Unit - V

6.7. Invariant Direct Sums.

Theorem :- 10

Let T be a linear operator on the space V, and let $W_1, \ldots, W_k$ and $E_1, \ldots, E_k$ $V = W_1 \oplus \cdots \oplus W_k$. Define $E_i(v) = E_i(x_1 + \cdots + x_k) = x_i \in W_i$. Then each E_i is a projection on V such that $E_i E_j = 0 \ \forall \ i \neq j$ and $I = E_1 + \cdots + E_k$. Then a necessary and sufficient condition that each subspace W_i be invariant under T is that T commute with each of the projections E_i. i.e. $TE_i = E_i T$, $i = 1, 2, \ldots, k$.

Proof :-

suppose T commutes with each E_i.

$$\text{i.e. } TE_i = E_i T.$$

Let $\alpha \in W_i$. Then $E_j \alpha = \alpha$.

$$T(\alpha) = T(E_j \alpha) = E_j(T\alpha).$$

$$\Rightarrow T(\alpha) \in \text{Range of } E_i = W_i.$$

$\therefore W_i$ is invariant under T.

Conversely, assume that each W_i invariant under T.

To r.t. TE_j ...

(9) $I(\alpha) = (E_1 + \cdots + E_k)\alpha$

$\alpha = E_1(\alpha) + \cdots + E_k(\alpha)$

$T(\alpha) = TE_1(\alpha) + \cdots + TE_k(\alpha)$.

Since $E_i\alpha \in W_i$, which is invariant under T. We must have $T(E_i\alpha) = E_i\beta_i$ for some vector β_i. Then $E_jT(E_i\alpha) = E_jE_i\beta_i$

$$= \begin{cases} 0, & \text{if } i \neq j \\ E_j\beta_j, & \text{if } i = j. \end{cases}$$

Thus $E_jT\alpha = E_jTE_1\alpha + \cdots + E_jTE_k\alpha$

$= E_j\beta_j = TE_j\alpha$

$\therefore E_jT = TE_j$.

This completes the proof of the theorem.

Theorem :- 11

Let T be a linear operator on a finite-dimensional space V. If T is diagonalizable and if $c_1, \ldots, c_k$ are the distinct characteristic values of T, then $\exists$ linear operators $E_1, \ldots, E_k$ on V such that

(i) $T = c_1E_1 + \cdots + c_kE_k$

(ii) $I = E_1 + \cdots + E_k$

(4)

(iii) $E_i E_j = 0$, $i \neq j$

(iv) $E_i^2 = E_i$ (E_i is a projection)

(v) the range of E_i is the characteristic space for T associated with c_i.

Conversely, if $\exists$ k distinct scalars $c_1, \dots, c_k$ and k non-zero linear operators $E_1, \dots, E_k$ which satisfy conditions (i), (ii) and (iii), then T is diagonalizable, $c_1, \dots, c_k$ are the distinct characteristic values of T, and conditions (iv) and (v) are satisfied also.

Proof :- Let T be diagonalizable, with distinct characteristic values $c_1, \dots, c_k$.

Let W_i be the space of characteristic vectors associated with the characteristic value c_i. By known theorem,

$$\dim V = \dim W_1 + \dots + \dim W_k \quad \text{and}$$

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

$$\Rightarrow V = W_1 \oplus \dots \oplus W_k.$$

We know that $E_1, \dots, E_k$ be the projection associated with this decomposition. Then (ii) (iii)

-valued functions on $[a, b]$. Then $L(g) =$

(4)

Let $\alpha \in V$.

$$I(\alpha) = \alpha = (E_1 + \cdots + E_k)\alpha$$

$$\Rightarrow \alpha = E_1(\alpha) + \cdots + E_k(\alpha)$$

$$T(\alpha) = TE_1(\alpha) + \cdots + TE_k(\alpha)$$

$$= c_1E_1(\alpha) + \cdots + c_kE_k(\alpha)$$

$$[\because E_i(\alpha) \in R(E_i) = W_i]$$

$$= (c_1E_1 + \cdots + c_kE_k)\alpha$$

$$\Rightarrow T = c_1E_1 + \cdots + c_kE_k$$

This proves (i).

Conversely, suppose T along with distinct scalars c_i and non-zero operators E_i satisfy (i), (ii) and (iii).

