that occurring in the set t-tuples of set X. With out loss of generality we can take m_1 to be at first component of that t-tuple $(a_1, a_2, \ldots, a_t)$

i.e. $m_1 a_1 + x_2 a_2 + \ldots + x_t a_t = 0$ (1)

By division algorithm, we can write, $x_i = q_i m_1 + s_i$, where $0 \le s_i < m_1$. Hence (1) becomes,

$m_1 b_1 + s_2 a_2 + \ldots + s_t a_t = 0$, where $b_1 = a_1 + q_2 a_2 + \ldots + q_t a_t$.

Now if $b_1=0$, then $a_1 = -q_2 a_2 - \ldots - q_t a_t$. But then G has a generator set containing less then t elements, a contradiction to the assumption that the smallest generator set of G contains t elements. Hence $b_1 \neq 0$. Since $a_1 = -b_1 - q_2 a_2 - \ldots - q_t a_t$, therefore, $\{b_1, a_2, \ldots, a_n\}$ is also a generator of G. But then by the minimality of m_1, $m_1 b_1 + s_2 a_2 + \ldots + s_t a_t = 0 \Rightarrow s_i = 0$ for all i. $2 \le i \le t$. Hence $m_1 b_1 = 0$. Let $C_1 = <b_1>$. Since m_1 is the least positive integer such that $m_1 b_1 = 0$, therefore, order of $C_1 = m_1$.

Let G_1 be the subgroup generated by $\{a_2, a_3, \ldots, a_t\}$. We claim that $G = C_1 \oplus G_1$. For it, it is sufficient to show that $C_1 \cap G_1 = \{0\}$. Let $d \in C_1 \cap G_1$. Then $d = x_1 b_1$, $0 \le x_1 < m_1$ and $d = x_2 a_2 + \ldots + x_t a_t$. Equivalently, $x_1 b_1 + (-x_2) a_2 + \ldots + (-x_t) a_t = 0$. Again by the minimal property of m_1, $x_1 = 0$. Hence $C_1 \cap G_1 = \{0\}$.

Now G_1 is generated by set $\{a_2, a_2, \ldots, a_t\}$ of t-1 elements. It is the smallest order set which generates G_1(because if G_1 is generated by less then t-1 elements then G can be generated by a set containing t-1 elements, a contradiction to the assumption that the smallest generator of G contains t elements). Hence by induction hypothesis,

$G_1 = C_2 \oplus \ldots \oplus C_t$

where $C_2, \ldots, C_k$ are cyclic subgroup of G that are either all are infinite or, for some $j \le t$, $C_2, \ldots, C_j$ are finite cyclic group of order $m_2, \ldots, m_j$ respectively such that $m_2 | m_3 | \ldots | m_j$, and C_i are infinite for $i > j$.

Let $C_i = [b_i]$, i=2, 3, …, k and suppose that C_2 is of order m_2. Then $\{b_1, b_2, \ldots, b_t\}$ is the generating set of G and $m_1 b_1 + m_2 b_2 + 0.b_3 + \ldots + 0.b_k = 0$. By repeating the argument given for (1), we conclude that $m_1 | m_2$. This completes the proof of the theorem.

4.6.3 Theorem. Let G be a finite abelian group. Then there exist a unique list of integers $m_1, m_2, \ldots, m_t$ (all $m_i > 1$) such that order of G is $m_1 m_2 \ldots m_t$ and G $= C_1 \oplus C_2 \oplus \ldots \oplus C_t$ where $C_1, C_2, \ldots, C_t$ are cyclic groups of order $m_1, m_2, \ldots, m_k$ respectively. Consequently, $G \cong Z_{m_1} \oplus Z_{m_1} \oplus \ldots \oplus Z_{m_t}$.