Also $T = c_1E_1 + \cdots + c_kE_k$ ——— (1)

We multiply both side of (1) by E_i.

$$\Rightarrow TE_i = c_iE_i$$

$$\Rightarrow (T - c_iI)E_i = 0 \ \forall i.$$

Since $E_i \neq 0$ $\exists$ $\alpha \in V$ such that $E_i(\alpha$

$$(T - c_iI)(E_i(\alpha)) = 0 \ \forall i.$$

$$\Rightarrow T(E_i(\alpha)) = c_i(E_i(\alpha))$$

$$\Rightarrow c_i \text{ is a characteristic value o}$$

If c is any scalar ...

$$(T - cI) = (c_1 E_1 + \cdots + c_k E_k) - c(E_1 + \cdots + E_k)$$
$$= (c_1 - c) E_1 + \cdots + (c_k - c) E_k$$

If $(T - cI)\alpha = 0$ we must have $(c_i - c) E_i \alpha = 0$.

If α is not the zero vector, then $E_i \alpha \neq 0$ for some i.

We have $c_i - c = 0$

$\Rightarrow c_i = c$ for some i.

T is diagonalizable if every non-zero vector in the range of E_i is a characteristic vector of T.

If $T\alpha = c_i \alpha$,

$$\Rightarrow (c_1 E_1 + \cdots + c_k E_k)\alpha = c_i I(\alpha)$$
$$= c_i (E_1 + \cdots + E_k)\alpha$$

$$c_1 E_1(\alpha) + \cdots + c_k E_k(\alpha) = c_i E_1(\alpha) + \cdots + c_i E_k(\alpha)$$

$$\Rightarrow (c_1 - c_i) E_1(\alpha) + \cdots + (c_k - c_i) E_k(\alpha) = 0.$$

ie $\displaystyle\sum_{j=1}^{k} (c_j - c_i) E_j \alpha = 0$

Hence $(c_j - c_i) E_j(\alpha) = 0$ for each j.

$E_j \alpha = 0$, $j \neq i$.

Since $\alpha = E_1\alpha + \cdots + E_k \alpha$ and $E_j \alpha = 0$ for $j \neq i$.

(b) We have ...

$\Rightarrow \alpha \in$ range of $E_i = W_i$.

This completes the proof of the theorem.

6.8 The Primary Decomposition Theorem

Theorem :- 12 (Primary Decomposition Theorem)

Let T be a linear operator on the finite dimensional vector space V over the field F. Let p be the minimal polynomial for T, $p = p_1^{r_1} \cdots p_k^{r_k}$ where the p_i are distinct irreducible monic polynomials over F and let r_i are +ve integers. Let W_i be the null space of $p_i(T)^{r_i}$, $i = 1, 2, \dots, k$. Then

(i) $V = W_1 \oplus \cdots \oplus W_k$

(ii) each W_i is invariant under T.

(iii) if T_i is the operator induced on W_i by T, then the minimal polynomial for T_i is $p_i^{r_i}$.

Proof :-

Let $f_i(x) = \dfrac{p(x)}{p_i(x)^{r_i}} = \prod_{j \neq i} p_j(x)^{r_j}$, $i =$

(7)

$, \dots, k$ — $\{$ — prime polyno-mials. By known theorem,

"Let f be a non-scalar monic polynomial over the field F and let $f = p_1^{n_1} \dots p_k^{n_k}$ be the prime factorization of f. For each j, $1 \le j \le k$, let $f_j = f / p_j^{n_j} = \prod_{i \ne j} p_i^{n_i}$. Then $f_1, \dots, f_k$ are relatively prime."

the polynomials $f_1(x), \dots, f_k(x)$ are relatively prime.

There are polynomials $g_1(x), \dots, g_k(x)$ such that $f_1(x) g_1(x) + \dots + f_k(x) g_k(x) = 1$.

$$\text{i.e.} \sum_{i=1}^{k} f_i g_i = 1.$$

If $i \ne j$ then $f_i(x) f_j(x)$ is divisible by the polynomial p, because if $f_i f_j$ contain each $p_m^{r_m}$ as a factor.

Let $h_i(x) = f_i(x) g_i(x)$ and

$$E_i = h_i(T) = f_i(T) g_i(T).$$

(8)

since $h_1(x) + \cdots + h_k(x) = 1$

$\Rightarrow h_1(T) + \cdots + h_k(T) = 1$

and p divides $f_i f_j$ for $i \neq j$. we

$E_1 + \cdots + E_k = I$.

Also $f_i(x) f_j(x) = p(x) q(x)$ $\forall i \neq j$ for some $q(x)$.

$f_i(T) f_j(T) = p(T) q(T) = 0$.

$\Rightarrow f_i(T) g_i(T) f_j(T) g_j(T) = 0$ $\forall i \neq j$.

$\Rightarrow E_i E_j = 0$ $\forall i \neq j$.

$\therefore E_1 + \cdots + E_k = I$ and $E_i E_j = 0$ $\forall i \neq j$

$\Rightarrow E_i^2 = E_i$ $\forall i$.

Now to S.T the range of E_i is exa

the subspace W_i.

is To P.T $E_i \subseteq W_i$.

If α is in the range of E_i, the

$\alpha = E_i \alpha$. $\Rightarrow E_i(\alpha) = E_i^2(\alpha) = E_i(\alpha) = \alpha$

so $p_i(T)^{r_i} \alpha = p_i(T)^{r_i} E_i \alpha$

$= p_i(T)^{r_i} f_i(T) g_i(T) \alpha$

(10)

$= 0 \quad \forall\, i = 1, 2, \dots, k.$

$(\because p^{r_i} f_i g_i$ is divisible by m)

$\therefore \alpha \in$ null space of $p_i(T)^{r_i}$.

$\Rightarrow \alpha \in W_i$

$\Rightarrow$ range of $E_i \subseteq W_i$ —— ①

Conversely suppose that α is in the null space of $p_i(T)^{r_i}$

If $j \neq i$, then $f_j g_j$ is divisible by $p_i^{r_i}$.

$\Rightarrow f_j(x)\alpha = q(x)\, p_i(x)^{r_i}$

$\Rightarrow f_j(T)\alpha = q(T)\, p_i(T)^{r_i}(\alpha) = 0 \quad (\because \alpha \in W_i)$

$\Rightarrow f_j(T)\, g_j(T)\alpha = 0$

$\Rightarrow E_j(\alpha) = 0$ for $i \neq j$.

Also $I = E_1 + \dots + E_k$

$\alpha = I(\alpha) = E_1(\alpha) + \dots + E_k(\alpha)$.

$E_j(\alpha) = 0 \quad \forall\, i \neq j$.

$\Rightarrow \alpha \in$ range of E_i

$\Rightarrow W_i \subseteq$ range of E_i —— ②

(10) ... we have

range of $E_i = W_i$.

By known theorem, $V = W_1 \oplus \dots \oplus W_k$.

Since $TE_i = T f_i(T) g_i(T)$

$f_i(T) g_i(T) T = E_i T \ \forall i$ each

W_i is invariant under T by known theorem.

If T_i is the operator induced on W_i by T, then evidently $p_i(T_i)^{r_i} = 0$, because by defn $p_i(T)^{r_i} = 0$ on the subspace W_i.

$\therefore$ The minimal polynomial for T_i divides $p_i^{r_i}$.

Conversely, let g be any polynomial such that $g(T_i) = 0$.

$\Rightarrow g(T) f_i(T) = 0$.

Thus $g f_i$ is divisible by the minimal polynomial p of T.

i.e. $p_i^{r_i} f_i$ divides $g f_i$.

$\Rightarrow p_i^{r_i}$ divides g.

Hence the minimal polynomial for T_i is $p_i^{r_i}$.

1) NOTE :-

11) If $E_1, \ldots, E_k$ are the projections associated with the primary decomposition of T, then each E_i is a polynomial in T and accordingly if a linear operator U commutes with T then U commutes with each of the E_i i.e. each subspace W_i is invariant under U.

DEFINITION :-

Let N be a linear operator on the vector space V. We say that N is nilpotent if there is some +ve integer r such that $N^r = 0$.

Theorem :- 13

Let T be a linear operator on the finite dimensional vector space V over the field F. Suppose that the minimal polynomial for T decomposes over F into a product of linear polynomials. Then there is a diagonalizable operator D on V and a nilpotent operator N on V such that

(i) $T = D + N$

(ii) $DN = ND$.

(12) Theorem: Let $p(x) = (x-c_1)^{r_1} \cdots (x-c_k)^{r_k}$ be minimal polynomial for T where $c_1, \ldots, c_k$ distinct scalars in F.

By known theorem, (P.D.T)

$V = W_1 \oplus \cdots \oplus W_k$ where W_i = null space of $(T - c_i I)^{r_i}$

Let $E_1, \ldots, E_k$ be the corr. projections.

Then W_i = range of E_i.

Let $D = c_1 E_1 + \cdots + c_k E_k$.

Since $I = E_1 + \cdots + E_k$

$T = TE_1 + \cdots + TE_k$

$D = c_1 E_1 + \cdots + c_k E_k$.

Let $N = T - D$

$= (T - c_1 I) E_1 + \cdots + (T - c_k I) E_k$

Then $N^2 = (T - c_1 I)^2 E_1 + \cdots + (T - c_k I)^2 E_k$.

In general, $N^r = (T - c_1 I)^r E_1 + \cdots + (T - c_k I)^r E_k$.