Proof. By theorem 4.6.2, $G = C_1 \oplus C_2 \oplus \ldots \oplus C_t$ where $C_1, C_2, \ldots, C_t$ are cyclic groups of order $m_1, m_2, \ldots, m_t$ respectively, such that $m_1 | m_2 | \ldots | m_t$. As order of $S \times T$ = order of S × order of T, therefore, order of G = $m_1 m_2 \ldots m_t$. Since a cyclic group of order m is isomorphic to Z_m group of integers under the operation addition mod m, therefore,

$$G \cong Z_{m_1} \oplus Z_{m_1} \oplus \ldots \oplus Z_{m_t}.$$

We claim that $m_1, m_2, \ldots, m_t$ are unique. For it, let there exists $n_1, n_2, \ldots, n_r$ such that $n_1 | n_2 | \ldots | n_r$ and $G = D_1 \oplus D_2 \oplus \ldots \oplus D_r$ where D_j are cyclic groups of order n_j. Since D_r has an element of order n_r and largest order of element of G is m_t , therefore, $n_r \le m_t$. By the same argument, $m_t \le n_r$. Hence $m_t = n_r$.

Now consider $m_{t-1} G = \{m_{t-1} g \mid g \in G\}$. Then by two decomposition of G we get

$$m_{t-1} G = (m_{t-1} C_1) \oplus (m_{t-1} C_2) \oplus \ldots \oplus (m_{t-1} C_t)$$
$$= (m_{t-1} D_1) \oplus (m_{t-1} D_2) \oplus \ldots \oplus (m_{t-1} D_{r-1}).$$

As $m_i | m_{t-1}$ (it means m_i divides m_{t-1})for all i, $1 \le i \le t-1$, therefore, for all such i, $m_{t-1} C_i = \{0\}$. Hence order of $(m_{t-1} G)$ i.e. $| m_{t-1} G | = |(m_{t-1} C_t)| = |(m_{t-1} D_r)|$. Thus $|(m_{t-1} D_j)| = 1$ for j=1, 2, …, r-1. Hence $n_{r-1} | m_{t-1}$. Repeating the process by taking $m_{r-1} G$, we get that $m_{t-1} | n_{r-1}$. Hence $m_{t-1} = n_{r-1}$. Continuing this process we get that $m_i = n_i$ for i=t, t-1, t-2, …. But $m_1 m_2 \ldots m_t = |G| = n_1 n_2 \ldots n_r$, therefore, r = t and $m_i = n_i$ for all i, $1 \le i \le k$.

4.6.3 Corollary. 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 nonnegative integer and a_i are nonzero non-unit in Z, such that $a_1 | a_2 | \ldots | a_r$. Further decomposition of A shown above is unique in the sense that a_i are unique.

4.6.4 Example. The abelian group generated by x_1 and x_2 subjected to the condition $2x_1 = 0$, $3x_2 = 0$ is isomorphic to Z/<6> because the matrix of these equation is $\begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$ has the smith normal form $\begin{bmatrix} 1 & 0 \\ 0 & 6 \end{bmatrix}$

4.7 KEY WORDS

Uniform modules**,** Noether Lashkar, wedderburn artin, finitely generated.

4.8 SUMMARY

In this chapter, we study about Weddernburn theorem, uniform modules, primary modules, noether-laskar theorem, smith normal theorem and finitely generated abelian groups. Some more results on noetherian and artinian modules and rings are also studied.

4.9 SELF ASSESMENT QUESTIONS

(1) Let R be an artinain rings. Then show that the following sets are ideals and are equal:

(i) N= sum of nil ideals , (ii) U = some of nilpotent ideals, (iii) Sum of all nilpotent right ideals.

(2) Show that every uniform module is a primary module but converse may not be true

(3) Obtain the normal smith form of the matrix $\begin{bmatrix} -x & 4 & -2 \\ -3 & 8-x & 3 \\ 4 & -8 & -2-x \end{bmatrix}$ over the ring Q[x].

(4) Find the abelian group generated by $\{x_1, x_2, x_3\}$ subjected to the conditions $5x_1 + 9x_2 + 5x_3=0$, $2x_1 + 4x_2 + 2x_3=0$, $x_1 + x_2 - 3x_3=0$

4.10 SUGGESTED READINGS

(1) Modern Algebra; SURJEET SINGH and QAZI ZAMEERUDDIN, Vikas Publications.

(2) Basic Abstract Algebra; P.B. BHATTARAYA, S.K.JAIN, S.R. NAGPAUL, Cambridge University Press, Second Edition.