Since $(x - c_i)^{r_i}$ is the minimal polynomial of T on W_i $(T - c_i I)^{r_i} = 0$ on W_i $\forall i$.

$\Rightarrow (T - c_i I)^{r_i} = 0$

$N^r = 0 \ \forall \ r \geq r_i$ for each i.

$\therefore N$ is nilpotent operator.

$\therefore T = D + N$ where D is diagonalizable and N is nilpotent operator.

Now suppose that we also have $T = D' + N'$ where D' is diagonalizable, N' is nilpotent and $D'N' = N'D'$.

We shall p.T $D = D'$ and $N = N'$.

Since D' and N' commute with one another and $T = D' + N'$. we see that D' and N' commute with T.

Thus D' and N' commute with any polynomial in T.

Hence they commute with D and with N.

Now we have $D + N = D' + N'$,

$$(\text{or})\quad D - D' = N' - N$$

and all four of these operators commute with one another.

Since D and D' are ~~both~~ both diagonalizab[le] and they commute they are simultaneously

Since N and N' are both nilpotent and they commute, the operator $(N'-N)$ is nilpotent. N and N' commute.

$$(N'-N)^r = \sum_{j=0}^{r} \binom{r}{j} (N')^{r-j} (-N)^j$$

and so when r is sufficiently large every term in this expression for $(N'-N)^r$ will be zero.

Now $D-D'$ is a diagonalizable operator which is also nilpotent such an operator is obviously the zero operator.

Since it is nilpotent, the minimal polynomial for this operator is of the form x^r for some $r \leq n$.

But then since the operator is diagonalizable, the minimal polynomial cannot have a repeated root, hence $r=1$ and the minimal polynomial is simply x, this s[...] the operator is zero.

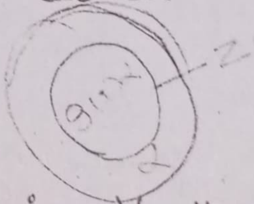
Thus $D = D'$ and $N = N'$.

(5) NOTE:- Let V be a finite dimensional vector space over an algebraically closed field F, the field of complex numbers. Then every linear operator T on V can be written as the sum of a diagonalizable operator D and a nilpotent operator N which commute. These operators D and N are unique and each is a polynomial in T.

7.1 CYCLIC SUBSPACES AND ANNIHILATORS

DEFINITION:-

If α is any vector in V, the T-cyclic subspace generated by α is the subspace $Z(\alpha;T)$ of all vectors of the form $g(T)\alpha$, g in $F[x]$. If $Z(\alpha;T) = V$, then α is called a cyclic vector for T.



DEFINITION:-

If α is any vector in V the T-annihilator of α is the ideal $M(\alpha;T)$ in $F[x]$ consisting of all polynomials g over F such that $g(T)\alpha = 0$. The unique monic polynomial p_α which generates this ideal will also be called the T-annihilator of α.

(16) Theorem :- 1

Q. Let α be any non-zero vector in linear

let p_α be the T-annihilator of α.

(i) The degree of p_α is equal to the dimension of the cyclic subspace $Z(\alpha; T)$.

(ii) If the degree of p_α is k, then the vectors $\alpha, T\alpha, T^2\alpha, \ldots, T^{k-1}\alpha$ form a basis for $Z(\alpha; T)$.

(iii) If U is the linear operator on $Z(\alpha; T)$ induced by T, then the minimal polynomial for U is p_α.

Proof :-

Let g be any polynomial over the field F. Write $g = p_\alpha q + r$ where either $r = 0$ (or) $\deg r < \deg p_\alpha = k$.

The polynomial $p_\alpha q$ is in the T-annihilator of α and so $g(T)\alpha = r(T)\alpha$.

Since $r = 0$ (or) $\deg r < k$, the vector $r(T)\alpha$ is a linear combination of the vectors $\alpha, T\alpha, \ldots, T^{k-1}\alpha$.

Since $g(T)\alpha$ is a typical vector in $Z(\alpha; T)$, this shows that these k-vectors span $Z(\alpha; T)$.

Let T be a linear operator on a finite dimensional vector space V and let W_0 be a proper T-admissible subspace of V. There exist non zero vectors $\alpha_1, \ldots, \alpha_r \in V$ with respective T-annihilators $p_1, \ldots, p_r$ such that (i) $V = W_0 \oplus Z(\alpha_1 ; T) \oplus \ldots \oplus Z(\alpha_r ; T)$

(ii) p_k divides p_{k-1}, $k = 2, \ldots, r$.

Furthermore, the integer r and the annihilators $p_1, \ldots, p_r$ are uniquely determined by (i), (ii), and the fact that no α_k is 0.

Proof :- Step 1 :-

There exists non-zero vectors $\beta_1, \ldots, \beta_r$ in V such that

(a) $V = W_0 + Z(\beta_1 ; T) + \ldots + Z(\beta_r ; T)$

(b) if $1 \leq k \leq r$ and $W_k = W_0 + Z(\beta_1 ; T) + \ldots + Z(\beta_k ; T)$

then the conductor $p_k = s(\beta_k ; W_{k-1})$ has maximum degree among all T-conductors into the subspace W_{k-1} i.e. for every k,

(20) $r_k = \max_{\alpha \in V} \deg s(\alpha; W_{k-1})$.

This step depends only upon the fact that that W_0 is an invariant subspace.

If W is a proper T_ invariant subspace, then $0 < \max_{\alpha} \deg s(\alpha; W) \leq \dim V$.

We can choose a vector β so that ~~deg s(β)~~ $\deg s(\beta; W)$ attains that maximum.

The subspace $W + Z(\beta; T)$ is then T- invariant and has dimension larger than $\dim W$.

Apply this process to $W = W_0$ to obtain β_1.

If $W_1 = W_0 + Z(\beta_1; T)$ is still proper, then apply the process to W_1 to obtain β_2.

Continue in that manner. Since $\dim W_k > \dim W_{k-1}$ we must reach $W_r = V$ in not more than $\dim V$ steps.

Step 2 :- Let $\beta_1, \ldots, \beta_r$ be non-zero vectors which satisfy conditions (a) and (b) of step 1.

Fix k, $1 \leq k \leq r$.

because any non-trivial linear relation between these would give us a non-zero polynomial g such that $g(T)\alpha = 0$ and $\deg g < \deg p_\alpha$ which is absurd.

This proves (i) and (ii).

Let U be the linear operator on $Z(\alpha; T)$ obtained by restricting T to that subspace.

If g is any polynomial over F, then

$$
\begin{aligned}
p_\alpha(U) g(T)\alpha &= p_\alpha(T) g(T)\alpha \\
&= g(T) p_\alpha(T)\alpha \\
&= g(T)\cdot 0 \\
&= 0
\end{aligned}
$$

Thus the operator $p_\alpha(U)$ sends every vector in $Z(\alpha; T)$ into 0 and is the zero operator on $Z(\alpha; T)$.

Furthermore, if h is a polynomial of degree $< k$, we cannot have $h(U) = 0$, for then $h(U)\alpha = h(T)\alpha = 0$.

This is a contradiction for the defn of p_α.

$\therefore$ p_α is the minimal polynomial for U.

This completes the proof of the theorem.

Let $\alpha_i = U\alpha$, $i = 1, \dots, k$, then the ... of U on the ordered basis $\mathcal{B} = \{\alpha_1, \dots, \alpha_k\}$ is

$$U\alpha_i = \alpha_{i+1}, \quad i = 1, \dots, k-1$$

$$U\alpha_k = -c_0\alpha_1 - c_1\alpha_2 - \dots - c_{k-1}\alpha_k$$

Where $p_\alpha = c_0 + c_1 x + \dots + c_{k-1}x^{k-1} + x^k$. The expression for $U^k\alpha + c_{k-1}U^{k-1}\alpha + \dots + c_1 U\alpha + c_0\alpha = 0$.

This says that the matrix of U in the ordered basis $\mathcal{B}$ is

$$
\begin{bmatrix}
0 & 0 & 0 & \cdots & 0 & -c_0 \\
1 & 0 & 0 & \cdots & 0 & -c_1 \\
0 & 1 & 0 & \cdots & 0 & -c_2 \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
0 & 0 & 0 & \cdots & 1 & -c_{k-1}
\end{bmatrix}.
$$

This is called the companion matrix of the monic polynomial p_α.

7.2 Cyclic Decompositions and the Rational Form

Definition :-

Let T be a linear operator on a vector space V and let W be a subspace of V. We say that W is T-admissible if

(i) W is invariant under T

(ii) if $f(T)\beta$ is in W, $\exists$ a vector γ in W such that $f(T)\beta = f(T)\gamma$.

We know that f divides each g_i.

Hence $\beta_0 = f\gamma$.

Since W_0 is T-admissible, $\beta_0 = f\gamma_0$

where $\gamma_0 \in W$.

$\therefore$ Each of the subspaces $W_1, W_2, \ldots, W_r$ is T-admissible.

Step-3:

There exist non-zero vectors $\alpha_1, \ldots, \alpha_r$ in V which satisfy conditions

(i) $V = W_0 \oplus Z(\alpha_1; T) \oplus \cdots \oplus Z(\alpha_r; T)$

(ii) p_k divides p_{k-1}, $k = 2, \ldots, r$.

Start with vectors $\beta_1, \ldots, \beta_r$ as in step 1.
Fix k, $1 \le k \le r$. We apply step 2 to the vector $\beta = \beta_k$ and the T-conductor $f = p_k$. We obtain

$$p_k \beta_k = p_k \gamma_0 + \sum_{1 \le i < k} p_k h_i \beta_i .$$

Where $\gamma_0 \in W_0$ and $h_1, \ldots, h_{k-1}$ are polynomials

Let $\alpha_k = \beta_k - \gamma_0 - \sum_{1 \le i < k} h_i \beta_i$

(24)

Since $\beta_k - \alpha_k \in W_{k-1}$,

$$s(\alpha_k; W_{k-1}) = s(\beta_k; W_{k-1}) = f_k \quad \text{--- (3)}$$

Since $p_k \alpha_k = 0$, we have $W_{k-1} \cap Z(\alpha_k; T) = \{0\}$. — (4)

Because each α_k satisfies (3) and (4), it follows that p_k is the T-annihilator of α_k.

In other words, the vectors $\alpha_1, \ldots, \alpha_r$ define the same sequence of subspaces $W_1, W_2, \ldots$ as do that vectors $\beta_1, \ldots, \beta_r$ and the T-conductors $p_k = s(\alpha_k, W_{k-1})$ have the same maximality properties (condition (b) of step 1).

The vectors $\alpha_1, \ldots, \alpha_r$ have the additional property that the subspaces W_0, $Z(\alpha_1; T)$, $Z(\alpha_2; T)$, ... are independent.

It is therefore easy to verify condition (ii)

Since $p_i \alpha_i = 0$ for each i, we have the trivial relation $p_k \alpha_k = 0 + p_1 \alpha_1 + \cdots + p_{k-1} \alpha_{k-1}$

Apply step 2 with $\beta_1, \ldots, \beta_k$ replaced by $\alpha_1, \ldots, \alpha_k$ and with $\beta = \alpha_k$.

... any vector in V and let

$f = s(\beta ; W_{k-1})$.

If $f\beta = \beta_0 + \sum_{1\le i\le k} g_i\beta_i$, $\beta_i \in W_i$ then (a)

f divides each polynomial g_i and $\beta_0 = f\gamma_0$, where γ_0 is in W_0.

If $k=1$, W_0 is T-admissible. In order to prove the assertion for $k>1$, apply the division algorithm.

(a) $g_i = fh_i + r_i$, $r_i = 0$ (or) $\deg r_i < \deg f$.

To s.T $r_i = 0$ for each i.

Let $\gamma = \beta - \sum_{1}^{k-1} h_i\beta_i$.

Since $\gamma - \beta \in W_{k-1}$, $s(\gamma ; W_{k-1}) = s(\beta ; W_{k-1})$

$= f$

$$f\gamma = \beta_0 + \sum_{1}^{k-1} r_i\beta_i .$$

Suppose that some r_i is different from 0.

Let j be the largest index i for which $r_i \neq 0$. Then $f\gamma = \beta_0 + \sum_{1}^{j} r_i\beta_i$, $r_j \neq 0$ —(1)

and $\deg r_i < \deg f$.

Let $p = s(\gamma ; W_{j-1})$.

Since W_{k-1} contains W_{j-1}, the conductor $f = s(\gamma ; W_{k-1})$ must divide p.

$p = fg$

Apply $g(T)$ to both sides of (1)

$p\gamma = gf\gamma$

$$p\gamma = g r_j\beta_j + g\beta_0 + \sum_{1\le i<j} g r_i\beta_i \quad \text{—(2)}$$

By defn, $p\gamma \in W_{j-1}$ and the last two terms on the right side of (2) are in W_{j-1}

$\therefore g r_j \beta_j \in W_{j-1}$.

Now we use condition (b) of step 1.

$$\begin{aligned}\deg (g r_j) &\geq \deg s(\beta_j ; W_{j-1})\\ &= \deg p_j\\ &\geq \deg s(\gamma ; W_{j-1})\\ &= \deg p\\ &= \deg (fg)\end{aligned}$$

Thus $\deg r_j \geq \deg f$.

This is a contradiction for the choice of j.

(ii) If $V = V_1 \oplus \cdots \oplus V_k$, where each V_i is invariant under T, then $fV = fV_1 \oplus \cdots \oplus fV_k$.

(iii) If α and γ have the same T-annihilator then $f\alpha$ and $f\gamma$ have the same T-annihilator.

(7) $\therefore \dim Z(f\alpha; T) = \dim Z(f\gamma; T)$.

Now we proceed by induction to s.T $r = s$ and $p_i = q_i$ for $i = 1, 2, \ldots, r$. The argument consists of counting dimension in the right way.

We shall give the proof that if $r \geq 2$ then $p_2 = q_2$ and from that the induction should be clear.

suppose that $r \geq 2$. Then

$\dim W_0 + \dim Z(\alpha_1; T) < \dim V$.

We know that $p_1 = q_1$,

We know that $Z(\alpha_1; T)$ and $Z(\gamma_1; T)$ have the same dimension.

$\therefore \dim W_0 + \dim Z(\gamma_1; T) < \dim V$.

Which shows that $s \geq 2$.

(8) not $p_2 = q_2$. From the two decompositions of V, we obtain two decompositions of the subspace p_2V.

$$(7)\; \begin{cases} p_2 V = p_2 W_0 \oplus Z(p_2\alpha_1; T) \\ p_2 V = p_2 W_0 \oplus Z(p_2\gamma_1; T) \oplus \cdots \oplus Z(p_2\gamma_2; T). \end{cases}$$

From ① and ②, we have $p_2\alpha_i = 0$, $i \geq 2$.

since we know that $p_1 = q_1$, fact (iii) above tells us that $Z(p_2\alpha_1; T)$ and $(Z(p_2\gamma_1; T)$ have the same dimension.

Hence it is apparent from (b) that

$\dim Z(p_2\gamma_i; T) = 0$, $i \geq 2$

We conclude that $p_2\gamma_2 = 0$ and q_2 divides p_2. The argument can be reversed to s.T p_2 divides q_2.

$\therefore p_2 = q_2$

This completes the proof of the theorem

Γ_k ... each p_i with $i < k$.

Step 4 :-

The number r and the polynomial $p_1, \ldots, p_r$ are uniquely determined by the conditions (i), (ii) and the fact that no α_k is 0.

Suppose that in addition to the vectors $\alpha_1, \ldots, \alpha_r$. We have non-zero vectors $\gamma_1, \ldots, \gamma_s$ with respective T-annihilators $g_1, \ldots, g_s$ such that

$$V = W_0 \oplus Z(\gamma_1 ; T) \oplus \cdots \oplus Z(\gamma_s ; T)$$

$$g_k \text{ divides } g_{k-1}, \quad k = 2, \ldots, s \quad \text{— (5)}$$

We s.T $r = s$ and $p_i = g_i$ for each i.

It is easy to see that $p_1 = g_1$. The polynomial g_1 is determined from (5) as the T-conductor of polynomials f say that $f\beta \in W_0$ for every $\beta \in V$.

is polynomials f such that the range of $f(T)$ is contained in W_0.

Then $S(V ; W_0)$ is a non-zero ideal

(26) ... polynomial ...

The polynomial g_1 is the monic gen... of that ideal, for this reason.

Each $\beta \in V$ has the form

$$\beta = \beta_0 + f_1\gamma_1 + \cdots + f_s\gamma_s \quad \text{and}$$

$$g_1\beta = g_1\beta_0 + \sum_1^s g_1 f_i \gamma_i.$$

Since each g_i divides g_1, we have $g_1\gamma_i = 0 \ \forall i$ and $g_1\beta = g_1\beta_0$ is in W_0.

Thus g_1 is in $S(V ; W_0)$.

Since g_1 is the monic polynomial of least degree which sends γ_1 into W_0, we see that g_1 is the monic polynomial of least degree in the ideal $S(V ; W_0)$.

By the same argument, p_1 is the generator of that ideal, so $p_1 = g_1$.

If f is a polynomial and W is a subspace of the set of all vectors ~~for~~ $f\alpha$ with $\alpha \in W$.

We have left to the exercises to proofs of the following three facts.

(ii) p and f have the same prime factors, except for multiplicities.

(iii) If $p = f_1^{r_1} \dots f_k^{r_k}$ is the prime factorization of p, then $f = f_1^{d_1} \dots f_k^{d_k}$ where d_i is the nullity of $f_i(T)^{r_i}$ divided by the degree of f_i.

Proof :-

Consider a cyclic decomposition

$V = Z(\alpha_1 ; T) \oplus \dots \oplus Z(\alpha_r ; T)$ of V.

Let $P_1 = p$, Let U_i be the restriction of T to $Z(\alpha_i ; T)$, then U_i has a cyclic vector and so p_i is both the minimal polynomial and the characteristic polynomial for U_i.

$\therefore$ The characteristic polynomial f is the product $f = P_1 \dots P_r$, is evident from the block form

$$A = \begin{bmatrix} A_1 & 0 & \dots & 0 \\ 0 & A_2 & \dots & 0 \\ 0 & 0 & \dots & A_n \end{bmatrix}$$

Which the matrix of T assumes in a suitable basis clearly $P_1 = p$ divides f.

This proves (i).

32

Obviously any prime divisor of p is a prime-divisor of f.

Conversely, a prime divisor of $f = P_1 P_2 \dots P_r$ must divide one of the factors P_i, which is divides P_1.

Let $p = f_1^{r_1} \dots f_k^{r_k}$ be the prime factorization of p by the primary decomposition theorem.

If V_i is the null space of $f_i(T)^{r_i}$, then $V = V_1 \oplus \dots \oplus V_k$ and $f_i^{r_i}$ is the minimal polynomial of the operator T_i, obtained by restriction T to the invariant subspace V_i.

Apply part (ii) to the operator T_i.

Since its minimal polynomial is a power of the prime f_i, the characteristic polynomial for T_i has the form $f_i^{d_i}$, where $d_i \geq r_i$.

Obviously $d_i = \dfrac{\dim V_i}{\dim f_i}$ and $\dim V_i = \text{nullity } f_i(T)^{r_i}$.

Since T is the direct sum of the operators $T_1, \dots, T_k$ the characteristic polynomial f is the product $f = f_1^{d_1} \dots f_k^{d_k}$.

Corollary :-

If T is a linear operator on a finite dimensional vector space, then every T-admissible subspace has a complementary subspace which is also invariant under T.

Proof :-

Let W_0 be an admissible subspace of V.

If $W_0 = V$, the complement is $\{0\}$.

If W_0 is proper, apply (C.D. Theorem) and let $W_0' = Z(\alpha_1; T) \oplus \cdots \oplus Z(\alpha_r; T)$.

Then W_0' is invariant under T and $V = W_0 \oplus W_0'$.

Corollary :-

Let T be a linear operator on a finite-dimensional vector space V.

(a) There exists a vector α in V such that the T-annihilator of α is the minimal polynomial for T.

(b) T has a cyclic vector $\Leftrightarrow$ the characteristic and minimal polynomials for T are identical.

Proof :-

If $V = \{0\}$, the results are trivially true. If $V \neq \{0\}$, let $V = Z(\alpha_1; T) \oplus \cdots \oplus Z(\alpha_r; T)$ where the T-annihilators $p_1, \ldots, p_r$ are such that p_{k+1} divides p_k, $1 \leq k \leq r-1$.

By known theorem (C.D.T), p_1 is the minimal polynomial for T.

is the T-conductor of V into $\{0\}$.

This proves (a).

We know that if T has a cyclic vector, the minimal polynomial for T coincides with the characteristic polynomial.

Choose any α as in (a).

If the degree of the minimal polynomial is $\dim V$, then $V = Z(\alpha; T)$.

Generalized Cayley - Hamilton Theorem :-

Let T be a linear operator on a finite-dimensional vector space V, let p and f be the minimal and characteristic polynomials for T, respectively.

(i) p divides f.

Note :-

If T is a nilpotent linear operator on a vector space of dimension n, then the characteristic polynomial for T is x^n.

Theorem :- 5.2

Let F be a field and let B be an $n \times n$ matrix over F. Then B is similar over the field F to one and only one matrix which is in rational form.

Proof :-

Let T be a linear operator on F^n which is represented by B in the standard ordered basis.

There is some ordered basis for F^n in which T is represented by a matrix A in rational form then B is similar to this matrix A.

Suppose B is similar matrix over F to another matrix C. which is in rational form.

This means simply that there is some ordered basis for F^n in which the operator T is represented by the matrix C.

If C is the direct sum of companion matrix C_i of monic polynomial's $q_1 \ldots q_s$ such that q_{i+1} divides q_i for $i = 1$ to $s-1$ then it is apparent that we shall have non-zero vectors $\beta_1 \ldots \beta_s$ in V with T- annihilators $q_1 \ldots q_s$ such that $V = Z(\beta_1 ; T) \oplus \cdots \oplus Z(\beta_s ; T)$.

But then by the uniqueness statement in the cyclic decomposition theorem the polynomials q_i all identical in the polynomials p_i which define the matrix A.

Thus $C = A$.

DEFINITION :-

An $n \times n$ matrix A which is the direct sum

$$A = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & A_r \end{pmatrix}$$

of companion matrix of non-scalar monic polynomial's $p_1, \ldots, p_r$ such that p_{i+1} divides p_i for $i = 1$ to $r-1$ will be said to be in rational form.